Certified Ethical Hacker (CEH) v 8 Study Guide

The EC-Council Certified Ethical Hacker Certification Exam is identified as exam code 312-50v8. The certification covers the fundamentals of hacking, foot printing, and scanning. This study guide will focus on Trojans, LINUX, Severs, Networks, and other forms of hacking to enable Ethical Hackers to succeed in their field.

www.trainace.com/security

Advanced Security is the Cyber Security training branch of TrainACE. We provide cyber classes that range from baseline (ie. The Certified Ethical Hacker and Security+) all the way up to the most advanced security courses on the planet like our Advanced Exploit Development class. Class options include in-classroom, custom on-site, live online and self-paced pre-recorded online. Get more information at www.TrainACE.com

Q: Robert hopes to start a career in computer security. As a new college-level student, he has just learned the term ethical hacking, which is a key part of secure information systems. Of the below options, choose the options which will be key areas of expertise for Robert's future career.

Answer is complete. Select more than one answer if applicable.

a. Robert needs to gain a large body of knowledge about how computers function, including with regard to networking and programming.
b. Operating systems are very important to Robert's career. Because companies will utilize varying operating systems, including Windows (multiple versions), Mac (multiple versions), UNIX, and Linux, he must develop an advanced understanding of each of the major operating systems.
c. Robert should gain familiarity with computing or hardware platforms, which are key to software development.
d. Scott should be able to write reports related to his field and have great expertise in communication relating to computer security.

Solution: **All of the above are correct.**

Breakdown: Each of the above areas is important for Robert's future career. In order to be an ethical hacker, he must understand how computers work, be able to work with any operating system (Windows, Mac, UNIX, and Linux), understand the underlying hardware platforms required, and be able to communicate with laypersons and other computer security professionals through correspondence and reports.

Q: Which type of hacker uses their computer knowledge to invade the privacy of others, thereby breaking security laws and rendering the security of information systems weak?

a. Red Card, or Security providing organizations
b. Gray Hat
c. Black Hat
d. White Hat

Solution: The correct answer is C.

Breakdown: Black Hat hackers have no qualms with breaking the law, bursting through security systems to access the private files and information of computers and individuals. They build their knowledge base in computer security to break security laws and weaken the security of information systems.

Hacker Classifications are as follows:

- **Black Hat Hackers** (Crackers): As above, these hackers seek to gain access to private files and information by attacking information systems.
- **Gray Hat Hackers**: This is the 'gray area' crowd. Sometimes they choose to defend an information system or network, and other times they put on their Black Hat and break laws to achieve their goals.
- **White Hat Hackers** (Ethical Hackers): These hackers have built their knowledge base in order to defend information systems. They use their computer skills to increase, rather than decrease, the security of networks.
- **Security Providing Organizations**: An organization or community that delivers computer security to networks and security systems.

Q: What is true about vulnerability in computer security?

a. This security weak spot is discovered and possibly exploited in a Target of Evaluation and results from failed analysis, design and implementation, or an operation.
b. It is caused by the incompetence of humans, natural disasters, or other indefensible situations.
c. This agent can take advantage of a weakness in an information system or network.
d. It is the threat or potential threat of a security violation and only occurs where there is a situation, action, or event that has the potential to break through security and damage a network or information system.

Solution: The correct answer is A.

Breakdown: **Vulnerability** is defined as a weak spot or lack of safeguarding procedure(s) that could likely be exploited by one or more threats, causing damage to a network and/or information system. Vulnerabilities can be found in hardware, firmware, software, applications, system utility and configuration settings/files, and operating systems.

A **threat** is simply the sign or indication of a possible negative event. A threat can be caused by a computer user or even through a natural occurrence. Unlike a threat, vulnerability is the agent that can or does exploit a weak point.

Q: **Which of the policies listed below is a valid set of rules regarding connecting to a system to an internal network while physically in a different location**?

a. Computer security policy
b. User Account Policy
c. Remote access policy
d. Network security policy

Solution: The correct answer is C.

Breakdown: A company's **remote access policy** sets forth rules for connecting to an internal network remotely.

A **network security policy**, conversely, is more general. It lays out the basic rules for accessing the computer network, describes how the rules will be enforced, and outlines the architecture of the network environment, including the security structure.

A **computer security policy** delivers a definition of various aspects of a company's computer system and gives an outline of its goals. This ranges from a highly professional and formal document to a relaxed and informal one. Security policies are enforced by organizational policies or security mechanisms.

The **user account policy** document is one that lays out the means for someone to request an account and/or maintain an account on the computer systems or networks of an organization.

Q: How can you establish that policies, configurations, and procedural changes/updates are made in a controlled and well-documented environment?

a. Vulnerability scanning
b. Compliance
c. Change management
d. Peer review

Solution: The correct answer is C.

Q: Security, which is a measurement of how safe a system or network is for individuals and organizations, is the condition of wellbeing of information and infrastructure. With a secure system, theft (particularly undetected), tampering, and/or disruption (through Denial of Service Attacks) of services and information are limited to low or tolerable levels. Select the elements of security from the list below.

Answer is complete. Select more than one answer if applicable.

a. Integrity
b. Availability
c. Non-Repudiation
d. Authenticity
e. Confidentiality

Solution: The correct answers are A, B, D, and E.

Breakdown: Elements of security:

1. **Confidentiality**: It is a bond of trust that involves refusing to reveal details about a company, product, resource, or any other sensitive and/or proprietary information.
2. **Authenticity**: Proof of identity and origination of information.
3. **Integrity**: The level of credibility, reliability, and reputation of data and/or resources, particularly with regards to stopping unapproved or unauthorized alterations.
4. **Availability**: It refers to the accessibility and ability to utilize information or resources when desired.
5. **Non-Repudiation** - refers to **inability** of a sender to separate or disconnect him/herself via message.

Background: **In her career as an Ethical Hacker, Diane has been assigned to a new project. She must test the security of a website. The only information that she is provided about the network infrastructure is as follows**:

- Diagrams from the network infrastructure
- Names and source code for necessary security tools
- Details about the IP addresses of the network

Q: Based on the information provided above, what testing methodology is being implemented by the website?

a. White-box testing
b. Black-box testing
c. Gray-box testing
d. Alpha or simulated testing

Solution: The correct answer is A.

Breakdown: With the information Diane has been given, she determines that their website is using the white-box testing method. It's a technique whereby an organization delivers a complete picture of the infrastructure to the team testing its website.

The testing technique known as "**black-box**" is a blind situation where the team is given no information the infrastructure of the website or organization. This is the least desirable of techniques because it is a high cost, time-consuming, and low ROI process.

Gray-box testing is a mix between white-box and black-box techniques. In this methodology, the testing team is given some background of system and can design/implement their security systems based on at least some knowledge of the system knowledge.

Q: How can gray box testing be distinguished from black hat testing?

a. In white box testing, the tester has no knowledge of the target. He was given only the company's name.
b. In black box testing, the test has complete knowledge of the internal company network.
c. In gray box testing, the tester has to try to gain access into a system using commercially available tools only.
d. In gray box testing, the attacker performs attacks with a normal user account to see if he can escalate privileges.

Solution: The correct answer is D.

In the **gray box testing**, the attacker carries out attacks using just a normal user account to see if he can escalate privileges.

White box testing is a security testing method that helps a security team to validate whether application implementation actually follows the intended design, to validate implemented security functionality, and to uncover exploitable vulnerabilities.

Black box testing assumes no prior knowledge of the infrastructure to be tested. The testers must first determine the location and extent of the systems before commencing their analysis.

Q: What core principle states that an individual or party cannot deny a role it had in an action or event (this would include document transmission and more.)?

a. Non-repudiation
b. Perjury
c. Confidentiality
d. Secrecy and Privacy

Solution: The correct answer is A.

Q: Microsoft's print and file servers are among the more common targets for hackers. Which of the below is a common—but potentially harmful—vulnerability?

a. XSS
b. SQL infraction
c. Missing patches
d. Poor IV standards

Solution: The correct answer is C.

Q: Grace has made a career as an **Ethical Hacker**. Her company asks her to test the security of their server against potential Denial of Service (DoS) attacks. In order to accomplish this, she sends ICMP ECHO packets en masse to a set computer. She is employing which of the below techniques against DoS attacks?

a. Smurf Denial of Service (DoS) attack
b. Ping Flood Denial of Service (DoS) attack
c. Teardrop Denial of Service (DoS) attack
d. Land Denial of Service (DoS) attack

Solution: The correct answer is B.

Breakdown: In testing the security, Grace utilized the Ping Flood style of attack. Here, the attacker delivers a mass quantity of ICMP packets, bombarding to a target computer.

By way of further explanation, here are the definitions for a Smurf DoS attack, a teardrop attack, and a land attack (were added for fluff only). A **Smurf DoS** attack is arranged when the attacker delivers a large quantity of ICMP “Echo requests” to IP broadcasting address or addresses. A spoofed address is used so as to mask the ICMP requests.

A **teardrop DoS** attack involves a sequence of data packets, which are directed to a target system or computer with overlapping and offset field values as well as over-sized payloads. Then the target computer or system will not be able to reassemble the packets and must therefore hang, crash, or even reboot.

Finally, with a **land DoS** attack, the attacker will send a hoax/spoofed TCP SYN packet where the target host’s IP address is filled in in two places: the source field and the destination field

---

Q: There are many credos within the computer security world. Which of the below groups believes that a hacker’s purpose is to make social change, regardless of whether it involves breaking laws and/or defacing webpages?

a. Hactivists
b. Script kiddies
c. Crackers
d. Phreakers

Solution: The correct answer is A.

Breakdown: Online hactivism has seen a great deal of growth lately. Hactivists believe that they can change society through their attacks.

The act itself is called **"Hacktivism,"** which is motivated by a political or social purpose. Hacktivists hack or break into a computer network or system and deface it, or bring it down through one of the above-mentioned attacks. A hacktivist has at his disposal the exact tools and methods as any other hacker.

Script kiddies have very limited hacking skills or programming experience and use open source and free hacking software.

Crackers use their expertise in hacking, programming, and attacks to carry out damaging and usually illegal activities.

Phreakers only rip off information from communication systems.

Q: Security teams should do which of the below to reduce attack surface?

a. Harvesting
b. Scanning
c. Hardening
d. Windowing

Solution: The correct answer is C.

Q: All but one of the statements below is false. Which one is correct?

Answer is complete. Select more than one answer if applicable.

a. A threat involves a series of events and/or circumstances and that enable someone or an agent of someone to cause damage relating to information by exploiting existing vulnerabilities in IT product(s).
b. A threat exists where there is a way for someone to violate security through a circumstance, capability, action, or event. A threat has the potential to cause a security breach and/or cause harm to a system.
c. A threat is some kind of weakness or possibly where there are too few safeguards in place that is open to exploitation through some vulnerability, which has the potential to cause harm to an information system or network.
d. A threat can cause harm in a variety of ways, including destruction of a system, disclosure or modification of the data contained within the system, and/or a DoS situation.

Solution: The correct answers are A, B, and D.

Breakdown: A **threat** is a warning of the potential for an undesirable event. Humans or even natural occurrences can be the cause of an undesirable result.

Q: In his profession as an Ethical Hacker, Chistov is often assigned jobs where he needs to test the security of a website. In this case, he is assigned to check the security of a new website. He can't remember what the first step is in malicious hacking, but he needs to know it in order to protect against hackers. What is the first step?

a. Maintaining Access
b. Scanning
c. Covering\Clearing Tracks
d. Reconnaissance
e. Gaining Access

Solution: **The correct answer is D.**

Breakdown: Here is the breakdown of phases in malicious hacking:

1. **Reconnaissance**: Attacker collects details about their intended victim.
2. **Scanning**: Attacker seeks out vulnerabilities, which he will later exploit.
3. **Gaining Access**: Attacker uses the above-discovered vulnerability in order to access the network or system.
4. **Maintaining Access**: Attacker keeps his system access long enough to complete the attack.
5. **Covering/Clearing Tracks**: Attacker takes steps to avoid being discovered or penalized under the crimes code.

Q: Adam is a malicious hacker who attacks a company's server. Once he has gotten in, he sets up a backdoor on the company's server and modifies the log files. Which of the above-discussed phases includes that modification?

a. Reconnaissance
b. Maintaining access
c. Gaining access
d. Covering/Clearing tracks

Solution: The correct answer is D.

Breakdown: So, as we know, Adam placed a backdoor on a company's server in order to ensure he has total at-will access. He maintains his access to the server in this manner. But Adam wasn't finished. After he placed the convenient backdoor, he carefully modified the log files on the server to avoid detection. This malicious act could actually clue the Network Administrator into the hacker's intentions and falls within the last step of the hacker's process—covering his tracks.

Q. Stepping away from Adam's attacks, here is a question about Certificates of Authority. If two unique corporations or companies go through a merger, what should they do to make sure that the Certificate of one company would trust the Certificate generated by the other?

a. Cross-certification
b. Public Key Exchange Authorization
c. Federated Identity
d. Must start from scratch – unique PKI system required.

Solution: The correct answer is A.

Q: Which authority of PKI will verify an applicant?

a. Certificate Authority
b. Registration Authority
c. Root Central Authority
d. Validation Authority

Solution: The correct answer is B.

Q: What is the definition of a script kiddie?

a. A script kiddie utilizes hacking programs found online and developed by someone else to hack into information systems and deface websites. He is not independently knowledgeable about hacking.
b. A script kiddie has lost the respect of others in an organization. His integrity is suspect.
c. A script kiddie focuses his attacks on communication systems.
d. A script kiddie has been working with various computer systems from a young age. He is an expert in many computer fields and operating systems. His knowledgebase in networks, frameworks, software, hardware, and others is advanced. He loves to root out vulnerabilities and threats on a server to boost its security.

Solution: The correct answer is A.

Breakdown: Answer B is actually the definition of a **disgruntled employee**. This kind of employee has lost the respect of his superiors and coworkers, and can be untrustworthy. Still, this kind of employee often is more educated and skilled than a script kiddie.

Q: How can a penetration tester be differentiated from an attacker?

a. A penetration tester uses various vulnerability assessment tools.
b. A penetration tester does not test the physical security.
c. A penetration tester does not perform a sniffing attack.
d. A penetration tester differs from an attacker by his lack of malicious intent.

Solution: The correct answer is D.

Breakdown: A **penetration test** is a technique of evaluating security of a system or network by simulating attacks. This process requires an active analysis of the system/network for potential vulnerabilities resulting from poor or improper system configurations, known and/or unknown hardware or software flaws, and/or operational weaknesses in process or technical countermeasures.

Q: What is the first thing an ethical hacker must do before running a pentest?

a. Perform an nmap scan.
b. Uncover social engineering metadata.
c. Print a findings report.
d. Obtain a signed document from senior management.

Solution: The correct answer is D.

Q: What are some end objectives of an effective pentesting attempt?

a. Verify whether, certain data could still be restored with a regular backup in the event of hardware damage.
b. Examine the IT infrastructure in terms of its compliance, efficiency, effectiveness, etc.
c. Identify vulnerabilities and flaws and improve security of technical systems.
d. Catalogue the assets and resources in a system.

Solution: The correct answer is C.

Breakdown: For a successful penetration test that meets a client's expectations, a clear definition of goals is absolutely essential. If goals are not attainable or able to be achieved efficiently, the tester should notify his client in the preparation phase and recommend alternative procedures (IT audit or IT security consulting services).

Q: Penetration tests occur in phasing. Recall from a previous question the terms ‘data gathering’ and reconnaissance. During which phase(s) do these two actions occur?

a. Out-attack phase
b. Post-attack phase
c. Attack phase
d. Pre-attack phase

Solution: The correct answer is D.

Breakdown: The first step is the pre-attack phase, where the penetration tester seeks out data about their target. Otherwise known as reconnaissance, the data collection stage is important because it is the foundation on which the rest of the attack is built. So the attacker gathers all the data, from scanning Whois, DNS, and any and all networks they can discover. Then he maps out the network and soon has in front of him a total picture, including the operating system and what applications are currently running on any one of the systems.

Q: Which of the below tools (based in Linux) can be used for penetration testing?

a. JPlag
b. Vedit
c. Ettercap
d. BackTrack (now KALI)

Solution: The correct answer is D.

Q: The PCI-DSS requires organization to perform external pentests. How often will this organization need to be done?

a. Once a quarter
b. At least once a year and after a major change or update
c. Every two years
d. Once a year

Solution: The correct answer is B.

Q: What method is the most widespread method for an attacker to find victims for social engineering strikes?

a. Phone
b. War driving
c. Session hijacking
d. Email

Solution: The correct answer is A.

Breakdown: Surprisingly enough **phone** attacks are the most common of the social engineering attacks. **What exactly is social engineering?** It's a way of conning people into divulging their personal and financial information, account logins, pin numbers, and passwords.

Sometimes **war driving** is referred to as access point mapping. This is when a hacker undertakes to find exploitable connections through locating wireless networks while driving.

Session hijacking refers to the abuse/unauthorized use of a computer session in search of private and/or proprietary information available on a computer system. This word is most often used to refer to the illicit theft of a 'magic cookie' used to allow a user to login via remote server.

TCP session hijacking occurs when a hacker seizes a TCP session between two machines that have already connected. This allows the hacker to skip past the initial authentication checks and achieve access to a computer system or network.

Q: Jay is using Facebook, Twitter, and other social networking sites to gather information on his targets. What sort of methods is he employing? (*Select 2.)*

a. Distributed denial of service attack
b. MiTM attack
c. Teardrop attack
d. SQL injection attack
e. Phishing attack
f. Social engineering attack

Solution: The correct answers are E and F.

Q. A tester detects an access point via WPA2 during a routine wireless penetration test. Which of the below attacks would be useful in obtaining a key?

a. First she needs to reset the MAC address of the wireless network card. Next, she can utilize the AirCrack tool to capture the key.
b. She should capture the WPA2 authentication handshake and then work to crack the handshake.
c. She should try the key cracking tool airodump-ng [airocrack-ng] through the network ESSID.
d. She must reset the network and start from scratch because WPA2 simply cannot be cracked.

Solution: The correct answer is B.

Q: What is the chief reason that using a stored biometric opens an individual up to an attack?

a. This kind of authorization runs a comparison on the original to the copy rather than the other way around.
b. The symbols used to represent a stored biometric might not be original in a digital or stored format.
c. An attacker can use the stored biometric data to easily masquerade as the individual identified by that data.
d. A stored biometric is no longer “something you have” and instead becomes “something you are.”

Solution: The correct answer is C.

Q: Which of the below scans can measure facial and other features through the use of a webcam or other digital camera capable of taking videos?

a. Iris scan
b. Facial recognition scan
c. Signature dynamics scan
d. Retina scan

Solution: The correct answer is A.

Q: You are starting a new Nessus policy and need to turn on (or enable) Global Variable Settings. Where should you go to enable them?

a. Plugins
b. General
c. Preferences
d. Credentials

Solution: The correct answer is C.

Q: A pentester (otherwise known as a penetration tester) keys in the below command. What kind of scan is this?

nmap -N -sS -PO -p 123 192.168.2.25

a. Idle scan
b. Intense scan
c. Stealth scan
d. Fin scan

Solution: The correct answer is C.

Q: If a hacker wanted to modify prices on a website, which of the below methods would he use? As an aside, there are no alerts shown through IDS.

a. XSS
b. Hidden form fields
c. SQL injection
d. Port scanning

Solution: The correct answer is B.

Q: What kind of a scan delivers specially designed packets to a system (remote) and then analyzes the output?

a. Active
b. Bounce
c. Passive
d. Directive

Solution: The correct answer is A.

Background: You run the following command in the command prompt:

Telnet <IP Address><Port 80>
HEAD /HTTP/1.0
<Return>
<Return>

Q: Which of the below of information collection methods did you use?

a. Port scanning
b. Dumpster diving
c. OS fingerprinting
d. Banner grabbing

Solution: The correct answer is D.

Breakdown: **Banner grabbing** is a type of enumeration/inventory technique utilized by hackers to extract information about computers and or hosts on a network and determining which services are active on its open ports. A **port** is a way separate systems can talk to each other, a medium. A port, a unique 16-bit code/number, distinguishes each service on any host. This can be used by hackers or by an administrator to perform an inventory check for their network.

OS Fingerprinting is the simplest and most straightforward way to discover which operating system is being used on a remote system. This kind of detection makes it much easier to hack a system. Fingerprinting compares data packets, which are sent by a target system. There are two categories of fingerprinting methods:

1. Active fingerprinting
2. Passive fingerprinting

With active fingerprinting, ICMP (Internet Control Message Protocol) messages are pushed to the target system. Ordinarily, remote system's response message will reveal the operating system. In **passive fingerprinting**, the hacker uses a 'sniffer' such as Wireshark to capture traffic, analyzing the number of hops to discover the operating system. In passive fingerprinting, no traffic is sent—it is only collected.

Dumpster diving refers to rummaging through an individual's waste/trash, including discarded mail, in an attempt to discover important or private information.

The first step in learning the specifics of the open ports on any system is **port scanning**. Hackers utilize port scanning to locate a "hackable" network or server with an easily detectible weakness, hole, or vulnerability.

Q: Which of the below techniques cannot be used to perform active OS fingerprinting?

Answer is complete. Select more than one answer if applicable.

a. Sniffing and analyzing packets
b. ICMP error message quoting
c. Sending FIN packets to open ports on a remote system.
d. Analyzing the email headers.

Solution: Answers A and D are correct.

These are ways to perform passive OS fingerprinting.

Email header passive OS fingerprinting: In this method an attacker uses the e-mail header to detect the remote OS. It (the header) is analyzed and gives information about the mail daemon of the remote computer. Each OS uses a special mail daemon, so an attacker can then figure out the OS.

The other options, ICMP error message quoting, sending FIN packets to open ports on a remote system, are active forms of fingerprinting for the OS.

Q: Which of the below types of privacy invasion involves modifying data or information before or during input into a computer system with the intent to steal or commit fraud?

a. Spoofing
b. Wiretapping
c. Eavesdropping
d. Data diddling

Solution: The correct answer is D.

Breakdown: **Data diddling** involves altering data prior to or during input to a computer in an attempt to commit fraud. It also is used to describe the act of deliberately changing information, programs, and/or documentation.

Eavesdropping is the act of snooping/listening in on private conversations. This is also the term used to describe attackers watching and analyzing network traffic.

Spoofing is a method used by hackers to make a transmission seem to have originated from a familiar or authentic source by faking IP addresses, email addresses, and caller ID. In IP spoofing, a hacker will tweak packet headers by inserting someone else's IP address to mask his identity. However, spoofing is not functional for surfing the web or chatting online because the responses will be misdirected by the false IP address.

Hackers use **wiretapping** to monitor phone and Internet communications where they are not a party. Wiretapping is actually legal, but ONLY with prior consent. Police officials and governmental authorities regularly utilize “legalized wiretapping” to in relation to investigations, whether public or secret.

Q: Molly is employed as an Ethical Hacker. Her newest project involves testing the security of a website. Which of the below are the 3 pre-testing phases of an attack used in measuring the security of this website?

a. Identifying the active system
b. Web server hacking
c. Enumerating the system
d. Session hijacking
e. Placing backdoors
f. Footprinting

Solution: These are the three pre-testing phases used in the attack:

(f) Footprinting
(a) Identifying an active system
(c) Enumerating a system

Q: Which of the below will record everything a user types using a keyboard connected to the machine it is installed within?

a. Firewall
b. Port scanner
c. Keystroke logger
d. Line conditioner

Solution: The correct answer is C.

A **firewall** is a utility that is used to protect an internal network or intranet against unauthorized access via the Internet or other external networks. A firewall sets restrictions on access (inbound and outbound) and performs analysis on traffic (between the network and the Internet).

If installed, a **keystroke logger** or keylogger will log and record everything a person types using their keyboard. Both hardware and software forms of keyloggers exist.

A **port scanner** is a software utility designed to search a network host for any open ports. It is useful to security teams performing security checks on their networks. However, it is also very useful to hackers targeting a network and its systems.

Background: Placing backdoors, web server hacking, and session hijacking are among the phases of executing attacks.

Q: From the below list, which, if any, of these tools can be used to obscure identity?

Answer is complete. Select more than one answer if applicable.

a. War dialer
b. Proxy server
c. IPChains
d. Anonymizer
e. Rootkit

Solution: Answers B, C, and D are correct.

Background: It is possible to mask your identity using firewalls (such as IPChains), a proxy server, or through an anonymizer.

A proxy server conceals the identity-related details of a user's machine, network, or system from others. The user's system first establishes a direct connection with a proxy server, and then that server then creates a connection with a remote host of the user’s choice.

Anonymizers help make a user's web surfing anonymous by removing any identifying details/information from a user's computer system while the user browses the Internet. This helps to secure the user's privacy.

Linux IPChains is free software that controls the filter and firewall capabilities on a Linux operating system. Network Administrators use it to ACCEPT, DENY, MASQ, or REDIRECT packets.

Linux IPChains: the kernel starts with three sets of rules, or chains, in the firewall as follows: input, output, and forward.

Note: Each packet (which may come from an Ethernet card or otherwise) that passes through the forward chain will also pass through the input and output chains.

A **war dialer** is a utility used by hackers to detect vulnerable modems; war dialers scan hundreds or thousands of phone numbers looking to discover an unauthorized way into the system. The tools available for this act are innumerable: a few include PhoneSweep, THC-Scan, and ToneLoc.

A **rootkit** is a toolkit or group of tools that can allow a hacker to seize administrative control of a computer system with no authorization. A rootkit does require root access to be installed onto the Linux operating system, but once it has been installed, the hacker has unlimited at-will root access.

Q: Which of the below tools can be used for footprinting?

Answer is complete. Select more than one answer if applicable.

a. Brutus
b. Sam spade
c. Traceroute
d. Whois

Solution: The correct answers are B, C, and D.

Breakdown: The traceroute, Sam spade, and whois utilities are useful for footprinting.

What is the SAM SPADE utility?

SAM SPADE is a software tool for discovering sources of email spam. It is named after a fictional private detective who unflinchingly sought out justice. The tool itself can request a DNS server to send back details about a domain, scan IP addresses for open ports, find the route of a packet transmitting between a machine and a remote system, and guess the origin of emails from their headers. It can also decode masked URLs.

What is the TRACEROUTE utility?

The TRACEROUTE utility will display the path of a specific IP packet. Traceroute uses ICMP (Internet Control Message Protocol) echo packets, displaying the Fully Qualified Domain Name (FQDN) as well as the IP address for any gateway along the route to its remote host.

Q: Markus works as an Ethical Hacker. His main project is to test the security of his client's website. He starts by performing footprinting and scanning. What does this entail?

Answer is complete. Select more than one answer if applicable.

a. Information-gathering
b. Determining the network range
c. Identifying all active machines
d. Finding any open ports and/or applications
e. Enumeration through a four-step process

Solution: Of the above choices, A, B, C, and D are correct.

Breakdown: In the **enumeration** phase, an attacker collects information and data, including the network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data. The methods utilized in this phase are listed below:

1. Obtaining Active Directory details and identifying vulnerable accounts
2. Discovering NetBIOS names
3. Employing Windows DNS queries
4. Establishing NULL sessions and queries

Q: Which of the below techniques uses a modem in order to automatically scan a list of telephone numbers?

a. War dialing
b. Warkitting
c. Warchalking
d. War driving

Solution: The correct answer is A.

War dialing uses a modem to auto-scan a list of phone numbers, often dialing each number in a local area code to search for computers, BBS systems, and fax machines. Hobbyists can use this technique for exploration, and crackers (hackers specializing in computer security) to guess passwords.

Warchalking is drawing symbols in public places to guerilla advertise an open Wi-Fi wireless network. The warchalker finds a Wi-Fi node and then draws a special symbol somewhere nearby. This is a portmanteau of the cracker terms war dialing + war driving.

Q: As Database Manager for a local company, Mick has a lot of responsibilities. He decides to set up remote control software on his work machine so that he will be able to login from home or otherwise. After installing the connection, he connects a modem to an otherwise-unused fax line. With no authentication to enable him to set a password for a host connection to the remote connection, Mick's remote connection will be accessible to for anyone to connect to his host system. Which of the below attacks can be performed on Mick's remote connection?

a. War dialing
b. Zero-day
c. War driving
d. Warchalking

Solution: The correct answer is A.

Q: Which of the below is a passive, non-direct information-gathering tool?

a. Ettercap
b. Whois
c. Nmap
d. Snort

Solution: The correct answer is B.

Breakdown: The **whois** tool is a so-called "passive" information-gathering utility. These kinds of queries can be used to discover the IP address ranges linked to a client or clients. A whois query can be run in most UNIX environments. With Windows, the whois tools, including WsPingPro and/or Sam Spade, will to do whois queries. Whois queries can be executed online via www.arin.net or at www.networksolutions.com.

Nmap is an *active* information-gathering tool. The **nmap** utility, or port scanner, is used to directly view open ports on a Linux system. Administrators can determine which of the services are currently available for external users.

Snort is more than just a character in a P.D. Eastman book. This tool is an *active* information-gathering utility. Snort is open source and designed for network intrusion prevention, as well as detection; Snort's system also operates as a network sniffer and records network activity matched with predefined signatures.

Three primary Snort modes are listed below:

- **Sniffer** mode: In this mode, snort will find the packets throughout the network and display them on the console in a continuous stream.

- **Packet logger mode**: This is the mode where packets are logged to the disk.

- **Network intrusion detection** mode: This mode offers the most options for configuration, and it also allows users to filter network traffic using their own sets of rules.

Like nmap and Snort, **Ettercap** is an active information-gathering tool. Ettercap, a UNIX and Windows-based tool for computer network protocol analysis and security audits, can intercept traffic on a network subnet/segment—thereby capturing user passwords and conducting *active* surveillance against common protocols.

Q: Determining which services are active on a target machine as well as possible entry points to attack, which of the below would you use?

a. Nmap scan
b. Ping
c. Traceroute
d. Banner grabbing

Solution: The correct answer is A.

Q: Chuck needs to perform a basic vulnerability scan using NMAP. When dealing with protocols like FTP and HTTP, what key engine does NMAP utilize?

a. SAINT
b. Metasploit
c. NESSUS
d. NMAP

Solution: The correct answer is D.

Q: While running an nmap scan for filtered ports, you send an ACK flag and receive a RST packet for open and closed ports. What kind of nmap scan did you run?

a. Null Scan -sN

b. Fin Scan -sF
c. XMAS Scan -sX
d. TCP ACK scan -sA

Solution: The correct answer is D.

Breakdown:

The TCP ACK Scan will not discover open and closed ports—it will determine whether or not a port is filtered or unfiltered. When an ACK flag is sent, Open/Closed ports will return RST. Any ports that do not respond are considered filtered.

Conversely, with **a NULL Scan**, no flags are set on a packet. The target must follow RFC 793, a TCP specification. If the port is open or filtered, it will receive no response. If the port is closed, it will receive RST.

In **Fin Scan**, a Fin flag is set on a packet. Again, the target must follow RFC 793. If a port is open or filtered, it will receive no response; yet it will receive RST if a port is actually closed.

In XMAS Scan, the FIN, URG, and PSH flags are set on a packet. The target must still follow RFC 793. It will receive no response if a port is open or filtered and will receive RST if a port is closed.

Reference: http://nmap.org/

Q: Which of the below Nmap commands is used to perform a UDP port scan?

a. nmap -sU
b. nmap -sS
c. nmap -sF
d. nmap -sN

Solution: The correct answer is A.

Breakdown:

The **nmap -sU** command performs a UDP port scan.

The **nmap -sS** command performs stealth scanning.

The **nmap -sF** command performs FIN scanning.

The **nmap -sN** command performs TCP NULL port scanning.

Q: Which nmap switch would you use to retrieve as many different protocols as possible that are being used by a remote host?

a. nmap -sO
b. nmap -sS
c. nmap -sT
d. nmap -vO

Solution: The correct answer is A.

The nmap -sO switch is used to scan IPs.

To search additional IP protocols, you can utilize the IP protocol scan. Such protocols include ICMP, TCP, and UDP. This scan will unearth uncommon IP protocols that could be active on a system.

Nmap will not allow you to combine the verbose and OS scanning options.

It will display the below error message:

Invalid argument to -v: "O"

The **nmap -sT** switch performs a TCP full scan.

The **nmap -sS** is performs a TCP half scan. Here an attacker will send a SYN packet to a target port.

Q: Which of the below represents the type of packet inspection used by a firewall when scanning the DMZ interface on a firewall Nmap reports that port 80 is unfiltered.

a. Deep
b. Stateless
c. Proxy
d. Stateful

Solution: The correct answer is B.

Q: As a contracted Ethical Hacker, Al has recently contracted to complete a project to do security checking on a website. He wants to find out which operating system is used by the web server. Which of the below commands can he use to complete this task?

Each correct answer represents a complete solution. Choose two.

a. nmap -v -O 208. 100. 2. 25
b. nc -v -n 208. 100. 2. 25 80
c. nc 208. 100. 2. 25 23
d. nmap -v -O [www.website.com]

Solution: The correct answers are A and D.

Breakdown: According to the scenario, Al will probably choose "nmap -v -O 208. 100. 2. 25" to uncover the OS used by the server. Verbose = -v / -O = TCP/IP fingerprinting (to guess the remote OS). Al could also use the DNS name of the website instead of using its server IP address. In this case, he would also use the nmap command "nmap -v -O www.website.com ".

Background: TCP/IP stack fingerprinting involves passive collecting of configuration attributes from remote devices during standard layer 4 network communications. These combinations could then be used to infer the remote operating system or to incorporate the information into a device fingerprint.

Q. Which of the below Nmap switches can be utilized to perform TCP/IP stack fingerprinting?

a. nmap -O -p
b. nmap -sU -p
c. nmap -sS
d. nmap -sT

Solution: The correct answer is A.

Q: Which of the below kinds of machines do security teams often use for attracting potential intruders?

a. Bastion host
b. Data pot
c. Files pot
d. Honeypot

Solution: The correct answer is D.

A **honeypot** is a machine/computer that can be used to draw in potential intruders or attackers. A honeypot has intentionally low security permissions and is useful in collecting intelligence about attackers and their tactics.

Q: Which of the below are password-cracking utilities? (Choose 3)

a. NMAP
b. John the Ripper
c. Cain and Abel
d. KerbCrack
e. Wireshark
f. WebGoat

Solution: The correct answers are A, B and D.

Background: Luke is an Ethical Hacker. In scanning his company's wireless network, he utilizes a free, open-source tool. The tool analyzes raw IP packets to discover the following:

- Which ports are open on the network systems?
- Which hosts are available on the network?
- Are there unauthorized wireless access points?
- Which services (application name, version) are the available hosts providing?
- Which operating systems (and OS versions) are the hosts running?
- Which types of packet filters/firewalls are being utilized?

Q: Based on the above information, which of the below tools is Luke using?

a. Nessus
b. Kismet
c. Nmap
d. Sniffer

Solution: The correct answer is C.

Nmap is an active data collection tool. The port-scanning ability of the nmap utility can be the open ports on a Linux machine. Administrators can employ this tool to discover which services are accessible to external users.

Q: Which of the below utilities is a protocol analyzer with the ability to capture packet traffic as it comes into the network ("in real time")?

a. NetWitness
b. Netresident
c. Snort
d. Wireshark

Solution: The correct answer is D.

Breakdown: **Wireshark** is a protocol analyzer with the ability to capture packet traffic as it comes into the network ("in real time"). It is free and open source, and will act as a packet sniffer, capturing network traffic for purposes of troubleshooting, development of software/communications protocol, analysis, and as a teaching tool. It was originally called Ethereal. Wireshark will work on Windows, Mac, Linux, or Unix machines

---

Q: Wireshark will excel in which one of the below situations you might face as an Ethical Hacker?

a. If you need to target networks using switches or so-called "full-duplex" hubs (which are actually switches).
b. If you need to target networks utilizing repeaters/hubs.
c. If your target is a Windows-based network.
d. If your target is a Linux-based network.

Solution: The correct answer is A.

Breakdown: When a device is a **hub**, it is convenient for capturing through **Wireshark**. A hub based on switches will only transmit 'clean' packets—whereas a real hub will simply act as a repeater with no verification of packets. Network hubs do not manage network traffic. Therefore, each packet that enters a port is repeated on every other port.

A **switch** learns and maintains a table of MAC addresses. A switch does not simply forward all packets to all other ports, but rather uses a bridge to determine which packets are forwarded to which ports.

Q: You need to obtain a packet capture for a network. Which of the below devices would allow you to capture a total picture of the traffic on the wire through Wireshark?

a. Network tap
b. Layer 3 switch
c. Network bridge
d. Router

Solution: The correct answer is B.

Q: Steve B. is a black hat and wishes to run a port scan on a machine he is attacking to try to find some open ports and other valuable information. He decides to use the nmap command to execute his scan. Because he is worried that the admin may be running

PortSentry in order to block any scans, he will slow the scan downs so that they are less suspicious. What nmap options can he use to do this?

a. nmap -sS -PT -PI -O -T1 <ip address>
b. nmap -sF -P0 -O <ip address>
c. nmap -sO -PT -O -C5 <ip address>
d. nmap -sF -PT -PI -O <ip address>

Solution: The correct answer is A.

Q: You want to access and pull password files from various websites. These passwords are stored within the index directory of a website's server. What could you use from the below options that would allow you to do this?

a. Google
b. Nmap
c. Whois
d. Sam Spade

Solution: The correct answer is A.

Google hacking is a way to find and retrieve password files which have been indexed within a web server's directory) from specified websites. Search queries on Google will potentially discover information from a web server's index directory.

Q: While browsing an online job board, you come across a job posting for tech professionals. You visit the company's website and analyze its contents and conclude that they are looking for professionals who possess a strong knowledge of Windows Server 2003 and Windows active directory installations. Which of the below hacking phase(s) does this fall under?

a. Reconnaissance
b. Gaining access
c. Covering tracks
d. Scanning

Solution: The correct answer is A.

Q. When a match for an alert rule is found in Snort, the intrusion detection system carries out which of the below actions?

a. Blocks a connection with the source IP address in the packet

b. Halts rule query, sends a network alert, and freezes the packet
c. Continues to analyze the packet until each rule has been checked
d. Drops the packet and selects the next packet detection option

Solution: **The correct answer is C.**

Background: Anonymizers are used to mask a user's web surfing. Anonymizers work by removing all identifying information from a computer throughout the time the user is surfing online. Internet users seeking privacy will use an anonymizer. Once they have enabled online access anonymization, each link they open for the remainder of the session will also be accessed anonymously, with no extra actions on the part of the user. However, anonymizers do have limitations.

Q: Which of the below represent examples of such limitations?

Answer is complete. Select more than one answer if applicable.

a. Secure protocols
b. Plugins
c. ActiveX controls
d. Java applications
e. JavaScript

Solution: Answers A, B, C, D, and E are correct.

Background: These are the limitations of anonymizers:

1. **Secure protocols** including '**HTTPS**:' will not be anonymized correctly by an anonymizer because a browser must be able access the site directly in order to maintain truly secure encryption.
2. Third-party plugins accessed by websites cannot be properly anonymized. There is simply no way to ensure that any independent direct connection between the user's machine and a remote site will remain established.
3. When a **Java application** is accessed via an anonymizer, it cannot circumvent a Java security wall.
4. **ActiveX applications** will have nearly unlimited access to the computer system of the user.
5. The **JavaScript** language will be disabled with anonymizers that are URL-based.

Q: Which of the below is true about the **TCP/IP model**?

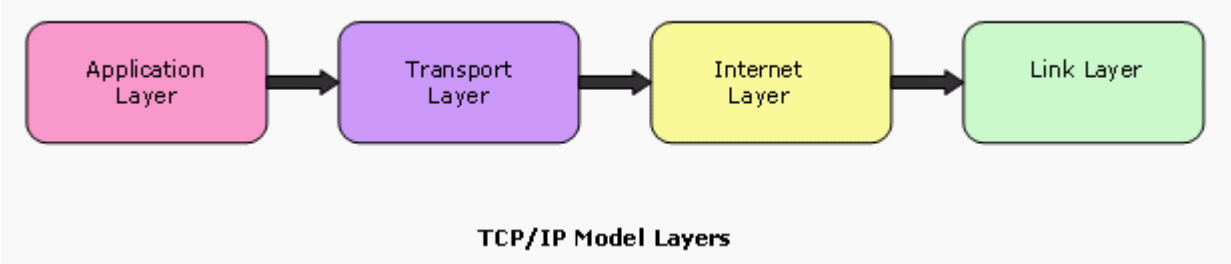
Answer is complete. Select more than one answer if applicable.

a. This model sets forth design guidelines and implementations for different networking protocols, enabling computers to interface through a network.
b. This model allows end-to-end connectivity, delineating the format of data as well as the way it is addressed, transmitted and/or routed, and even how it will be received.
c. This data model has five (5) separate layers of abstraction.
d. Each layer of this model contains several different protocols.

Solution: The correct answers are A, B, and D.

Background: As a description framework used in computer network protocols, the TCP/IP model sets forth the design guidelines in a general sense as well as the specific networking protocol implementation. This creates a way for computers to interface via network connections. TCP/IP does provide end-to-end connectivity, and also delineates the way in which data must be formatted, as well as addressed, transmitted and routed, and even the way it will be received. There are various protocols for communication services to and from computers. Another name used for this model is the Internet model or the DoD model (this is because it was created by the Department of Defense).

There are four unique layers in the TCP/IP model. This is represented in the below image. The Internet Engineering Task Force (IETF) maintains the TCP/IP model and other related protocols. In another model, the OSI Reference Model, there are actually seven (7) layers. The TCP/IP model has fewer steps because it allows applications to manage actions past a certain layer.



TCP/IP Model Layers

The Application Layer (or Layer 4)

Programs communicate through application layers. Think of it as a “user interface layer.” Through application layers, browser, file-sharing software, email software, and other user-facing (the user interacts with the software directly) software can interact. Other aspects handled in this layer include encryption and session details.

The Transport Layer (or Layer 3)

In the transport layer, devices will negotiate to determine how to talk to each other over a network. This involves such decisions as communication type (e.g., User Diagram Protocol or

Transmission Control Protocol), the window size, which port, how to deal with errors, as well as sequencing. Most work done in device communications is completed through this layer.

The Internet Layer (or Layer 2)

The Internet Layer is where IP addressing, internetworking (connecting one network with others through gateways), and path determination occur. The path that a packet will take through a network is handled in this layer through routers. The protocols in this layer will examine multiple avenues to determine the most efficient way for one host to connect to the other.

The Link Layer (or Layer 1)

The link layer is responsible for encapsulating the data. The network type will determine which way this layer accomplishes it task—which encapsulation protocol is appropriate. Some of them include Ethernet, Frame Relay, PPP, HDLC or CDP. The physical connection between the devices (as well as the topology of the network) plays a major part in the selection.

Regarding answer C above: this option is invalid, as the TCP/IP model consists of not five (5) or seven (7) abstraction layers, but **a total of four (4)**.

Q: Phil needs to procure information related to a server with an IP address range that is within the IP address range that is used in Brazil. There are many registries available online for discovering the details of web server IP addresses, or reverse Domain Name Service (DNS) lookup. Which of the below registries will be most useful to him?

a. RIPE NCC
b. APNIC
c. ARIN
d. LACNIC

Solution: The correct answer is D.

Phil needs to obtain information about a web server situated in Brazil. Registries are available throughout the world, most often broken up into geographic locations. So the Latin American and Caribbean Internet Addresses Registry, or LACNIC, is the Regional Internet Registry for the Latin American and Caribbean regions and is therefore the best registry for doing a DNS lookup. LACNIC is one of five (5) regional Internet registries available worldwide. Its chief purpose is to assign and administrate IP addresses for the region of Latin America and parts of the Caribbean.

The Réseaux IP Européens Network Coordination Centre, or **RIPE NCC**, is the Regional Internet Registry (RIR) for Europe, the Middle East, and certain parts of Central Asia.

The Asia Pacific Network Information Centre (**APNIC**), Regional Internet Registry for the Asia Pacific region, assigns and administers numerical resource allocation as well as registration services to support the global operation of the Internet

The American Registry for Internet Numbers (**ARIN**) is the Regional Internet Registry (RIR) for Canada, parts of the Caribbean, some North Atlantic islands, and the United States.

Q: Routing protocols are used to show how computers communicate. From the below options, select the two routing protocols:

a. TCP or SMTP
b. BGP
c. UDP
d. RIP

Solution: The correct answers are B and D.

Q: Which of the below is a good definition the principle of **least privilege**?

a. A manager should have all the access and privileges of his or her employees.
b. People at the bottom of an organization's hierarchy should have lower privileges than the highest members of the hierarchy.
c. All users should need to input a unique password before given any access.
d. Users should have access only to the data and services that are necessary and important to perform their job(s).

Solution: The correct answer is D.

Q: Erik is a System Administrator. He has the responsibility to ensure network security for an organization. Erik is currently working with the advanced features of a Windows firewall in order to block/prevent a client machine from responding to any pings. Which of the below advanced setting types will require modification?

a. ICMP
b. SMTP
c. SNMP
d. UDP

Solution: The correct answer is A.

According to the scenario, Erik must modify the settings related to the Internet Control Message Protocol, or **ICMP**. ICMP is a protocol used when PING commands are issued and received, as well as when a ping is being responded to. This is an important part of IP that is used to report errors in datagram processing. A datagram is a basic transfer unit that is associated with packet-switched networks, an independent entity of data that carries enough information to be routed from its source to a destination computer.

Simple Mail Transfer Protocol **(SMTP-25**) is a protocol that sends e-mail messages between servers.

The Simple Network Management Protocol (**SNMP-161**) allows a router, switch, or other monitored device to run an SNMP agent. This protocol enables the management of multiple network devices from a remote workspace.

User Datagram Protocol (**UDP**) is generally used for “one-to-many” communications, through broadcast and/or multicast IP datagrams. This protocol does not guarantee delivery or verify sequencing for any datagram because it is a connectionless and often unreliable communication protocol. However, UDP provides faster transmission of data between TCP/IP hosts than TCP.

Background: When data provided to a caching name server that has not originated from a non-authentic source (in other words, a DNS source), this is called DNS cache poisoning. Once a DNS server receives this non-authentic data and caches it for future performance increases, it will be considered “poisoned” because it will thereafter supplying server clients with that non-authentic data.

Q. In order to determine the end-time for DNS cache poisoning, which of the below DNS records should you examine?

a. MX
b. NS
c. PTR
d. SOA

Solution: The correct answer is D.

Background: A **start of authority** (SOA) record contains information about the DNS zone on which it is stored and about other DNS records. A DNS zone is the area of a domain that is within the responsibility of a specific DNS server. There is only one SOA record for each DNS.

As stated above, when data is provided to a DNS serve that did not originate from authoritative Domain Name System (DNS) sources (whether due to intentional or unintentional

circumstances), it is called **DNS Cache poisoning**. To perform such an attack, the attacker discovers and takes advantage of a flaw in the DNS software. A server must correctly validate DNS responses have originated from an authentic source, or the server may end up caching incorrect entries locally and inevitably deliver them to users whom key in identical requests. Also called a “mail exchanger record,” an **MX** is also stored in the zone file of Domain Name Server (DNS). The MX record associates a domain name to another domain name sorted within an address record (an “A” record).

A name server record, or **NS** record, establishes the server that is considered an authoritative server for the DNS zone.

The **pointer record** (PTR), is housed on the Domain Name System (DNS) database responsible for mapping an IP address to a specific host name on the in-addr.arpa domain. These records are used when performing reverse DNS lookups.

Q: Which of the below items is a straightforward example of two-factor authentication?

a. Fingerprint and smartcard
b. Username/login and password
c. ID and token or pin
d. Iris scanning and fingerprinting

Solution: The correct answer is A.

Q: Which of the below methods would succeed in protecting a router from prospective smurf attacks?

a. Disabling the ability to forward ports on the router
b. Placing the router into broadcast-only mode for a full cycle
c. Disabling the router from accepting any broadcast ping messages
d. Installing a new router in the DMZ

Solution: The correct answer is C.

Q: Which information can an attacker get after tracerouting any network?

Answer is complete. Select more than one answer if applicable.

a. Network topology
b. Web administrator email address
c. Firewall locations
d. Trusted routers

Solution: The correct answers are A, C, and D.

What is Google hacking?

Google hacking is a method of utilizing the Google search engine and other Google apps to discover security holes in the configuration and/or computer code of websites use. Keying in advanced operators in the Google search engine enables a hacker to pinpoint specific strings of text in a search result.

Q: Which of the below terms is a valid Google search operator that can be used in searching for a specific file type?

a. filetype
b. inurl
c. file type
d. intitle

Solution: The correct answer is A.

The **filetype** Google search query operator can be utilized to search a specify file type. If you wanted to search all pdf files with the word hacking in their filenames, you could key in the search query filetype:pdf pdf hacking.

inurl is used to search for specified text within a URL of websites.

file type, with a space between words, is not a valid search operator.

intitle can be used to search for specified text in website titles.

Q: You need to obtain the default security report from Nessus. Which of the below Google search queries could you use?

a. filetype:pdf "Assessment Report" nessus
b. link:pdf nessus "Assessment report"
c. filetype:pdf nessus
d. site:pdf nessus "Assessment report"

Solution: The correct answer is A.

Q: Nessus is a proprietary vulnerability scanner utilized by many organizations. Which of the below is a technique used by vulnerability scanners?

a. Banner grabbing
b. Port Scanning
c. Analyzing service responses
d. Malware analysis

Solution: The correct answer is C.

Q: Which of the below ways could be used to defeat a multi-level security solution?

a. Leak data via asymmetric routing.
b. Leak data via a covert channel.
c. Leak data via steganography.
d. Leak data via an overt channel,

Solution: The correct answer is B.

Q: Administrators use Remote Desktop to gain access their servers from different locations. In which of the below ways could a hacker exploit Remote Desktop to gain access?

a. Capture any LANMAN (or LM) hashes and crack each of them with Cain and Abel.
b. Capture the RDP traffic and then decode with Cain and Abel.
c. Utilize a social engineering tool to capture the domain name of the remote server.
d. Scan the server to see what ports are open.

Solution: The correct answer is B.

RDP is an acronym for Remote Desktop Protocol.

Q: Which of the below options represents the best defense against privilege escalation (exploitation of a bug) vulnerability?

a. Patch all computers and servers immediately after the release of any updates.
b. Run apps without administrator privileges and download a content registry tool for storage of tracking cookies.
c. Run services with your least privileged account(s) and then implement multi-factor authentication, or MFA.
d. Monthly reviews of user and administrator roles.

Solution: The correct answer is C.

Q: Various devices, in the form of hardware and software, can emulate key computer services, such as browsers and email. Through these tools, system administrators can determine what vulnerabilities are enabling a hacker to break into a system. What is another name for this kind of device?

a. Honeypot
b. Router
c. Port Scanner
d. Core Switch

Solution: The correct answer is B.

Q: As the Security Consultant for a firm, Ingrid must check security for her client's network. Her client informs her that of his many concerns, the security of the firm's Web applications hosted on its Web server is the most important to him. With this in mind, which of the below should be Ingrid's highest priority?

a. Setting up an intrusion detection system (IDS).
b. Configuring a believable honeypot.
c. Scanning for open ports.
d. Scanning and removing vulnerabilities.

Solution: The correct answer is D.

Q: Detective controls help administrators find problems within an organization's processes. Choose the two options below that represent this kind of control.

a. Audits
b. DRP
c. CCTV
d. Encryption
e. Two-factor or multi-factor authentication

Solution: The correct answers are A and D.

Q: IPSec offers which of the below?

a. DDOS protection
b. Non-repudiation
c. Anti-virus protection
d. Availability

Solution: The correct answer is B.

Q: Rodger, a security administrator, is very worried about his system becoming infected with a virus. He decides to implement a multi-layered strategy involving anti virus software on each of his client machines as well an e-mail gateway. What form of attack will this defend against?

a. Scanning attack
b. Social engineering attack
c. ARP spoofing attack
d. Forensic attack

Solution: The correct answer is B.

Q: The use of alert thresholding in an intrusion detection system (IDS) can reduce the repeated alerts. However, it will introduce one of the below vulnerabilities. Which one?

a. The IDS does not distinguish among packets originating from different sources.
b. An attacker, working slowly enough, may be able to evade detection by the IDS.
c. Network packets will be dropped once the volume exceeds the threshold.
d. Thresholding disables the IDS' ability to reassemble fragmented packets.

Solution: The correct answer is A.

Q: Which of the below netcat command switches will you use to telnet a remote host?

a. nc -t
b. nc -z
c. nc -g
d. nc -l -p

Solution: The correct answer is A.

Background:

A free networking utility called Netcat will read and write data across network connections through the TCP/IP protocol.

Netcat will provide outbound and inbound connections for TCP and UDP ports.

- Special tunneling, such as UDP to TCP, where users can specify all network parameters;
- Quality scanning of ports;

- Advanced configurations and options, such as the buffered send-mode (one line every N seconds), and hexdump (to stderr or any specified file) of data (sent or received);
- Optional RFC854 telnet code parser and responder.

Common Netcat switches:

Command	Description
nc -d	Detach Netcat from the console.
nc -l -p [port]	Create a simple listening TCP port. Adding 'u' will put it into UDP mode.
nc -e [program]	Redirect stdin/stdout from a program.
nc -z	Port scanning.
nc -g or nc -G	Specify source routing flags.
nc -t	Telnet negotiation.
nc -w [timeout]	Set a timeout before Netcat automatically quits.
nc -v	Put Netcat into verbose mode.

Q: Ian must analyze the results of an internal vulnerability scan to be run on website hosting servers. The code is written in Java and his team lead wants to it for buffer overflow vulnerabilities using the SAINT scanning tool. Why should Ian discourage his team lead from this avenue?

a. SAINT, as an automated vulnerability assessment tool, is too resource-heavy.
b. Java is not vulnerable to buffer overflow attacks.
c. All vulnerability signatures will need to be manually updated before SAINT will run a scan.
d. The SAINT scanner fails to incorporate the new OWASP Top 10 web application scanning policies and procedures.

Solution: The correct answer is B.

Background: **Because Java uses a sandbox** to isolate code, it is not vulnerable to buffer overflow attacks. Most web and application servers, as well as web application environments are actually susceptible to buffer overflows. However, environments written in interpreted languages such as Java or Python are a notable exception. They are immune to these attacks (except for overflows within an Interpreter).

Q: Scott, a professional Ethical Hacker, has been assigned to do security and vulnerability testing for an organization. In order to find out whether certain computers are connected to the server or not, he will need to ping about 500 computers. Which of the below techniques would save him time and energy?

a. PING
b. NETSTAT
c. Ping sweeping
d. TRACEROUTE

Solution: The correct answer is C.

Breakdown: The **Ping sweeping** technique allows you to ping a batch of devices and get the list of active devices. It is a tedious task to ping every address on the network, the ping sweeping technique is highly recommended.

The **ping** command-line utility tests connectivity with a host on a TCP/IP-based network by sending a series of packets to a destination host.

Q: **How** can an attacker discover what rules have been set up on a specific gateway?

a. Firewalking
b. Firewalling
c. OS Fingerprinting
d. Ping Scan

Solution: The correct answer is A.

Breakdown: The **Firewalking** technique can help a hacker learn which rules have been set up on a gateway. Packets are ordinarily sent to a remote host with the exact TTL of a target. **Hping2** be used for firewalking as well.

Q: What is the process of identifying hosts or services by sending packets into the network perimeter to see which ones get through?

a. Firewalking
b. Enumerating
c. Trace-configuring
d. Banner Grabbing

Solution: The correct answer is A.

Q: Which of the below statements are true about N-tier architecture? (Choose two.)

a. N-tier architecture requires at least one logical layer.
b. Each layer should exchange information only with the layers above and below it.
c. When any layer is modified or updated, the other layers must also be updated so that they agree.
d. Each layer must be able to function on a physically independent system.

Solution: The correct answers are B and D.

Q: Which of the below can be used to determine which range of IP addresses is mapped to live hosts?

a. TRACERT utility
b. Ping sweep
c. PATHPING
d. KisMAC

Solution: The correct answer is B.

Q: You need to find out which protocols a router or firewall blocks as well as which protocols a router or firewall will simply pass onto downstream hosts.

You are going to map out any intermediate routers or hops between a scanning host and your target host. After viewing the results, you need to identify which ports are open. The tool displays "A!" when it determines that the metric host is directly behind the target gateway. Which tool are you using for the scan?

a. Firewalk
b. NMAP
c. HPing
d. Traceroute

Solution: The correct answer is A.

Background: **Hping** is a TCP/IP packet crafter that can be utilized to create IP packets containing TCP, UDP, or ICMP payloads. All header fields can be modified and controlled using the command line. A good understanding of IP and TCP/UDP is mandatory to use and understand the utility, which was actually used to exploit the idle scan technique from another utility by the same developer.

Q: War dialers are used to scan thousands of phone numbers to detect any modems that have vulnerabilities. This provides an attacker with unauthorized access to a target computer. Which of the below utilities would work for war dialing?

Each correct answer represents a complete solution. Choose two.

a. ToneLoc
b. THC-Scan
c. Wingate
d. NetStumbler

Solution: Answers A and B are correct.

Breakdown: Both the **THC-Scan** and **ToneLoc** tools can be used for war dialing.

Q: Which of the below network scanning utilities is a TCP/UDP port scanner that can also operate as a ping sweeper and/or hostname resolver?

a. Netstat
b. SuperScan
c. Hping
d. Nmap

Solution: The correct answer is B.

Breakdown: **SuperScan** is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver as well. Given a range of IP addresses to ping, it will resolve the host name of a remote system.

Q: Which is the correct sequence of packets needed to perform the 3-way handshake method?

a. SYN, SYN/ACK, ACK
b. SYN, ACK, SYN/ACK
c. SYN, ACK, ACK
d. SYN, SYN, ACK

Solution: The correct answer is A.

Background: The **TCP/IP 3-way handshake** method is used by the TCP protocol to establish a connection between a client and the server. It involves three steps:

1. In the first step of the three-way handshake method, a SYN message is sent from a client to the server.

2. In the second step of the three-way handshake method, SYN/ACK is sent from the server to the client.
3. In the third step of the three-way handshake method, ACK (usually called SYN-ACK-ACK) is sent from the client to the server. At this point, both the client and server have received an acknowledgment of the TCP connection.

Q: In which of the below scanning methods do Windows operating systems send only RST packets irrespective of whether the port is open or closed?

a. TCP FIN
b. TCP SYN
c. FTP bounce
d. UDP port

Solution: The correct answer is A.

Background: In the **TCP FIN scanning** method, Windows sends only RST packets whether or not the port is open. TCP FIN scanning is a type of stealth scanning where the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker

---

Q: In which of the below methods does a hacker send SYN packets followed by a RST packet?

a. XMAS scan
b. TCP FIN scan
c. TCP SYN scan
d. IDLE scan

Solution: The correct answer is C.

Breakdown: In a **TCP SYN scan**, an attacker will send SYN packets followed by a RST packet. This is also known as half-open scanning because a full TCP connection is never opened.

Steps of TCP SYN scanning:

1. Send a SYN packet to a target port.
2. If it is open, you will receive a SYN/ACK message.
3. Send an RST packet to break the connection.
4. If an RST packet has been received, it indicates that a port is closed.

Xmas scans: In Xmas Tree scanning, multiple flags (at least FIN, URG and PSH) will be added. If a target port is open, the service running on that target port will discard the packets without

sending a reply. According to specification RFC 793, when a port is closed, a remote system will reply with the RST packet.

Q: **The attacker works through a spoofed IP address to send a** SYN packet to a target. Which of the below methods did he choose?

a. IDLE
b. NULL
c. TCP FIN
d. XMAS

Solution: The correct answer is A.

Breakdown: In the **IDLE scan** method, an attacker delegates sending the SYN packet (to a target) to a spoofed IP address. The IDLE scan is initiated with a third party's IP address and therefore this is the only totally stealth scan technique. This makes it very difficult to detect the hacker, since the IDLE scan uses a different address from the attacker's own.

What is a sequence number?

A sequence number is a 32-bit number ranging from 1 to 4,294,967,295. Data sent over a network is broken into packets at the source and then reassembled at a destination system once it arrives. Each packet includes a sequence number used by the destination system to reassemble the data packets correctly upon arrival. When a system boots, it has an initial sequence number (ISN). As each second passes, the ISN will be incremented by 128,000. When the system connects and establishes a connection with another system, the ISN will be incremented by 64,000.

For example, if a host has an ISN 1,254,332,454 and the host sends one SYN packet, the ISN value will be incremented by 1: Therefore, the new ISN will be 1,254,332,455.

Conditions	Increment in the ISN Value
Transfer of SYN packet	1
Transfer of FIN packet	1
Transfer of ACK packet	0
Transfer of SYN/ACK packet	1
Transfer of FIN/ACK packet	1
Passage of 1 second	128,000
Establishment of one connection	64,000

Q: Which of the below scanning methods is most accurate and reliable, with the downside being that it is also incredibly easy to detect?

a. TCP SYN/ACK

b. TCP FIN
c. TCP half-open
d. Xmas Tree

Solution: The correct answer is A.

Background: Although the TCP SYN/ACK connection method is very reliable, it is easy to discover. A hacker should avoid this scanning method

---

Q: While performing a security assessment of a web server, Erin realizes she needs to identify a cross-site scripting vulnerability. Which of the below suggestions would correct the vulnerability?

a. Inform the Web Administrator that all Web application data inputs must be validated before they are processed.
b. Add a warning to users that cookies can be transferred only via a secure connection.
c. Disable ActiveX support within all Web browsers.
d. Disable Java applet support within all Web browsers.

Solution: The correct answer is A.

Breakdown: Validating data input is the most efficient and secure method of fixing cross-site scripting vulnerabilities because this will address cross-site scripting on ActiveX controls and Java applets downloaded to the client as well as vulnerabilities within server-side code for an application.

Disabling cookies will do nothing to counter cross-site scripting.

XSS vulnerabilities do exist in downloaded Java applets and/or ActiveX controls, but such controls will be executed on the client and do nothing to solve the server-side vulnerability due to cross-site scripting.

Q: Which of the below is not a packet capturing utility?

a. Cain
b. Aero peek
c. Wireshark
d. Aircrack-ng

Solution: The correct answer is D.

Q: An attacker sends **a** FIN packet to a target port. What type of stealth scanning did he likely use?

a. TCP FIN scanning
b. TCP FTP proxy scanning
c. TCP SYN scanning
d. UDP port scanning

Solution: The correct answer is A.

Port scanning is a process of connecting to TCP and UDP ports to discover services and applications active on a target system. Data packets are sent teach port to collect information.

Q: Nick needs to send a file to an FTP server. It will be segmented into several packets, sent to the server, and reassembled upon reaching the destination target (the FTP server). In order to maintain the integrity of the packets, which information will help Nick accomplish his task?

a. Sequence number
b. TTL
c. Checksum
d. Acknowledgement number

Solution: The correct answer is A.

Q: Fred is an Ethical Hacker. His newest assignment is to test the security of his company's website. Once he performs a Teardrop attack on the web server, it crashes. Why did this happen?

a. The server is not capable of handling overlapping data fragments.
b. Ping requests at its server level are too high.
c. The ICMP packet is too large. It cannot be larger than 65,536 bytes.
d. The spoofed TCP SYN packet that contains the target's IP address has been filled in at both source and destination fields.

Solution: The correct answer is A.
Breakdown: In performing a Teardrop attack, Fred sent a series of data packets with overlapping offset field values to the web server. The server was unable to reassemble the packets correctly and is therefore forced to crash, hang, or reboot.

Background: When you receive e-mail with an attachment and execute the file on your machine, you get this message:

'EICAR-STANDARD-ANTIVIRUS-TEST-FILE!'

In Notepad or TextEdit, you see the below string:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Q: Which countermeasure should you take?

a. Run your antivirus program.
b. No action necessary.
c. Search for files that match the name of the attachment and remove them from your drives.
d. Shut down or restart your system and check to see what processes are running.

Solution: The correct answer is B.

The message displayed upon execution indicates that the attachment might be the **EICAR virus**, which checks to see whether an antivirus is effective. The EICAR (EICAR Standard Anti-Virus Test File) virus file tests the response AV programs. It allows you to discover whether your system is protected without causing actual damage to your system.

Q: Which of the below would you use to perform HTTP tunneling?

Answer is complete. Select more than one answer if applicable.

a. HTTPort
b. Tunneled
c. BackStealth
d. Nikto

Solution: The correct answers are A, B, and C.

Breakdown: HTTPort, Tunneled, and BackStealth will perform HTTP tunneling. Nikto is a Web scanner.

Q: A company blocked all ports through an external firewall and will only allow port 80/443 to connect. You want to use FTP to connect to a remote server online. How will you get around the firewall?

Answer is complete. Select more than one answer if applicable.

a. HTTPort
b. BackStealth
c. Nmap
d. BiDiBLAH

Solution: Answers A and B are correct.

HTTP tunneling refers to the technique of using various network protocols to perform communications, which are then encapsulated using the HTTP protocol. The HTTP protocol then acts as the wrapper for a specific covert channel that the tunneled network protocol uses to communicate.

The **HTTPort tool** is used to create a transparent tunnel via proxy server or firewall. This enables the user to operate Internet software from behind the proxy. It will bypass HTTPS and HTTP proxies, transparent accelerators, and even firewalls.

Q: An employee in your company is suspected of downloading ftp of sensitive and proprietary data onto a competitor's remote ftp server. FTP and ports are not allowed by the company's firewall. Which technique might the employee be using?

a. Tor Proxy Chaining software
b. IP spoofing
c. HTTP tunneling

Solution: The correct answer is C.

IP-spoofing is when an attacker masks his source address by forging the header to contain a different address. Then he can make it seem like a packet was sent via another machine. A response will be sent back to a forged/spoofed source address by the target machine.

Tor is a network of virtual tunnels that work like a big chain proxy. The identity of the originating computer is hidden and a random set of intermediary nodes is used to reach a target system.

Q: You configured a rule on a gateway device that blocks external packets with source addresses from inside the network. Which type of attack are you attempting to protect your network against?

a. DOS attack
b. IP spoofing
c. Egress filtering
d. ARP spoofing

Solution: The correct answer is B.

Packet filtering is a defense against IP spoofing attacks. The gateway to a network usually performs ingress filtering, or blocking packets from outside the network that use an internal source address. So attackers cannot spoof the address of an internal machine and trick the network into trusting the connection.

ARP spoofing is also called ARP cache poisoning or ARP poison routing. It is a technique used to attack a local area network, or LAN. ARP spoofing can enable an attacker to intercept data frames on a LAN, modify its traffic, or even stop the traffic. However, the attack can only be used on local networks.

Egress filtering works on outgoing packets, by blocking the packets from inside the network with a source address that is not internal. This prevents an attacker within a network from filtering by launching IP spoofing attacks against external machines.

Background: **Brutus** is a password-cracking tool used to crack the below authentications:

- FTP (File Transfer Protocol)
- HTTP (Basic Authentication)
- HTTP (HTML Form/CGI)
- POP3 (Post Office Protocol v3)
- SMB (Server Message Block)
- Telnet

Q: Which of the below attacks can Brutus perform to crack a password?

Each correct answer represents a complete solution. Choose three.

a. Dictionary attack
b. Brute force attack
c. Replay attack
d. Hybrid attack
e. Man-in-the-middle attack

Solution: The correct answers are A, B, and D.

Breakdown: In a **brute force attack**, the attacker will work through software that attempts a large number of different key combinations to guess passwords. To prevent such attacks, users should create passwords that are complex and therefore more difficult to guess.

Server Message Block (SMB) signing is a security feature of Windows operating systems. SMB signing ensures that the transmission and reception of files across a network are

not altered in any way.

Note: Enabling SMB signing on the network reduces the performance of the network because of the increased processing and network traffic required to digitally sign each SMB packet.

Q: What uses a 160-bit hash to prevent against brute force attacks?

a. PGP
b. MD5
c. SHA-1
d. RSA

Solution: The correct answer is C.

Q: Which of the below attacks uses a pre-calculated hash table, a structure that maps keys to values, to retrieve plain text passwords?

a. Dictionary attack
b. Rainbow attack
c. Hybrid attack
d. Brute Force attack

Solution: The correct answer is B.

Background: A **rainbow attack** uses a hash table, also called a hash map, to retrieve plain text passwords. This kind of attack is one of the fastest methods of password cracking. Through it, the hacker calculates all possible hashes for a set of characters, which are then stored in a table, known as the **Rainbow table**.

Q: A rainbow table is rendered useless with the use of which of the below?

a. Uju beans
b. Pepper
c. Salt
d. Cinnamon

Solution: The correct answer is C.

Q: Bryant is a Network Administrator of a TCP/IP network. There are DNS resolution issues with the network. Which of the following utilities could be used to diagnose the problem?

a. NSLOOKUP
b. PING
c. TRACERT
d. IPCONFIG

Solution: The correct answer is A.

NSLOOKUP is a diagnostic tool for catching and troubleshooting Domain Name System (DNS) issues. NSLOOKUP will send queries to a DNS server and obtain detailed responses at the command prompt. This is useful for verifying that resource records have been added or updated correctly within a zone, as well as debugging other server-related problems.

Q: Which of the below tools could potentially be used for Windows password cracking, Windows enumeration, and/or VoIP session sniffing?

a. Cain
b. L0phtcrack
c. John the Ripper
d. Obiwan

Solution: The correct answer is A.

Cain and Abel is a multipurpose tool that will assist with Windows password cracking, VoIP session sniffing, and Windows enumeration. It is capable of performing the following types of attacks to crack passwords:

- Dictionary attack
- Brute force attack
- Rainbow attack
- Hybrid attack

L0phtcrack will identify and resolve security vulnerabilities that resulted from the use of weak passwords. This tool will recover account passwords of Windows and Unix accounts to access user and administrator accounts.

John the Ripper is a speedy password-cracking tool for most versions of UNIX, Windows, DOS, BeOS, and Open VMS. It also supports Kerberos, AFS, and Windows NT/2000/XP/2003 LM hashes.

Q: An attacker who captures the VoIP traffic on a network can use which of the following tools to recreate a conversation from the captured packets?

a. HPing
b. NMAP
c. Cain and Abel
d. VoIP-killer

Solution: The correct answer is C.

Q: Scott is a professional Ethical Hacker and is responsible for security testing of a company's website. He realizes that UDP port 137 of the company's web server is open. Assuming that the Network Administrator of the company did not modify the default port values of any services, which of the below services will be found to be running on UDP 137?

a. NetBIOS
b. HTTP
c. HTTPS
d. TELNET

Solution: The correct answer is A.

NetBIOS is a Microsoft service that will enable applications on different machines to communicate within a LAN. The default port value of NetBIOS Name Resolution Service is 137/UDP.

Q: In DNS Zone transfer enumeration, an attacker tries to get a copy of the entire zone file for a domain from its DNS server. The information gleaned from the DNS zone can be used to collect usernames, passwords, and other sensitive and valuable information. An attacker must first connect to the authoritative DNS server for the target zone. In addition, the attacker may launch a DoS attack against the zone's DNS servers by flooding them with a high volume of requests. Which of the below tools can this attacker use to perform the DNS zone transfer?

Answer is complete. Select more than one answer if applicable.

a. NSLookup
b. Dig
c. Host
d. DSniff

Solution: The correct answers are A, B, and C.

An attacker can choose Host, Dig, or NSLookup for this DNS zone transfer.

DSniff is a sniffer that can be used to record network traffic.

Q: Scott works as a Security Professional testing the security of a web server. He needs to find information about all network connections and listening ports, listing them in numerical form. Which of the below commands will he use?

a. netstat -an
b. netstat -e
c. netstat -r
d. netstat -s

Solution: The correct answer is A.

According to the scenario, Scott will use the **netstat -an** command to accomplish the task. The netstat -an command is used to get information of all network connections and listening ports in numerical form.

netstat -e will display Ethernet information.

netstat -r will display routing table information.

netstat -s will display per-protocol statistics. The default setting is for statistics to be displayed for TCP, UDP, and IP.

Q: Which of the below options could represent countermeasures against NetBIOS NULL session enumeration on Windows 2000?

Answer is complete. Select more than one answer if applicable.

a. Disable TCP port 139/445
b. Disable all SMB services on individual hosts by unbinding WINS Client TCP/IP from the server's control panel/interface.
c. Edit registry key HKLM\SYSTEM\CurrentControlSet\LSA and input the value RestrictAnonymous.
d. Deny any and all unauthorized inbound connections from connecting to TCP port 53.

Solution: The correct answers are A, B, and C.

NetBIOS NULL session vulnerabilities are difficult to protect against, particularly if NetBIOS is an integral part of the infrastructure. Take the below steps to reduce NetBIOS NULL session vulnerabilities:

1. You can disable access to the TCP 139 or TCP 445 ports, blocking NULL sessions, which require this access.

2. You could also ostensibly disable SMB services completely on individual hosts by unbinding the WINS Client TCP/IP from the server's interface.

3. You can also block/restrict anonymous users by modifying the registry values in the below manner:

   a. Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA.

   b. Choose edit > add value.

      - Value name: RestrictAnonymous
      - Data Type: REG_WORD
      - Value: 2

TCP port 53 is the default port for a DNS zone transfer. Disabling it will restrict DNS zone transfer enumeration, but will not be an effective countermeasure against NetBIOS NULL session enumeration.

Q: You have just installed a Windows 2003 server. What action should you take regarding the default shares?

a. You should disable them.
b. You should disable them only if it is a domain server.
c. Modify the values so that they are hidden shares.
d. Windows Server operations/services require these default shares, so they should be left as-is.

Solution: The correct answer is A.

Unless they are absolutely necessary to system function, **default shares** should be disabled, as they pose a significant security risk. These kinds of shares give intruders the means to hack into your server.

Q: Masquerading (attempting to impersonate a person or another machine), providing false information, or denying the existence of a transaction or event is classified as which of the below forms of attack?

a. A dictionary attack
b. A repudiation attack
c. A DDoS attack
d. A reply attack

Solution: The correct answer is B.

Through a faked digital signature, email spoofing, and/or taking on the IP address of another machine, an attacker performs a **repudiation attack**. The attack may also involve an attempt to give misleading and incorrect information or the denial that a real event or transaction occurred.

For a distributed denial of service (**DDoS**) attack, an attacker would act through multiple computers in the network that were previously infected. These 'distributed' computers will act together to send out fake messages on behalf of the hidden attacker to increasing the volume of phony traffic. In a distributed denial-of-service attack, multiple machines can generate more attack traffic than just one machine and they are more difficult to turn off than one attack machine. In addition, each attack machine can be stealthier, making it harder for network administrators to stop the attack.

In a **replay attack**, attackers will capture packets containing passwords or digital signatures as the packets transmit between two distinct hosts. The attackers will then resend that captured packet to the target system in order to try to force an authenticated connection.

In a **dictionary attack**, a 'dictionary' of common words is used to discover user passwords. It can also use common words in both upper and lower case to discover a password.

Q: **As a network administrator, you** want to secure your company's FTP server so that no non-authorized users can gain access to it. How can you do this?

a. Disable anonymous authentication.
b. Enable anonymous authentication.
c. Stop FTP service on the server.
d. Disable the network adapter on the server.

Solution: The correct answer is A.

Anonymous authentication allows access to an FTP site without a user account and password. So you will need to disable anonymous authentication to prevent unauthorized users from accessing the FTP server. You can do this through the IIS (Internet Information Services) Manager.

Q: Your computer uses the Windows 2000 Server OS. You need to improve the security of the server. Which of the below changes are required to accomplish this?

Answer is complete. Select two answers from the below choices.

a. Remove the Administrator account
b. Enable the Guest account.
c. Rename the Administrator account.
d. Disable the Guest account.

Solution: Answers C and D are correct.

Q: Your Company has developed publicly hosted web apps and uses an internal Intranet protected by firewall. Which of the below techniques would provide some protection against enumeration?

a. Reject all email received via POP3.
b. Remove “A records” for internal hosts.
c. Allow full DNS zone transfers to non-authoritative servers
d. Enable null session pipes

Solution: The correct answer is B.

Q: Scott, an Ethical Hacker, has responsibility to test the security of his company’s website. First, he performs an SNMP scanner, **snmpbulkwalk**, to send SNMP requests to several IP addresses. Though he attempts multiple community strings, he gets no response. Which of the below options could be a cause for this situation?

Answer is complete. Select more than one answer if applicable.

a. The target system is using SNMP version 2, which cannot be scanned by snmpbulkwalk.
b. The target system has halted SNMP services.
c. Scott was searching for the **Public** and **Private** community strings, but the company’s previous team had altered the default names.
d. The target system is unreachable due to low Internet connectivity.

Solution: The correct answers are B, C, and D.

Q: Which of the following techniques will perform a Connection Stream Parameter Pollution (CSPP) attack?

a. Adding a single quote after a URP with no resolving quote.
b. Inserting malicious JavaScript code into the input parameters.

c. Adding several parameters with the same name in HTTP requests.
d. Injecting parameters into the connection string—use semicolons as a separator.

Solution: The correct answer is D.

What is snmpwalk?

Snmpwalk, an SNMP application, pulls SNMP GETNEXT requests to query a network entity for a so-called tree of information. Here is the command syntax for SNMP:

Q: Which of the following statements are true about SNMPv1 and SNMPv3 enumeration?

Answer is complete. Select more than one answer if applicable.

a. Every version of SNMP protocols uses community strings in a clear text format, and is therefore easily recognizable.
b. Simple Network Management Protocol (SNMP) is a TCP/IP standard protocol used to monitor and manage hosts, routers, and other devices within a network.
c. SNMP enumeration involves gathering information about host, routers, devices etc. with the help of SNMP.
d. Implementing Access control list filtering to allow only access to the read-write community from approved stations or subnets can be an effective countermeasure against unauthorized SNMP enumeration.

Solution: Answers B, C, and D are correct.

Breakdown: SNMP version 3 does provide data encryption; however, SNMP version 1 utilizes a clear text protocol—which offers limited security via community strings. Therefore, SNMP v1 is actually used more commonly than v3. By default, the names of the community strings are public and private and will be transmitted in clear text format.

Background: Scott works as a professional Ethical Hacker. His latest project is testing the security of a company. He first wants to execute an SNMP enumeration of the web server to collect information about the hosts, routers, and other devices in the network. Unfortunately, without entering a password for the SNMP service, he cannot perform the SNMP scan. He has a theory that the default names may still be in use. He enters the default password and gets the SNMP service details.

Q: Which of the below are the default passwords for SNMP?

Answer is complete. Select more than one answer if applicable.

a. Administrator
b. Password
c. Public

d. Private

Solution: The correct answers are C and D.

Q: What version of SNMP will not send passwords and messages in clear text format?

a. SNMPv3
b. SNMPv1
c. SNMPv2c
d. SNMPv2

Solution: The correct answer is A.

Q: **The** IP Network Browser will scan a specific IP subnet and displays the devices that are actively responding on that subnet. It will then query the devices that responded through SNMP. Which of the below ports would be used by IP Network Browser to scan devices with SNMP enabled?

a. 22
b. 161
c. 21
d. 80

Solution: The correct answer is B.

Q: Which of the below choices would be effective countermeasures against SNMP enumeration?

Answer is complete. Select more than one answer if applicable.

a. Disabling the SNMP service or simply removing the SNMP agent.
b. Where disabling SNMP is not possible, changing the default PUBLIC community name to something else.
c. Enable the Group Policy security setting, “Additional restrictions for anonymous connections.”
d. Allowing reasonable or even unrestricted access to NULL session pipes and shares.

Solution: The correct answers are A, B, and C.

This is a list of effective countermeasures against SNMP enumeration:

1. Answers A, B, and C above.
2. **Restrict** access to NULL session pipes and shares.

3. Run an upgrade on SNMP Version 1 to the most recent version.
4. Access control list filters that will only allow entry and use of the read-write community from specifically authorized stations and/or subnets.

Q: Because SNMP is not generally audited it can pose a significant threat, particularly if it has not been configured properly. Attackers are likely aware that SNMP can be used for account and device enumeration. SNMP has two passwords to access and adjust the configuration of the SNMP agent from a management station: the read-only community string and the read-write community string. Which of the below tools/utilities would be useful for SNMP enumeration?

a. SNMPEnum
b. SNMP Agent
c. SNMP Util
d. SNMP Manager

Solution: The correct answer is C.

Breakdown: **SNMPUtil** is a command-line tool that gathers Windows user accounts information via SNMP in Windows system. Using this tool you can gather information such as routing tables, ARP tables, IP Addresses, MAC Addresses, TCP/UDP open ports, user accounts and shares.

Q: This web application from Open Web Application Security Project (OWASP) has well-known vulnerabilities (this app was deliberately developed as a way to teach ethical hackers how such vulnerabilities could be exploited).

a. BackTrack
b. WebVuln
c. Hackme.com
d. WebGoat

Solution: The correct answer is D.

General Information: OWASP created another web security application that serves as an excellent testing tool for students and professionals, WebScarab. This app will intercept agent HTTP and HTTPS requests from a user agent and edit them before they are sent to the destination server.

Q: Which of the following best dictates if certain behaviors are allowed on a system or server?

a. Data Loss Prevention Policy

b. Acceptable Use Policy
c. Network Firewall
d. Information Security Policy

Solution: The correct answer is D.

Q: What risk could be posed by having an open port 25 on a server?

a. Unrestricted sharing of printers
b. Active mail relay
c. Clear text authentication could easily be faked.
d. Web portal data leak

Solution: The correct answer is B.

Q: In an asymmetric encryption scheme, any user may create an encrypted message, but only an administrator with a private key can decrypt messages. Which of the below are examples of asymmetric encryption, a scheme in which any user could encrypt messages through a public key? (Choose 2.)

a. PGP (Pretty Good Privacy)
b. 3DES, or Triple DES
c. RSA, an algorithm for public-key cryptology
d. SHA1, or secure hash algorithm (designed by the U.S. National Security Agency)

Solution: The correct answers are A and C.

Q: Arnold is working as a Network Security Professional. His project is testing the security of his company's website. He determines that the company has blocked all ports except port 80. Which of the below attacks could he use to send insecure software protocols?

a. URL obfuscation
b. Banner grabbing
c. HTTP tunneling
d. MAC spoofing

Solution: The correct answer is C.

Breakdown: The organization had blocked all ports outside of port 80. Therefore, Scott can use **HTTP tunneling** to send insecure software protocols.

MAC spoofing is a technique that involves the modification of the assigned Media Access Control (MAC) address of one machine, exchanging it instead with MAC address accepted by the target system.

Using the **URL obfuscation** technique, an attacker can bypass filters or other defenses put in place to block specific IP addresses by altering the format of URLs.

Q: What is the Advanced Encryption Standard (AES) is primarily used for?

a. Key exchange
b. Bulk data encryption
c. Key creation
d. IPSec

Solution: The correct answer is B.

Q: Which of the below password-cracking tools will work within the UNIX or Linux environment?

a. Brutus
b. Cain and Abel
c. John the Ripper
d. Ophcrack

Solution: The correct answer is C.

Breakdown: John the Ripper (JTR) is a password-cracking utility that can be used within UNIX, Linux, and Windows environments. JTR is capable of both dictionary (entering hundreds—or millions of words to attempt decryption) and brute force attacks. Brute force attacks are also known as exhaustive key searches. Both dictionary and brute force attacks are most often mounted when an account lockout policy is not in place—in other words, a security team should simply lock out an account when too many failed password attempts have been made.

Q: Which of the below hacking assaults allow you to bypass an access control list on servers or routers, helping you to mask your presence?

Each correct answer represents a complete solution. Choose two.

a. DNS cache poisoning attack
b. DDoS attack
c. MAC spoofing attack
d. IP spoofing attack

Solution: Answers C and D are correct.

Breakdown Either the IP spoofing attack or the MAC spoofing attack will mask an identity within the network. MAC spoofing is a hacking technique where an assigned Media Access Control (MAC) address is changed to another system's MAC address—in the attempt to be accepted on the system, which may allow the bypassing of access control lists (ACLs) on servers or routers (either masking the presence of a computer on a network, or allowing the system to successfully impersonate an authorized machine).

DNS cache poisoning occurs when non-authoritative information (not from accepted DNS sources) is dumped or placed onto a DNS server, rendering it 'poisoned,' as the information can no longer be proven safe. User clients are then supplied with this non-authentic data, which may or may not be malicious.

Q: Which of the below assertions are accurate with regard to session hijacking?

Answer is complete. Select more than one answer if applicable.

a. It involves the exploiting of a valid computer session, or a session key, to gain unauthorized access to information and/or services in a target system.
b. To accomplish TCP session hijacking, a hacker will take control of a TCP session between two machines.
c. It can be accomplished through IP spoofing and is possible because authentication usually occurs only at the start of a TCP session.
d. It is used to slow down the functioning of network resources within a target system.

Solution: The correct answers are A, B, and C.

Breakdown: **Session hijacking** occurs when a hacker gains unauthorized access to a TCP session when it has already started. It takes control of the session when it is between two machines, utilizing a valid computer session. That session is also referred to as a 'session key.' This process often involves the theft of a so-called magic cookie used to prove the authenticity of a user to a remote server.

Q: How does an operating system protect login passwords?

a. It stores all passwords in a protected segment using non-volatile memory.
b. It encrypts the passwords using an encoder, and decrypts them as necessary.
c. It stores all passwords within a secret file that is hidden from its users.
d. It performs a one-way hash of the passwords.

Solution: The correct answer is D.

Breakdown: A one-way hash is also known as a fingerprint or compression function. Some possible algorithms include MD4, MD5, SHA and SHA256. The one-way hash involves a mathematical function of a variable-length string. It can also be used to create digital signatures and/or file identification.

Q: In which of the below attacks will an attacker use packet sniffing to access and analyze network traffic between two parties, thereby stealing the session cookie?

a. Session sidejacking
b. Session fixation
c. Cross-site scripting
d. ARP spoofing

Solution: The correct answer is A.

Breakdown: In **Session sidejacking**, an attacker will perform packet sniffing to access and analyze network traffic between two parties in an attempt to rip off the session cookie. Many websites use SSL encryption for their login pages to prevent attackers from viewing the password, but for the remainder of the session do not use any encryption. This allows attackers a chance to intercept data submitted to the server post-login, as well as any webpages viewed by the client after they have logged in. Unfortunately, this data includes the session cookie, making it easy for the attacker to impersonate the victim—even when the victim's password has never been revealed.

In **Session fixation**, the attacker exploits a system's vulnerability to fixate or set a target user's session identifier (SID). This method of attack requires a user to adopt the SID, ordinarily through a link sent in an e-mail containing the SID chosen by the attacker. From that point, the hacker can access the site through the SID, posing as the victim.

In **cross-site scripting**, the attacker fools the user's computer into executing malicious code, which is treated as trustworthy since it appears to belong to the server. The attacker can use this opportunity to grab a copy of the cookie or implement other operations.

Q: Which of the below statements is not true about firewalking?

Answer is complete. Select more than one answer if applicable.

a. It can be useful in discovering the types of ports or protocols capable of bypassing a specific firewall.

b. In order to perform firewalking, an attacker must have an address accepted as secure by the firewall as well as one that is not accepted by the firewall.
c. Firewalking works on UDP packets.
d. In this technique, the attacker will transmit a crafted packet with a TTL (time-to-live) value that will expire after one hop past the firewall.

Solution: The correct answer is C.

Breakdown: Fire walking is a way to determine how a packet will move from an untrusted external host to a protected internal host through a firewall. This will allow the attacker to discover which ports are open and whether these packets can pass through the packet-filtering devices of the firewall.

Q: Alice wants to prove her identity to Robert. Robert asks Alice to provide him with her password, which Alice dutifully provides (possibly after some transformation with a hash function); meanwhile, Eve was observing the conversation and records the password. Later, Eve connects to Robert posing as Alice, providing the password read from the previous session. Bob accepts it, unaware that Eve is not Alice. What kind of attack does this describe?

a. Replay
b. Session fixation
c. Cross-site scripting
d. Firewalking

Solution: The correct answer is A.

Q: Which of the below commands can be used to scan ports?

a. nc -z
b. nc -g
c. nc -t
d. nc -w

Solution: The correct answer is A.

The nc -z command will switch the netcat command into port scanning mode. Netcat is a free networking tool that will read and write data via network connections using the TCP/IP protocol.

Q: Scott is a Security Administrator. To access his laptop, he only needs to enter a 4-digit personal identification number (PIN). He also set a token to perform offline checking whether he has input the right PIN. Which of the below attacks is a foreseeable result of Scott's folly?

a. Brute force
b. Replay
c. Smurf
d. Man-in-the-middle

Solution: The correct answer is A.

A **brute force attack** is conceivable and possibly even likely to occur on Scott's laptop. Since his PIN contains merely 4 digits, it is highly vulnerable to a brute force attack.

However, because the token checks the PIN offline, a man-in-the-middle attack is not feasible. **Man-in-the-middle attacks** involve an attacker successfully inserting an intermediary program between two interacting hosts. The intermediary software or program will make it possible for attackers to observe and even alter communication packets as they pass between the hosts. Once the communication packets sent from one host have been intercepted, the altered packet can be sent to the receiving host, so it seems legitimate.

Q: Jacob is his company's security engineer and several employees are requesting that they have remote access to their work machines. What will he use to limit the risks of an MiTM attack?

a. IPSec
b. SSL
c. TLS
d. HTTP over DNS

Solution: The correct answer is A.

Background: Yuri works as a full-time contracted Ethical Hacker. He recently was hired to complete a security check for a website. In his security check, he is able to teal the Security Accounts Manager (SAM) file from the server he was testing. Here is the output:

```
Dick:501:D4DCC2975DC76FB2AAD3B435B51404EE
Bruce:500:5351CF62FC930923AAD3B435B51404EE
Administrator:1002:8AD7EAA34F1A9A31DA5A59A9D0150C17
Alfred:1001:F1402A82F3AB3A2EBA12F405D7E7327B
```

Q: Given the above list, whose account will Yuri attack and break into in order to obtain administrator privileges?

a. Administrator
b. Alfred
c. Bruce
d. Dick

Solution: The correct answer is C.

RID 500 is used for the Administrator account. In the given scenario, the RID code of Mr. Wayne is 500. Therefore, Yuri will break Mr. Wayne's account to obtain administrative privileges.

Q: In attempting to crack the password of Server Message Block (SMB), which of the following tools would prove useful?

Answer is complete. Select more than one answer if applicable.

a. L0phtCrack
b. Pwddump2
c. SMBRelay
d. KrbCrack

Solution: Answers A and C are correct.

L0phtCrack is a Windows password recovery tool that will assist hackers with dictionary, brute force, and hybrid password-cracking attacks. In addition, L0phtCrack is capable of capturing SMB packets on a local network segment as well as capturing the login sessions of separate users.

SMBRelay is an SMB server used to grab usernames and password hashes from inbound SMB traffic.

Pwddump2 will extract password hashes from a Security Accounts Manager file—on Windows systems.

KrbCrack is a Kerberos (a computer authentication protocol which works through tickets) password cracker and sniffer.

Q: Which of the below tools would be useful for achieving connection to a remote computer and then executing a Trojan on it?

a. PsExec

b. Remoxec
c. GetAdmin.exe
d. Hk.exe

Solution: The correct answer is A.

The **PSExec** tool lightweight telnet-replacement utility that will execute a process or processes on remote machines; it allows complete interactivity for console applications. With PsExec, there is no need to manually install software on a remote machine in order to execute remote processes.

Q: In performing a security audit, you discover that the password policy only requires 5 characters with letters and numbers (no special characters). Why might this method be problematic?

a. It isn't; this is a strong password policy.
b. The policy ought to also require special characters.
c. This password policy is too weak for several reasons.
d. The password policy should require a minimum of 6 characters.

Solution: The correct answer is C.

A good password policy would involve a **minimum of 6 characters**, and require **letters and numbers**. However, a good policy would also **sets how often passwords must be changed**, and determine for how long a history should be kept. This is a very weak password policy.

Q: Which of the below are the well-known weaknesses/downsides of LAN Manager hash?

Answer is complete. Select more than one answer if applicable.

a. LM hash will convert any lowercase passwords to uppercase.
b. Hashes in LM hash are transmitted in clear text via the network.
- Passwords longer than 7 characters are split up into 2 sections, with a max of 14 characters.
c. It does not use cryptographic salt.
d. It uses only 16-bit encryption.

Solution: Answers A, B, C, and D are correct.

LAN Manager hash, or LM hash, is the hash technique most often used by Microsoft LAN Manager and Microsoft Windows (at least for versions before to Windows NT) to store user passwords. It is highly vulnerable to a multitude of password-cracking techniques. Although it is

based on sound principles, its weaknesses mean that passwords can be easily cracked through the hash, which

Major security weaknesses within LAN Manager hash include the following:

- LM hash will convert any lowercase passwords to uppercase.
- Hashes in LM hash are transmitted in clear text via the network.
- Passwords longer than 7 characters are split up into 2 sections, with a max of 14 characters.
- It does not use cryptographic salt, which is a standard technique used to protect against dictionary or rainbow attacks.
- Passwords under 8 characters reveal themselves through the hacker, as it will cause the hashing of 7 null bytes.

Q: Because system administrators, in managing use of their network, universally use passwords for access control, password-hacking techniques continue to crop up and advance. Password stealing allows hackers to utilize user credentials and could potentially be the cause of significant data losses from the system. Which of these is NOT a type of password attack?

a. Phishing
b. Shoulder surfing
c. Password hashing
d. Social engineering

Solution: The correct answer is C.

Password hashing is a method of password encryption prior to its storage so that system password databases cannot easily be decrypted. Password hashing is effective in limiting damage, so long as the proper method of hashing is utilized. Other terms that are used in place of password hashing include message digests and data fingerprinting.

The Human Side

Social engineering – when an unknown person manipulates a victim into divulging information or taking the action that the attacker wants. This often involves contrived circumstances, such as fooling a user into believing they are someone familiar. It could also involve ‘tailgating’ behind a person they recognize on the network. Social engineering exploits the ‘human factor,’ where people respond differently to the human element. This may also involve information gathering, whether through ‘dumpster diving,’ or some other method. This is one of the methods hackers use to infiltrate a corporate network, and a large gap in the security of most companies.

Phishing, a social engineering method, is used to swindle users into providing information about themselves and their machines. Phishing relies heavily on the low usability of current security methods to protect against these kinds of attacks. Email spoofing is particularly common in phishing attacks, where an email will request details and information from a user, hooking them by providing a spoofed address of a recognizable and trustworthy website. Often the website is practically a copy of the legitimate website, fooling users into trusting it.

In addition to the above, **shoulder surfing** is another social engineering trick. It uses the direct observation technique. The obvious example is peering over someone's shoulder when they input a password or PIN.

Q: Which of the below methods of information discovery is used by governmental authorities and the police?

a. Spoofing
b. Wiretapping
c. Phishing
d. SMB signing

Solution: The correct answer is B.

Q: Which of the below account authentications are supported by SSH-1 protocol but not SSH-2 protocol?

Answer is complete. Select more than one answer if applicable.

a. Kerberos authentication
b. Rhosts (RSH-style) authentication
c. Password-based authentication
d. TIS authentication

Solution: The correct answers are A, B, and D.

The SSH-2 protocol supports Publickey, (including DSA, RSA, and OpenPGP), Hostbased, and Password-based authentication types.

Note: SSH-1 supports a wider range of account authentication types, including the above and RSA only, RhostsRSA, Rhosts (RSH-style), TIS, and Kerberos authentication types.

Q: What are the disadvantages of the successor to the NTLM (NT LAN Manager) Web authentication scheme?

Answer is complete. Select more than one answer if applicable.

a. It is vulnerable to brute force attacks.
b. It will only work with Microsoft Internet Explorer.
c. Passwords will be sent in clear text format to a Web server.
d. Passwords will be sent in hashed format to a Web server.

Solution: Answers A and B are correct.

The following are the downsides of the NTLM Web Authentication Scheme:

Breakdown: NTLM Web authentication is not entirely safe because NTLM hashes (or challenge/response pairs) can be cracked with the help of brute force password guessing. The "cracking" program would repeatedly try all possible passwords, hashing each and comparing the result to the hash that the malicious user has obtained. Another major downside is that this authentication technique only functions on one browser: Microsoft Internet Explorer, forcing all users to login through IE.

Q: Which of the below statements is accurate regarding Digest Access Authentication scheme?

a. It often uses the base64 encoding encryption scheme.
b. A password will be sent over a network in clear text format.
c. A username and password are required for each request, not only when the user initially logs in.
d. A valid response from the user will include a checksum of the username, the password, the given random value, the HTTP method, and the requested URL.

Solution: The correct answer is D.

The **Digest Authentication** scheme replaces the Basic Authentication scheme. Based on the challenge response model, digest authentication never sends a password in clear text format. Instead, passwords are transmitted as an MD5 digest.

Q: Which of the below Web authentication techniques uses a single sign-on scheme?

a. Basic
b. Digest
c. NTLM
d. Microsoft Passport authentication

Solution: The correct answer is D.

Breakdown: Microsoft Passport authentication uses single sign-on authentication. Users only remember one username and password to be authenticated for the use of multiple services. Microsoft Passport was formerly known as Microsoft Wallet or .NET Password, Microsoft Password, Windows Live ID, and more recently, “Microsoft account.” The service has a history of security vulnerabilities and a trail of patches and fixes that were reported by ethical hackers around the globe.

Q: What is L0phtcrack (LC4) used for?

a. To launch DDoS attacks using cracks in the network.
b. To run lofty port scans for all open services on a target network.
c. It is a Windows password-cracking utility.
d. It is an effective network traffic-sniffing tool,

Solution: The correct answer is C.

Q: Which of the below rules are common to password policies?

Answer is complete. Select more than one answer if applicable.

a. Users must use only words found in a dictionary or including their street address or other personal information.
b. Users must include one or more special characters.
c. Users must include one or more numerical digits.
d. Users must make use of both upper- and lower-case letters (case sensitivity)

Solution: **The correct answers are** B, C, and D.

Breakdown: A password policy is encourages users to use strong passwords and update them properly in order to enhance a web server’s security.

Q: Fred is a professional Ethical Hacker. One of his responsibilities includes security testing the web server of his company. His machine is using Windows Server 2003. If Fred suspects that a friend of his installed the keyghost keylogger onto his machine, which of the following solutions should he execute?

Answer is complete. Select more than one answer if applicable.

a. Use a network monitor, which will alert him when an application attempts to make an unauthorized network connection (to send the data with the typed information).
b. Use on-screen keyboards and speech-to-text conversion software that can also be useful against keyloggers, as no typing or mouse movements are involved.
c. Use commercially available anti-keyloggers such as PrivacyKeyboard.
d. Remove the SNMP agent or disable the SNMP service.

Solution: The correct answers are A, B, and C.

Breakdown: **Network monitors** (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "phoning home" with his or her typed information.

On-Screen Keyboards and other accessibility tools will defeat some keyloggers, but is not an effective solution with all keyloggers, because many of these still send keyboard signals. In addition, screenshots can accomplish the same purpose. It is still recommended, but not by itself.

PrivacyKeyboard, or another anti keylogger, will be an effective countermeasure, as these applications have been built specifically to protect against keylogging software. If run frequently, they can limit the amount of information delivered to a hidden keylogger before it's discovered.

Q: Email tracking comes under which of the below hacking phase(s)?

a. Scanning
b. Maintaining Access
c. Gaining access
d. Reconnaissance

Solution: The correct answer is D.

Q: In which of the below attacks involves an attacker creating IP packets with a faked source IP address with the intent of masking his identity or impersonating another system?

a. Cross-site request forgery
b. Polymorphic shell code attack
c. Rainbow attack
d. IP address spoofing

Solution: The correct answer is D.

Breakdown:

Cross-site request forgery, which is also known as a one-click attack or session riding, occurs when a hacker sends unauthorized commands from a user that a website already trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF works through exploitation of the trust that a website has in a user's web browser. This method often uses social engineering—for example, the hacker will send a link via message or email—and the user will be tricked into opening a link that contains a malicious request. Through this link, the attacker can force the victim to execute a command, such as a funds transfer, information modification, or logout.

Q: Which of the below tools are used for anti-phishing?

a. Netcraft
b. eBlaster
c. Spector
d. Legion

Solution: The correct answer is A.

The **Netcraft** website stores the data of phishing websites and offers a toolbar that analyzes website authentication. Periodically, Netcraft will poll web servers to discover the OS version as well as the server's software version. Netcraft offers anti-fraud/anti-phishing services, application testing, and PCI (Payment Card Industry) scanning. In addition, Netcraft can be used for analysis in the following areas: market share of web servers, operating systems, hosting providers, and Secure Sockets Layer (SSL) authorities.

Q: Aaron's server is Linux-based, and he wants to use a tool to filter packets by MAC address and TCP header flags. One of the below tools will work for this task. Which one?

a. PsExec
b. Chkrootkit
c. PsLogList
d. IPTables

Solution: The correct answer is D.

IPTables is the replacement for the IPChains firewall used by earlier versions of Linux (before the Linux 2.4 kernel and later versions).

Q: Rueben has been given the task of testing security for his employer's website. He first installs a rootkit on the Linux server of the network. Once a rootkit has been installed, what capabilities will an attacker have on a system or network?

Answer is complete. Select more than one answer if applicable.

a. Attackers can secretly execute packet sniffers in order to grab passwords.
b. Attackers can conduct a buffer overflow or overrun.
c. Attackers will be able to input a Trojan in the OS to gain anytime access (also known as backdoor access).
d. Attackers are able to replace utility programs that otherwise might be used to detect their activity on the system.

Solution: The correct answers are A, C, and D.

Breakdown: A **rootkit** is a set of tools or utilities that enable an unauthorized user to take over a system free from detection.

A **packet sniffer** or network analyzer intercepts traffic passing over a network or a part of a network, recording the information (called a packet capture).

A **buffer overflow** or overrun is accomplished when an attacker sends input to a web application that forces the application to input more data in a buffer than it is capable of storing, potentially crashing the application, corrupt data, or allow the execution of the attacker's code. Attackers will often utilize buffer overflows in order to corrupt the execution stack of a web application. They cause the web server to execute code, possibly attempting to take control of the machine.

Background: The EC-Council group has divided Trojans into seven primary types:

1. **Remote Access Trojans**: They allow attackers to gain full control over computer systems. Remote access Trojans are usually set up as client/server programs, so that an attacker can connect to the infected system and control it remotely.
2. **Data Sending Trojans**: They are used to capture and redirect data. eBlaster is an example of this type of Trojan. It can capture keystrokes, passwords, or any other type of information and send them back to the attacker via email.
3. **Destructive Trojans**: They are used to destroy files or operating systems.
4. **DoS Attack Trojans**: They are designed to cause a DoS attack.
5. **Proxy Trojans**: They are designed to work as proxies. These programs can help a hacker hide and perform activities from the victim's computer.
6. **FTP Trojans**: They are specifically designed to work on port 21. These Trojans allow a hacker to upload, download, or move files on the victim's computer.

7. **Security Software Disabler Trojans**: They are designed to attack and kill antivirus or software firewalls. The goal of disabling these programs is to make it easier for the hacker to control the system.

Q: After placing a Trojan file trojan.exe within a text file readme.txt via NTFS streaming, how can the Trojan be extracted from the readme.txt file?

a. c:\> cat trojan.exe
b. c:\> cat readme.txt > trojan.exe
c. c:\> cat trojan.exe > readme.txt > trojan.exe
d. c:\> cat readme.txt:trojan.exe > trojan.exe

Solution: The correct answer is D.

Q: You work as a network security administrator. You suspect that someone has gained access to your machine and used your e-mail account. To uncover potential viruses installed on your computer, you run a full scan. However, you do not find any illegal software. Which of the below security attack types often run in the background on a machine?

a. Rootkit
b. Hybrid
c. Replay
d. Zero-day

Solution: The correct answer is A.

A **zero-day attack** (or zero-hour attack), exploits a vulnerability that currently does not have a fix or solution. Often, the security team is unaware of the vulnerability until “day zero.”

Q: Peter wishes to use the Stenographic file system method for encryption of data and to hide private information. Which of the below are potential storage locations for him?

Each correct answer represents a complete solution. Choose three.

a. Unused sectors
b. Flow space
c. Hidden partition
d. Slack space

Solution: Answers A, C and D are correct.

In the Stenographic file system, files are stored to encrypt data in an efficient, untraceable way. There are 3 methods/places for hiding this data within disk space:

- Unused sectors
- Slack space
- Hidden partition

Q: Alan is resigning from a company for personal reasons and now wants to send out proprietary and secret information about the company. So he edits an image file, using tool image hide and embedding the damaging file within his image, and then sends it to his private email account. The mail server doesn't recognize the file within his image file, and does not filter it. What is his technique called?

a. Web ripping
b. Social engineering
c. Email spoofing
d. Steganography

Solution: The correct answer is D.

Alan utilized the **Steganography** technique to transmit malicious data. Steganography is the art/science of concealing data/information by embedding one harmful message within another seemingly innocuous message.

Q: Which of the below tools can be used to hide secret data within a text file?

a. Image hide
b. Snow.exe
c. SARA
d. Fpipe

Solution: The correct answer is B.

Breakdown: **Snow.exe** is a steganography tool that can be used to embed and mask secret data within simple text files. Since spaces and tabs are usually not visible in text viewers, where the file will likely open, messages can be effectively snuck in without cluing in an unguarded observer.

Watermarking is an irreversible process wherein information is permanently embedded into digital media. While steganography attempts to conceal the existence of the code,

watermarking is primarily about the robustness; does it show up properly after it has been modified. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital form. Unlike metadata, watermarking does not modify the size of the carrier signal. This protection method is considered a passive protection, because it doesn't degrade the data or restrict access.

Q: You have installed a keylogger on Margaret's computer, complete with password protection. In the final step, or the covering tracks step, which of the following actions would you perform before walking away?

Answer is complete. Select more than one answer if applicable.

a. Clear the recent docs from her registry.
b. Clear all caches.
c. Delete the cookies.
d. Disable auditing.
e. Change the user account password for the operating system.

Solution: The correct answers are A, B, C, and D.

Background: Covering Tracks is the final and very important step in remote hacking. All logs should be removed from the target system. When the target system is Linux or UNIX, all entries of the /var folder must be removed. On Windows, it is important to delete all events and logs, an action that keeps the hacker's identity hidden. In addition, security events or error messages logged during the process should be removed to avoid detection. Hackers will therefore either clear those event logs or disable auditing altogether.

Q: A hacker successfully broke into an application, but then failed to cover his tracks in the enterprise systems. The forensics investigator found it quite simple to follow the hacker's actions back to the source. What action could a hacker take to prevent being discovered and/or identified?

Answer is complete. Select more than one answer if applicable.

a. Use Armor Tools.
b. Disable auditing.
c. Run Traceless.
d. Clear the event log.

Solution: The correct answer is B.

Q: In order to determine how a Windows server has been attacked, you check the event logs for traces of the hacker's activity. You look for patterns in the hacker's behavior that might later lead to identifying the responsible party. Luckily, one of the below tools has been used on the system that will capture these events. Which is the correct tool?

a. Auditpol
b. WinZapper
c. Evidence Eliminator
d. ELSave

Solution: The correct answer is A.

Background: Through **Auditpol** a systems administrator can enable or disable system auditing (from the command line). It is also useful in discovering what quality of logging a security team previously implemented. Auditpol is incorporated into the Windows NT Resource Kit.

Q: Ralph needs to demonstrate a type of attack that an ordinary firewall and IDS system would not detect. It should only be able to be discovered through tcpdump, which captures each packet that enters or leaves a server machine. Ralph therefore initiates his TCP connection with a server using port 80. He uses two distinct hosts on two distinct networks; one network acted as server while the other acted as a client. Even with the most current version of Snort, updated to include the latest rule sets, installed and running throughout the demonstration, Snort did not raise an alarm about any attack. Which of the below attack types does Ralph's demonstration explore?

a. Inside-Out Attack
b. White-listing attack
c. Covert channel attack
d. Tor attack

Solution: The correct answer is C.

Breakdown: A **Covert Channel** is a channel utilized for unauthorized and policy-breaking communication that allows information to be moved through a network that goes under the wire of any firewalls or intrusion detection systems. Thus the attacker is able to send information in and out without detection. The technique is effective because it sends information through and via ports that the firewall expects will be trustworthy.

Zero Day Attacks can be prevented with something called "Application Whitelisting," which blocks unauthorized applications from running on a system. The systems administrator keeps a list of acceptable/authorized applications and any other application will not be allowed to initiate/run. Applications are checked against the whitelist when they attempt to load—an added

security step is to include a hashing prevention method. **White listing** is more secure than **black listing**, which is a list kept of all the disallowed applications.

Inside-Out Attacks, otherwise known as firewall piercing, rely on the principle that a firewall cannot and should not try to protect a network against internal users. So the attacker tries to attack from the internal network by establishing a connection from a trusted machine inside a network to an outside, untrusted machine.

Tor (formerly an acronym for "The Onion Router) is an anonymizing "virtual circuit" system with a bit of a dicey history. Although Tor advertises itself as an anonymity tool for "ordinary people who want to follow the law," in reality it is often used for carrying out attacks without giving away your identity—defamation, fraud, and identity theft. The tool gives hacktivists and malicious hackers alike the chance to dodge surveillance and/or traffic analysis on a network. Tor has, however, many weaknesses.

Q: How can a covert channel be utilized (select all that apply)?

a. To transfer files between the hacker's system and a target system, or from the target system to the hacker's machine.
b. To execute/launch applications and processes on the target system.
c. To avail the hacker of an interactive, remote control from the hacker's machine to the target machine.
d. To securely and secretly detect any violations of any corporate firewall rules, and observe any hacking patterns without frightening off the hacker.

Solution: The correct answers are A, B, and C.

Q: After a series of confusing and frustrating attacks, a company decides to hire you to do a security audit of its network. The company is suspicious that the attacks, which seem to have no clear purpose, might be the folly of a malicious insider or a disgruntled employee. Therefore, they direct you to perform security tests that will reveal any inside attacks initiated from within their corporate network. Which of the tests below would prove useful under these circumstances?

Each correct answer represents a complete solution. Choose two.

a. Social Engineering
b. DNS Tunneling
c. Bypass corporate filter firewall rules from inside-out
d. Reverse Engineering

Solution: Answers B and C are correct.

Breakdown: Several utilities have been developed to accomplish **DNS Tunneling**. One example is DNScapy, which was designed to allow security teams to detect holes in their security. These utilities allow hackers to gain access to a website or connect to a hotspot that they otherwise would be prevented from accessing due to HTTP proxies.

As described above, an inside-out attack allows an ethical hacker or malicious hacker to bypass firewall rules by initiating the connection from inside a network.

Background: After checking a log from Snort, you notice the following:

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0xA1D95   Ack: 0x53   Win: 0x400
.
.
.

05/20-17:06:58.685879 192.160.13.4:31337 -> 172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0xA1D95   Ack: 0x53   Win: 0x400
```

Q. Your systems administrator needs to report back to the company with details about the network. What kind of attack has most likely occurred according to the information given in the log above?

a. Back orifice
b. BoBo
c. Netbus
d. SubSeven

Solution: The correct answer is A.

Breakdown: Port 31337, where the packets initiate from, is often the port used by Back Orifice. An attacker uses Back Orifice (BO) to install an inconspicuously sized program on a machine, using another machine to remotely control that server program through a graphical interface. Then communication can flow through TCP or UDP network protocols between the two components.

Netbus is a program used to remotely control (and is often used by hackers to attack) Microsoft Windows systems. Netbus also utilizes two components. Before Back Orifice, Netbus was widely used—now they are often used in conjunction with each other. Some of the capabilities of Netbus include tunneling protocol, keystroke logging and injection, screen captures, launching applications, searching files, forcing shutdown, and tunneling.

SubSeven functions in much the same way as the above-mentioned tools, but has more features than Netbus, including webcam capture and a user-friendly registry editor. However, it cannot log activity. Antivirus programs ordinarily detect it.

Q: Which of the below NETSTAT command parameters would display all active TCP connections as well as the TCP and UDP ports in a listening state?

a. -a
b. -b
c. -e
d. -f

Solution: The correct answer is A.

- -a: Displays all active TCP connections as well as the TCP and UDP ports in a listening state?
- -b: Displays the binary program's process file name associated with every connection and/or listening port. Time-consuming.
- -e: Displays statistics, including packets (sent, received) and more. This can be combined with -s.
- -f: Displays (in Windows Vista or newer versions of Windows only) absolute domain names for non-domestic addresses.

Q: Which of the below NETSTAT command parameters would display an IP routing table?

a. -p
b. -r
c. -s
d. -t

Solution: The correct answer is B.

Background: A Trojan virus has been placed onto your server. It is sending data from your server to the attacker's machine. Then you see the hacker has entered the below command:

nc -l -u -p 22222 < /etc/passwd

Q: What will this command do?

a. It will securely delete the /etc/password from your server.
b. It will download the /etc/password from your server to the attacker's machine.
c. It will load or restore the /etc/passwd file on your server.
d. It will run an update on the /etc/password of your server.

Solution: The correct answer is B.

Q: William is learning about ICMP tunneling and needs to know which of the below statements does not represent a fact about this covert connection technique. Which of the below does not apply to ICMP tunneling?

a. You can use ping requests and replies in order to tunnel complete TCP traffic
b. You can use it to tunnel another protocol via ICMP (Internet Control Message Protocol).
c. You can use it to bypass firewalls because they will not restrict ICMP packets.
d. You can use it to send ICMP packets in an encrypted form over an HTTP port.

Solution: The correct answer is D; all other statements are true.

Q: A hacker wishes to use a netbus Trojan on the Windows program, chess.exe. He will use his program to break into the target machine. Which of the below tools should he choose to do this?

Answer is complete. Select more than one answer if applicable.

a. Beast
b. Tripwire
c. Wrapper
d. Yet Another Binder

Solution: The correct answer is C.

Breakdown: A **wrapper** is a program that is used to combine a harmful executable file with a harmless executable file.

Q: In his Network Security Administrator position, Vernard has the responsibility to observe, secure, and analyze the network of his company. At the moment, Vernard is most concerned to learn that it is possible for others to utilize bypass authentication in order to access his company's network. This gives them more permissions than they were intended to have, and creates a vulnerability that could compromise his company's data, secrets, and client list. What is the name used for this activity, which is often called privilege escalation?

a. Rootkit
b. Boot sector
c. Master Boot Record

d. Backdoor

Solution: The correct answer is D.

A **backdoor** would be blamable for this kind of privilege escalation. A backdoor is a software application, program, or account created or modified to access to the target system by bypassing security checks. Security professionals and vendors skim off time by using backdoors to bypass the security checks during the troubleshooting phases of a project. However, backdoors are also a threat that allows attackers to break in undetected and should be taken seriously to prevent their exploitation.

Q: Which of the below could be signs of a virus attack on a machine?

Each correct answer represents a complete solution. Choose two.

a. Unclear monitor display
b. Corrupted or missing files
c. Sudden reduction in system resources
d. Faster read/write access of the CD-ROM drive

Solution: The correct answers are B and C.

Q: A web server you are working with hits 100,000,000 total visits and immediately crashes. What kind of malicious code may have been used to cause this sudden crash?

a. Polymorphic Virus
b. Worm
c. Virus
d. Logic Bomb

Solution: The correct answer is D.

A type of malware, a **logic bomb** will execute a malicious action or function once a specific condition has been met, such as a specific date/time has been reached. In this situation, the logic bomb lay dormant until the web server hit 100,000,000 total visits. A logic bomb can be set to delete files, shut down a system, or a multitude of other functions.

Worms are standalone applications/programs that copy themselves from system to system, often through networks. They do not require a host file to replicate itself. Even a worm that has no function other than to replicate itself can prove problematic as it causes an uptick in network traffic/consumes bandwidth. There may also be payload/malicious code embedded within the worm.

Background: Troy is the Marketing Manager for a company. Because he often faces with the public, his email account is often subject to various scams and other attacks. Upon arriving to work today, Troy notices an email with the subject “Urgent Security Message.” In the body of the e-mail, it says, “User must remove Boot.ini file due to corrupted data. This file is potentially harmful to user’s operating system.”

Q: Troy is not easily scammed. After puzzling it over, he does a quick online search about the Boot.ini file, which turns out to be a vital system file. In fact, it is what loads the OS! Which attack type was carried out (but ultimately unsuccessful) against Troy?

a. Multipartite
b. Hoax
c. Polymorphic
d. Macro

Solution: The correct answer is B.

Breakdown: **A** virus **hoax** falsely warns an attacker’s victim that a threat is imminent where none is actually present. Troy’s many years of experience have taught him to always research where his expertise runs short.

Q: Which of the below statements is accurate regarding the distinction between computer worms and Trojan horses?

a. Trojan horses are harmful to computers and networks while worms are not.
b. Trojan horses are a form of malicious code, while worms are not (worms lay dormant until other code executes itself to complete a malicious act).
c. Worms replicate themselves while Trojan horses do not.
d. Worms can be sent through emails while Trojan horses can only be installed directly or remotely onto a system through a network.

Solution: The correct answer is C.

Breakdown: A **Trojan horse** is a malicious program code that masks itself as an ordinary and safe program. When a Trojan horse program is running, its hidden code will begin to destroy or scramble information, files, and data on the target hard disk.

Worms, unlike Trojan horses, are able to replicate themselves using computer networks and security holes. Worms may either cause an increase in bandwidth or come with payload, or malicious code that has been attached to a worm.

Q: Where a user lacks permissions to list directory contents, yet can still achieve access to the directory and the contents—so long as he uses the correct path and filename through FTP. What is this kind of FTP access called?

a. Hidden FTP
b. Blind FTP
c. Passive FTP
d. Secure FTP

Solution: The correct answer is B.

Breakdown: **Blind FTP** (also called anonymous FTP) allows users to go directly to a specific directory so long as they use the correct path and file name. One limitation is that these users may not peruse other items without first entering their path and filenames. Blind FTP is considered more secure.

Q: Which of the below tasks would a malicious bot or botnet be capable of performing?

Select the best answer.

a. Launching DDoS attacks
b. Collecting email addresses from within contact forms and/or guestbooks.
c. Downloading an entire website to drain a target's bandwidth
d. Stealing confidential and/or financial information, including credit card account numbers, logins, etc.
e. All of the above.

Solution: The correct answer is E. All of the above answers are accurate.

Breakdown: An Internet robot, or malicious bot, runs different automated tasks, often simple and repetitive—but at a much faster rate than an individual could manually complete. Here are some activities that can be performed by one of these bots:

- Launching DDoS attacks
- Collecting email addresses from within contact forms and/or guestbooks.
- Downloader bots will drain a target's bandwidth by actually downloading the entire website
- Stealing confidential and/or financial information, including credit card account numbers, logins, etc.
- Scraping of websites to steal and plagiarize website content.
- Purchase of tickets in order to resell
- Resource farming on many online games is accomplished via bots.

Q: Eric is always struggling with computer issues. When Eric opens a website, it starts an automatic download containing harmful code onto his machine. What should he do to prevent this from occurring in the future?

Each correct answer represents a complete solution. Choose two.

a. Implement File Integrity Auditing
b. Disable Active Scripting
c. Configure Security Logs
d. Disable ActiveX Controls

Solution: Answers B and D are correct.

Eric could disable certain ActiveX Controls—disallow unauthorized controls and/or active scripts through the web browser. This would enhance, but not completely shield, his computer from browsing sessions.

Q: Veronica is an Ethical Hacker. Her newest assignment is website security testing before the company's website is relaunched. In order to determine how viruses might affect the server, she places one on the system. With no alerts raised by the antiviruses, which were installed and running at the time, the virus infects the system. Which of the below could serve as explanations for this situation?

Answer is complete. Select more than one answer if applicable.

a. Veronica modified the unique hash/signature identifying the virus.
b. Veronica developed a completely new virus.
c. Veronica installed a virus that was not incorporated in the database of the antiviral program that was running on the server.
d. The virus has mutation engine, which has provided further encrypted code in addition to the current code of the virus.

Solution: The correct answers are A, B, C, and D.

Breakdown: A **signature-based anti-virus program** will not be able to detect all computer viruses. Signature-based anti-virus applications search for recognizable patterns of data/information within executable code:

- If the attacker has altered the virus signature, any signature-based antivirus software will be unable to identify and locate the virus.
- If a new virus arrives on the scene and an antivirus database has not been updated to include it, the new virus will not be discovered by the antivirus
- A polymorphic virus mutates itself through encryption and modification, preventing an antivirus from discovering the file/virus.

- Generic signatures can discovery new viruses (or their variants) by detecting recognizable malicious code in files.
- Sandboxing and analyzing file can help an antivirus capture malicious executable code.

Promiscuous mode, which often requires administrative access, is enabled by setting a network card up in such a way that all traffic received by the network will be sent to the CPU (rather than packets specifically coded to be received by the CPU). This is useful for packet sniffing, logging traffic and decoding it for information.

Q: The Internet Protocol Suite includes several dozen distinct protocols all utilized to accomplish different tasks. Which of the below protocols will match an IP address to MAC addresses on a network interface card?

a. ARP
b. RARP
c. PIM
d. DHCP

Solution: The correct answer is A.

Breakdown:

Address Resolution Protocol (ARP) is one protocol of the TCP/IP protocol suite used for maintenance of networks. ARP is used to resolve an IP address to its matching media access control (MAC) address.

Q: An attacker is searching for a GUI utility (for a Windows machine) that will allow him to accomplish Man-in-the-Middle attacks, ARP "poisoning," and sniffing? Which of the below would allow the attacker to launch those attack types?

a. wsniff
b. CAIN
c. Airjack
d. Ettercap

Solution: The correct answer is B.

Breakdown: **ARP Spoofing** works by poisoning the Address Resolution Protocol's cache by sending phony replies from one node—claiming to be another, authorized node—tricking the network into sending data to the attacker when it believes it is sending it to an authorized node within the subnet. This requires the authorized node to have sent a more general request that the attacker can intercept and utilize in creating a false reply.

Q: Evan modifies the MAC address on a sniffer program so that it is the same as an open port on a target's system, fooling the network into routing his machine into the system successfully. What is this called?

a. MAC flooding
b. IP spoofing
c. MAC duplicating
d. ARP spoofing

Solution: The correct answer is C.

Breakdown: In a MAC duplicating attack, the attacker utilizes a MAC address from within the target's network to trick the switch into accepting that there are two ports with the same MAC address. To launch this attack, the attacker will alter the MAC address on his machine to match the MAC address of the target's port. Whereas in ARP spoofing the attacker will poison an ARP cache to confuse the host into allowing the sniffer to enter the network, in a MAC duplicating attack, the data will be forwarded to both the target port as well as the phony port through which the attacker is operating—therefore, no IP forwarding is necessary.

Q: Nate wants to carry out an ARP poisoning attack and needs to know which of the below tools would be useful in launching this type of attack.

Answer is complete. Select more than one answer if applicable.

a. Arpspoof
b. Ettercap
c. Cain and Abel
d. Brutus

Solution: The correct answers are A, B, and C.

Breakdown: **Arpspoof**, which can be utilized by network testers and malicious hackers to launch an ARP poisoning attack, is part of a collection of tools by dsniff. In addition to Arpspoof, Cain and Abel and/or Ettercap can also be used in launching ARP poisoning attacks.

Q: Which of the below types of attack will enable an attacker to sniff data frames within a local area network (LAN) or even to stop network traffic entirely?

a. Session hijacking
b. Port scanning
c. ARP spoofing
d. Man-in-the-middle

Solution: The correct answer is C.

Q: Jared is a security consultant. Many of his fellow employees are being redirected to a different website when they enter the public e-mail site access address into their browser. This alternate website requests that users validate their identity through entering their login information and password. In order to validate this change, Jared uses his iPhone to access the e-mail website. Instead of being directed to the new login/password page, his iPhone browser sends him directly to the original page. What attack has the company likely suffered?

a. DNS zone transfer attack
b. Directory traversal attack
c. DNS cache poisoning
d. Web cache poisoning attack of the email server

Solution: The correct answer is C.

Q: Ralph wants to install a packet sniffer named Windump—which is the functional Windows equivalent of the Linux-based TCPDump—and needs to first create a library. Which of the below options represents the name of the library Ralph must install on his Windows machine?

a. WinTCP
b. WinPCAP
c. idconfig
d. Winconf

Solution: The correct answer is B.

Breakdown: **WinDump** is the Windows equivalent of Linux-based TCPDump. WinDump can be used to view, assess/diagnose, and save network traffic. It is useful for many of the Windows operating systems, including Windows 95, 98, ME, NT, 2000, XP, 2003 and Vista. WinDump requires the WinPcap library and drivers for packet capturing. In addition, WinDump utilizes the 802.11b/g wireless capturing technique (802.11b and 802.11g are the most popular of the amendments to the original 802.11 MAC and physical layer (PHY) specifications for wireless LAN communication) and the CACE Technologies AirPcap adapter, available from Riverbed Technology. AirPcap will capture 802.11 WLAN packets for analysis and is popular due to its integration with Wireshark.

WinPcap, the library utilized by WinDump, is designed to allow link-layer access within Windows environments. Monitoring software (such as WinDump) uses this Windows-equivalent port of the libpcap library for capturing and transmitting packets without going through the computer networking protocol suite (the protocol stack). In addition, WinPcap includes drivers that support kernel-level filtering of packets, an engine for network statistics, and remotely capturing packets. Files saved by WinPcap can be read by a multitude of tools, including Bit-Twist, Firesheep, Kismet, L0phtCrack (Windows XP or later), nmap, Snort, Suricata, WinDump, Wireshark, URL Snooper, and more.

Q: Henry attacks the CAM switches of a network. What kind of attack has he performed?

a. ARP spoofing
b. IP address spoofing
c. DNS cache poisoning
d. MAC flooding

Solution: The correct answer is A.

An attacker performs **MAC flooding** by attacking the CAM (Content Addressable Memory) switches of a network. This technique will compromise the security of a network's CAM table by exploiting the limitations of the CAM Table (which can only hold so many entries). CAM Table Overflows are accomplished by sending an influx of mostly phony MAC addresses into the table until it reaches its threshold. At that point, the switch will cease to bridge its packets to the proper ports, and simply flood all ports with traffic as if it were a hub—this is called 'failopen mode.' It consumes the memory (which is already limited) of the switch.

Q: Two of the statements below are correct. Can you identify which?

a. In a spoofing attack, the valid user may still be active, but the attacker will utilize that user's identity and/or data (the valid user's session is not interrupted).
b. A session hijacking attack occurs when a hacker steals the session key or magic cookie, taking over the session and disconnecting the valid user.
c. A session hijacking attack occurs when a hacker steals the session key or magic cookie, taking over the session *without* disconnecting the valid user.
d. In a spoofing attack, the valid user must not be active so that the attacker may access the IP address or other identifying data, masquerading as the valid user until the valid user's session becomes active again.

Solution: The correct answers are A and C.

Breakdown: **Session hijacking** is very important to security professionals, since HTTP cookies, which are used to maintain most online sessions, can easily be viewed and/or stolen

by a potential hacker through a multitude of attack types.

In a **spoofing attack**, the attacker will initiate a Wi-Fi or GSM—cellular network—and wait for users to connect. At that point, the attacker is able to intercept or modify the user communication, opening up a range of attack opportunities, including phishing.

Q: Which of the below can be used by an attacker to control a malicious bot?

a. IRC channels
b. Websites
c. FTP servers
d. IM tools

Solution: The correct answer is A.

Breakdown: Because **IRC** (Internet Relay Chat) connections ordinarily are not encrypted and remain connected for extended periods, IRC channels have become a very attractive target for crackers.

Q: Against which of the below attacks will the SSH protocol provide protection?

Each correct answer represents a complete solution. Choose two.

a. Broadcast storm
b. DoS attack
c. IP spoofing
d. Password sniffing

Solution: The correct answers C and D.

Secure Shell (SSH) is a protocol that provides solid encryption, authentication, and secure communication capabilities via normally insecure channels. SSH chiefly utilizes automatic public key encryption as for user identification/authentication, but it can also be configured manually. SSH will secure a connection by encrypting user passwords and other important user data, including about the user's machine and/or network. As stated above, SSH will also provide some protection against a variety of attacks, including IP spoofing, packet spoofing, password sniffing, and eavesdropping. The SSH protocol accesses TCP port 22 as its default port and then will operate within the application layer.

Background: In passive packet sniffing, no packet will be generated by the sniffer utility. Packets are simply gathered up by the tool; it acts as a network probe/snoop, analyzing and

capturing the traffic without intercepting or altering it. An active sniffer, on the other hand, will create and send spoofed packets as a means to manipulate switches into treating the false MAC address as if it were genuine. Active sniffers also capture packets. Any sniffing that takes place on a network using switches will by definition fall under the active sniffing category.

Q: Which of the below are the parts of active sniffing?

Answer is complete. Select more than one answer if applicable.

a. ARP spoofing
b. MAC flooding
c. OS fingerprinting
d. MAC duplicating

Solution: The correct answers are A, B, and D.

Breakdown: **OS fingerprinting** is simply used for mapping remote networks and discovering where exploitable vulnerabilities exist on a network—a useful tool for security professionals and hackers. It does not, however, fall under the active sniffing category, as it will not modify any packets. **MAC flooding**, **ARP spoofing**, and **MAC duplicating** are all used in active sniffing techniques.

Q: Andrew needs to view network packets in a continuous-stream display. Which Snort mode will access the network packets and display them in this manner on Andrew's console?

a. Packet logger
b. Output module
c. Sniffer
d. Network intrusion detection

Solution: The correct answer is A.

Q: Jerome is a security professional. His newest assignment is to implement some countermeasures against attacks—in particular, sniffer attacks. If given the below choices, which items would be useful to him?

Answer is complete. Select more than one answer if applicable.

a. Use only encrypted protocols for communications.
b. Use switches rather than hubs/repeaters. Switches will only send information/packets to a specific, correct host predefined by the network.
c. Utilize tools such as StackGuard or Immunix System to prevent attacks.

d. Decrease the network range of the network, thereby avoiding some attack attempts on wireless networks.

Solution: The correct answers are A, B, and D.

Q: Erin is a claims processor for a local insurance company. One morning, she receives an email that has been marked urgent from a client. The client says she has uploaded several pictures of her damaged vehicle and the scene of the accident online and provides a link, purportedly to these photos. Although this is not the usual process for reviewing claims, Erin clicks on the link. The link takes her to an unfamiliar website, and she sees no pictures, so she simply closes her browser and goes back to work on a different claim. Later on, Erin notices that her workstation is running much more sluggishly than it ever has before. In addition, documents are taking far more time to load than usual. Of the below scenarios, which seems the most likely under the circumstances?

a. Erin's system was subjected to a malicious pharming attack.
b. Erin was the victim of a vishing attack (also known as a social engineering attack).
c. Erin was the victim of a phishing attack.
d. Erin's system is running slowly due to an issue with capacity planning.

Solution: The correct answer is C.

Breakdown: Phishing attacks are often carried out through e-mails; the e-mail will appear to originate from a genuine source and will contain language that aims to fool the recipient into clicking on a link. The link will launch a spoofed webpage, which is simply a cover for the attacker to break into the victim's machine.

Scenario: A coworker (who also happens to be a hacker) renamed or moved a file in order to fool his victim into believing the file does not exist. The co-worker pretends to assist the victim, speculating that he can help restore the file to its rightful location intact. The victim, who is eager to get back to work and avoid getting in trouble for the information loss, gratefully accepts. At this point, the co-worker/hacker says that the hacker can only accomplish the task by logging on as the victim—possibly even pointing out that it is against company policy and could get the co-worker/hacker into trouble. The victim will plead for their coworker to do whatever is necessary to restore the file, even if it is against company policy. Appearing to agree begrudgingly, the co-worker/hacker restores the file, and in the process swipes the victim's login and password. This has two affects: first, the hacker bolsters his reputation among his co-workers and therefore can more easily access their machines and information, and second, the hacker may now skip past the regular support channels and go unnoticed as he enters the system with authorized login information.

Q: What is the above attack called?

a. Dumpster diving
b. Piggybacking
c. Tailgating
d. Reverse social engineering

Solution: **The correct answer is B.**

In **tailgating**, an unauthorized individual wearing a phony ID badge will enter into a restricted area by following close behind an authorized individual through an entrance that requires key access. The genuinely authorized individual probably will be unaware that they provided this access, and therefore will not alert security.

Piggybacking, although similar to tailgating, has some key differences. Piggybacking is often accompanied by a backstory or con that tricks the victim into providing the access willingly. It is possible for piggybacking to occur without the knowledge, consent, or intention of the victim—or it can be done with the victim's permission (but without awareness of the hacker's true purpose).

Q: Abby is a dedicated and responsible IT technician. One morning, Abby receives an e-mail from her company's manager asking her to provide her logon ID and password, but Abby is aware that the company policy specifically forbids its users from revealing logon IDs and passwords to anyone. Abby immediately notifies the systems administrator about the email. In his response to her, he agrees with her and congratulates her on avoiding the attack. What is the name of the attack that Abby avoided?

a. Trojan horse
b. Replay attack
c. Social engineering
d. DoS

Solution: The correct answer is C.

Q: In Jeremy's work as an IT Technician, he is responsible for setting up security for his company's entire network. He is specifically attentive to protecting the company's userbase from social engineering attacks. Which of the below approaches are frequently employed by social engineering hackers?

Answer is complete. Select more than one answer if applicable.

a. Trojan horse

b. Personal approaches
c. Telephone
d. Brute force
e. E-mail

Solution: The correct answers are A, B, and E.

Q: Which of the below are examples of passive attacks?

Answer is complete. Select more than one answer if applicable.

a. Dumpster diving
b. Placing a backdoor
c. Shoulder surfing
d. Eavesdropping

Solution: The correct answers are A, C, and D.

Q: Igor is employed as an Ethical Hacker for a successful company. His supervisor assigns him the responsibility of security testing his company's website. Igor's first step is to begin dumpster diving to collect as much information as possible about his company. Which of the below phases of malicious hacking does dumpster diving come under?

a. Gaining access
b. Reconnaissance
c. Maintaining access
d. Scanning

Solution: The correct answer is B.

Breakdown: According to the above description, Igor has gone dumpster diving, which is part of the reconnaissance phase of malicious hacking. Reconnaissance, which is the first phase in hacking, consists of information gathering and analysis.

Q: Ryan works as a programmer. Ordinarily, Ryan utilizes the company's work-from-home setup and only comes into the office on Wednesdays. On one particular Wednesday, after being yelled at by his immediate supervisor for procrastination, he took a little time to jot down the usernames and passwords of coworkers as they entered into the system (he was able to view this information on their computer monitors). Which of the below social engineering attacks did he just perform?

a. Authorization by third party

b. Shoulder surfing
c. Important user posing
d. Dumpster diving

Solution: The correct answer is B.

Shoulder surfing is a type of in-person/personal approach attack in which the attacker collects information while physically present. In performing this attack, the attacker will generally watch the target's keyboard while the target is entering in login/password information at a specific access point. This direct observation technique is very effective in crowded places, where the attacker would go unnoticed amongst the hustle and bustle. IT professionals often have opportunities to shoulder surf.

Q: Which of the below social engineering attacks would involve an attacker damaging a target's machine and/or other device and then be on hand, advertising himself as an expert person who is able to fix the damage and solve any other resulting problem?

a. Important user posing attack
b. In-person/personal approach attack
c. Impersonation attack
d. Reverse social engineering attack

Solution: The correct answer is D.

Breakdown: A **reverse social engineering** attack is carried out in person when an attacker manipulates and cons their target into believing that the attacker is an expert ready to solve a problem that the target already has or will have in the future. The attacker often causes the problem (or plans to cause it) in the first place.

Q: As the Network Administrator for a bank, Tim is worried that his clients are potentially vulnerable to phishing attacks by hackers using phony bank websites. How can Tim protect his clients?

a. MAC
b. Two factor authentication
c. Three factor authentication
d. Mutual authentication

Solution: The correct answer is D.

Breakdown: In **mutual authentication**, both parties must authenticate each other. If either attempt fails, communication will be refused. Mutual authentication works much like ordinary

authentication—but mutual authentication incorporates client authorization through digital signatures. Developers often call mutual authentication “2-way authentication.” If the client cannot be authenticated, the server refuses to communicate with the client—and if the server’s authenticity cannot be verified, the client will not trust the server and will refuse further communication. A successful development of mutual authentication will also provide protection from Man-in-the-Middle Attacks, keyloggers, Trojan horses, and pharming (“phishing minus the lure,” where a machine is infected with malicious code that quietly redirects them to phony websites) and its implementation should also be alongside other methods of security protection.

Q: Which of the below statements are true about a phishing attack?

a. This type of attack will direct a target to input information and passwords into the fields of a website that appears to be genuine.
b. This type of attack involves an attacker transmitting several SYN packets to the victim’s machine or server.
c. This attack type is designed to secretly secure login information from others, including usernames and passwords, as well as information about financial accounts.
d. This attack is carried out via spoofing of e-mail accounts, instant messaging accounts, and social networking accounts.

Solution: The correct answers are A, C, and D.

Breakdown: Phishing attacks are carried out at incredibly high rates with varying degrees of sophistication. At times, these attacks include elements of the other attack types. They rely on the ignorance of users in determining whether a website and/or e-mail has come from a genuine source. This human element is decidedly difficult for security professionals to impact, but through multiple-layer, mutual authentication, antivirus, and other defenses, security professionals may achieve some level of protection for their systems.

Q: An attacker sends an e-mail containing a link to a website with a very similar URL as that of a major banking institution, concealing its malicious nature. The attacker hopes that the recipient will miss some difference in this URL and attempt to log in, providing a password and potentially a pin number or other account detail to the attacker. What technique has this phishing attack employed related to the URL of the website?

a. Dumpster diving
b. URL obfuscation
c. Shoulder surfing
d. Reverse social engineering

Solution: The correct answer is B.

Q: Into which two primary categories can all social engineering attacks be divided?

a. Insider-based attacks and outsider-based attacks
b. Human-based and computer-based attacks
c. Fear-based and persuasion-based attacks
d. Phishing-based and spear-phishing based attacks

Solution: The correct answer is B.

Q: **Social engineers** use their influence and persuasive skills to deceive others into providing them with important and personal/proprietary information. What are the steps utilized by hackers in carrying out social engineering attacks?

a. Choose target, Research target, Develop rapport, Exploit relationship
b. Research target(s), Develop rapport, Select victim(s), Exploit relationship(s)
c. Research target, Select target, Develop rapport, Exploit relationship
d. Select target, Develop rapport, Research target, Exploit relationship

Solution: The correct answer is C.

Q: Social engineering attacks are widespread and potentially quite damaging to a company and its machines. How can a security team protect its systems and users against social engineering attacks?

Answer is complete. Select more than one answer if applicable.

a. Use appropriate firewalls and tools based on best practices.
b. Implement and enforce appropriate security rules, procedures, and policies.
c. Foster an open-minded corporate culture and transparent environment.
d. Put in place appropriate security training for non-IT personnel.

Solution: The correct answer is B.

Enforcement of appropriate security rules and policies around passwords, clear rules about each team member's duties, and accountability will improve security and protect employees from such attacks. Clearly explain to employees that the service desk is the sole point of contact for user issues, including troubleshooting and system analysis. Providing clear examples and relevant training related to social engineering attacks will also be useful.

Q: Ralph, a malicious hacker, transmits an ICMP packet which is more than 65,536 bytes to his target's system. What kind of attack has he carried out?

a. Fraggle
b. Ping of death
c. Teardrop
d. Jolt

Solution: The correct answer is B.

In the **ping of death attack**, the attacker will transmit an ICMP packet greater than 65,536 bytes. Today's operating systems often are built to handle packets of this size and/or are protected by firewalls, which now block ICMP pings.

In a **teardrop attack**, a series of data packets are sent to the target system with overlapping offset field values. As a result, the target system is unable to reassemble these packets and is forced to crash, hang, or reboot.

In a **fraggle DoS attack**, an attacker sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the intended victim.

Q: Maria is an Ethical Hacker. She has been given responsibility for managing a project to test the security of a subsidiary's website. In one of her tests, she attempts to carry out a DoS attack on the subsidiary's web server and discovers that the firewall of the server is blocking ICMP messages, but failing to check UDP packets. In a follow-up test, she sends a large volume of UDP echo request traffic to the IP broadcast addresses of the web server utilizing a spoofed source address that matches the server. What kind of attack is she testing against the server?

a. Ping flood attack
b. Teardrop attack
c. Fraggle DoS attack
d. Smurf DoS attack

Solution: The correct answer is A.

Q: Robin, a professional Ethical Hacker, has been assigned to a project involving security testing of her company's website. She is utilizing the TFN and Trin00 tools to security test the web server for vulnerabilities. What kind of attack can Robin carry out against the web server with those two tools?

a. Brute force attack

b. Cross site scripting attack
c. Reply attack
d. DDoS attack

Solution: The correct answer is D.

Breakdown: In distributed denial of service (DDoS) attacks, an attacker will use several machines throughout a target network that he has already successfully infected. These machines will behave as zombies, working as a team to transmit nonsense messages to cause a large uptick in phony traffic. This type of attack is quite advantageous since multiple machines will generate more attack traffic than a single machine, it is difficult to block/turn off multiple attack machines rather than a single machine, and multiple machines can utilize stealth techniques that make them very difficult to discover and stop. TFN and TRIN00 are two of the tools that are capable of DDoS attacks.

Q: An attacker transmits a spoofed TCP SYN packet utilizing the IP addresses of a target for both the source field and the destination field?

a. Smurf DoS attack
b. Fraggle DoS attack
c. Land attack
d. Jolt DoS attack

Solution: The correct answer is C.

Breakdown: In **a land attack**, the attacker transmits a spoofed TCP SYN packet in which the IP address of the target host is filled in both the source field and the destination field.

Q: In which of the below ways can a security team protect its systems against devastating DDoS attacks?

Answer is complete. Select more than one answer if applicable.

a. Implementation of intrusion detection systems
b. Limit the network bandwidth
c. Utilize network-ingress filtering
d. Block unknown and troublesome IP addresses
e. Implement LM hashes for passwords

Solution: Answers A, B, C, and D are correct.

Useful methods for DDoS attack prevention include the following:

- Router filtering
- Block undesirable IP addresses
- Permit network access only to desirable traffic
- Disable unneeded network services
- Update antivirus software consistently
- Establish and maintain appropriate password policies, particularly for access to privileged accounts (UNIX root or Microsoft Windows NT Administrator)
- Limit network bandwidth
- Network-ingress filtering
- Implement automated network-tracing tools

Background: Barney is an Ethical Hacker. He has been given a new project: security testing for a new website developed by his company. In his initial tests, he discovers that the web server is highly vulnerable to a special type of DoS attack. He then suggests the following steps be taken to protect the web server:

- Disable IP-directed broadcasts at the router level
- Configure all local machines to refuse responses ICMP packets intended to be transmitted to IP broadcast addresses

Q: Which of the below DoS attacks has Scott discovered as a vulnerability for the We-are-secure security network?

a. Jolt attack
b. Smurf attack
c. Teardrop attack
d. Fraggle attack

Solution: The correct answer is B.

Breakdown: According to the countermeasures he suggests, Barney has determined that the web server is likely vulnerable to Smurf DoS attacks. In a **Smurf DoS attack**, the attacker transmits a large volume of ICMP echo request traffic to the IP broadcast addresses utilizing the spoofed source address matching that of the anticipated victim.

Q: Which of the below constitute malicious activities executed by a bot/botnet?

Each correct answer represents a complete solution. Choose three.

a. Malicious downloader programs that download entire websites.
b. Spambots can harvest emails from contact forms or guestbook pages.
c. Honeypot detection.

d. Bots and botnets can operate as viruses or as worms.

Solution: The correct answers are A, B, and D.

A malicious bot is automated software that can be used for various unethical activities. A bot/botnet can be used to perform any or all of the below malicious activities:

- As a spambot, it captures email addresses and information from online guestbooks.
- As a malicious downloader program, it drains bandwidth by downloading whole websites
- As a web scraper, it will harvest webpage content and use it without permission on auto-generated “doorway” pages.
- Hackers can use bots/botnets as viruses or worms.
- DDoS attacks can be performed through this malware.
- Botnets/bots can be directed to modify the names of malware-containing files to mimic user search queries—often carried on peer-to-peer filesharing groups.

A **Botnet** is malware that will permit attackers to control an infected machine. Also called “web robots, Botnets tend to be implemented as part of a network of infected computers .

Q: An investigator tested a hacked network in an attempt to uncover the source of the hacking activity. He soon realized that the administrator account password had been obtained from a local source, despite the server’s anti-virus and anti-spyware software. This tells him the method chosen by the attacker. What is it?

a. Stealth anonymizer
b. Hardware keylogger
c. SNMP community strings
d. SMB signing

Solution: The correct answer is **B.**

Breakdown: Anti-virus or anti-spyware products are unable to detect a hardware keylogger on their own. As previously discussed, it is imperative to take numerous steps to uncover remote keylogging programs. It is best to run an anti-keylogger program with relative frequency to limit the number of hours/days a keylogger will be able to collect and send data.

Q: Because your company’s server is becoming increasingly unresponsive and its listen queue quickly reaching its capacity, you suspect that an attacker has been carrying out SYN flooding attacks on the server. In this attack the table reserved for half open TCP connections This attack works by filling up the table reserved for half open TCP connections in the operating system's TCP IP stack. In a 3-way TCP handshake, what missing process is likely contributing to this attack?

a. SYN-ACK
b. SYN
c. ACK
d. ACK-SYN

Solution: The correct answer is C.

Q: Which of the below constitute methods that could be used to protect against session hijacking?

Answer is complete. Select more than one answer if applicable.

a. Regenerating a session id after the user has successfully logged in.
b. Using a short, straight number or string as the session key.
c. Encrypting any and all data transmitted between the parties, especially the session key.
d. Alter the session cookie's value with each request.

Solution: The correct answers are A, C, and D.

Here are some techniques for protecting against session hijacking:

- The session key should be comprised of a long and random number or string, reducing the risk of an attacker successfully guessing the key and/or discovering it through a brute force attack.
- After each successful login, regenerate the session ID, thereby preventing session fixation an attacker will not know the user's session ID post-login.
- Encrypt all data transmitted between parties–especially the session key. Although this does prevent against sniffing-style attacks, other session hijacking techniques may still be successful. Web-based banks often use this method.
- If necessary, check to ensure that the user's IP address matches the past session's IP address with each request. Individuals with the same IP address will still be able to carry out attacks. In addition, users will often be unhappy with this style of protection, as it is disruptive when switching between IP addresses.
- Modify the session cookie's value upon each request, cutting short an attacker's window to carry out malicious activities. Attacks will be easier to uncover when using this method—but it will cause some disruption of browser functionality (the back button will not work) and other technical issues.

Q: Phil advises his company's development team to utilize a random long number for session keys in order to mitigate security issues. What attack is he attempting to prevent?

a. IP Spoofing
b. Misdirected Trust
c. Brute force
d. Blind Hijacking

Solution: The correct answer is C.

Q: Anna is an employed Ethical Hacker. She is leading her team in the task of security testing their company's website. Anna discovers that the network suffers from a vulnerability to Man in the Middle Attacks, because users are not authenticated within the key exchange process of the cryptographic algorithm. Which of the below cryptographic algorithms is being used?

a. Twofish
b. Diffie-Hellman
c. RSA
d. Blowfish

Solution: The correct answer is B.

Breakdown: **Diffie-Hellman encryption** is a protocol used to resolve key agreement.

Cryptography is used to encrypt and decrypt messages/packets. When text is encrypted, it will be unreadable; once it has been decrypted, it will be readable.

Cryptography terms include the below:

- Plaintext: A user can read this text.
- Ciphertext: This text can be transformed to a non-readable format.
- Encryption: The process of crafting ciphertext from plaintext.
- Decryption: The process of transforming ciphertext to plaintext.
- Cipher: An algorithm that is utilized to encrypt and decrypt text.
- Key: Element of encrypting and decrypting text.

Q: Which sort of attack is the Man in the Middle Attack?

a. Active
b. Passive
c. Active and passive
d. Neither active nor passive.

Solution: The correct answer is A.

Q: Which of the below can be utilized by hackers to accomplish session hijacking?

Answer is complete. Select more than one answer if applicable.

a. Session fixation
b. Session sidejacking
c. Cross-site scripting
d. ARP spoofing

Solution: The correct answers are A, B, and C.

Q: Which of the below attack methods will force a user's session ID to a set value?

a. Max Age attack
b. Zero-day attack
c. FMS attack
d. Session Fixation attack

Solution: The correct answer is D.

Q: In this style of hijacking, the authentication check is executed only when a session is open. A hijacker who effectively launches this attack will be able to control a connection throughout the session's duration. After successfully stealing the session cookie, an attacker can masquerade as a user or hijack a session throughout its lifetime. Which of the below countermeasures would be useful in preventing this type of hijacking?

Each correct answer represents a complete solution. Choose two.

a. Ignore unknown or suspicious links sent through email or instant message.
b. Regenerate the session cookie once a browser session has closed.
c. Decrease the cookie's life span.
d. Regenerate a session ID after a user has logged in.

Solution: The correct answer is C.

Breakdown: Reducing the session of a cookie will improve security, because an expired cookie will cause interruptions in the application's usage.

Q: Heidi is responsible for testing a web application for potential vulnerabilities. She runs a sniffer, attempts to predict the session ID, and then attempts to connect using the details

of an authorized user as if they were her own. What vulnerability is she concerned with based on the information provided above?

a. Cross site scripting
b. Insecure direct object reference
c. Session hijacking
d. SQL injection

Solution: The correct answer is C.

Q: What is another word for Which of the below consists of exploiting insufficient security validation/sanitization of user-supplied input file names?

a. Intuitive Force
b. Hybrid
c. Dictionary
d. Directory traversal

Solution: The correct answer is A.

Directory traversal (or path traversal) involves exploiting inadequate security validation/sanitization of input file names supplied by users, so that characters denoting the command "traverse to parent directory" are passed through to the file APIs. An attacker can simply guess how many levels there are from the user-generated filenames to the parent directory.

Q: Jared's company is utilizing an Apache server that came pre-loaded with default and sample files, plus applications, configuration files, scripts, and webpages. The server is set up to enable content management and remote administrative services; debugging is also enabled. Anonymous users are able to access the administrative functions of this server. What is the issue with this setup?

a. Runs a performance test on the server to check CPU utilization with default files and passwords.
b. Server misconfiguration attacks exist that are specifically aimed to discover and exploit this kind of setup on web and application servers.
c. There's no issue so long as Jared deploys the server within the production application environment.
d. There's no issue; the default features will allow users to leverage the server's features and functions.

Solution: The correct answer is B.

Q: As a senior developer, Rudy is cognizant of security threats and develops web application code that recognizes when a malicious user has made a URI request for a file or directory. Upon such a request, her code will actually build a full path to the file/directory (as long as it exists) and normalize every character (for example, %20 will be converted to spaces). Which of the below is she attempting to prevent?

a. Security misconfiguration
b. Cross site scripting
c. SQL injection
d. Directory traversal attacks

Solution: The correct answer is D.

Background: An attacker wants to discover and capture user account files and passwords. She tries to navigate to the following webpages:

http://target.tgt/../../etc/password

http://target.tgt/../../etc/shadown

Q: What kind of attack is she launching?

a. Rainbow table attack
b. Brute force attack
c. Dictionary-based attack
d. Directory traversal attack

Solution: The correct answer is D.

Q: On reviewing the pages of your online-based store, you discover that some changes have been made that you did not initiate or authorize. What kind of attack may have been launched against your web server?

a. Session hijacking
b. DoS or DDoS
c. DNS cache poisoning
d. Social engineering

Solution: The correct answer is C.

Breakdown: Whether intentional or accidental, **DNS cache poisoning** occurs when data is provided to the caching name server that cannot be traced back to the correct, authoritative

Domain Name System (DNS)

Q: Michael wants to mitigate his web application against a specific vulnerability. He wants to make sure that user-supplied parameters placed into HTTP headers will be vetted for illegal characters, including carriage returns (%0d) and newlines (%0a). Which attack type is Michael attempting to stamp out?

a. SQL injection
b. HTTP response splitting
c. Broken authentication/Session Management
d. Security misconfiguration

Solution: The correct answer is B.

Q: A hacker wants to launch a brute force attack but isn't sure which port he should use. Which of the below is generally the target of such an attack? What can this attack accomplish?

a. Port 25: Emails may be sent from this open port.
b. Port 22: Remote login by guessing passwords/usernames.
c. Port 21: Check for available FTP accounts.
d. Port 80: Send repetitive or numerous TCP handshake attacks.

Solution: The correct answer is B.

Q: In analyzing SSH logs for the security team, Amy realizes that two different attacks are being launched against the network. The attacker attempted to gain access by first utilizing a single user ID and then attempts hundreds of different passwords (password1, password2, password3, etc.). Then the attacker tried several different user IDs (userid1, userid2, userid3, etc.) with different passwords. Several IP addresses were apparent in the SSH. The most common attempts for user IDs included root, admin, administrator, MySQL, Oracle, Nagios. Which of the below attacks have been attempted against their network?

Each correct answer represents a complete solution. Choose two.

a. Bit flipping attack
b. Replay attack
c. Brute force attack
d. Dictionary attack

Solution: The correct answers are C and D.

Q: An attacker inserts an intermediary application between two hosts in the process of communicating with each other. What kind of attack does this represent?

a. Denial of Service
b. Password guessing
c. Dictionary
d. Man-in-the-middle

Solution: The correct answer is D.

Q: A DNS server returns incorrect IP addresses and diverts traffic to the wrong machine. What has occurred?

a. TCP FIN scanning
b. DNS poisoning
c. TCP SYN scanning
d. Snooping

Solution: The correct answer is B.

Q: Cryptographic techniques are utilized by encrypted viruses to prevent detection. Which of the below statements accurately describes encrypted viruses and their characteristics?

Answer is complete. Select more than one answer if applicable.

a. They will shield clients from DNS cache poisoning.
b. They allow DNS servers to transfer records away from the master server.
c. In outward appearance, they are very similar to polymorphic viruses.
d. Each infected machine will have a virus with a distinct signature.

Solution: The correct answers are C and D.

Q: How can security professionals shield clients from the phony DNS data generated in DNS cache poisoning?

a. BINDER
b. Split-horizon DNS

c. Stub resolver
d. Domain Name System Extension (DNSSEC)

Solution: The correct answer is D.

Breakdown: Domain Name System Security Extension (**DNSSEC**) was created to protect clients from phony DNS data (often generated by DNS cache poisoning). By checking the digital signature, a feature required of all answers, a DNS resolver verifies whether information matches, in complete and correct form, the information on the relevant authoritative DNS server.

DNSSEC is a collection of Internet Engineering Task Force (IETF) specifications aimed at securing information provided by a Domain Name System (DNS). It is a collection of extensions to DNS providing origin verification of DNS data, authenticated denial of existence, and data integrity—but not confidentiality or availability.

Q: Which protocol below is used for wireless networks and provides similar security as other protocols provide for wired networks?

a. WTLS
b. WAP
c. WEP
d. WPA2

Solution: The correct answer is D.

The **WPA2** standard is an updated version of WPA and is also known as IEEE 802.11i. WPA2 provides improved protection for wireless networks as compared to the WPA and WEP standards. It is also accessible as WPA2-PSK (for home environments) and WPA2-EAP (for enterprise environments).

The Wireless Transport Layer Security (**WTLS**) is a security layer of WAP designed for securing a wireless environment. WTLS provides privacy, data integrity, and authentication for wireless client-server communications.

Q: Benson sets the value of a watch at $269.00. A hacker modifies the watch's value to $26.99 through an HTML editor. The hacker then submits the slightly modified HTML page, concluding a transaction for the item. What kind of attack did the hacker use to purchase the watch for a fraction of its intended cost?

a. SQL injection
b. Hidden field manipulation
c. Cross site scripting
d. Buffer overflow

Solution: The correct answer is B.

Breakdown: When developers work under tight deadlines, they may take the shortcut of utilizing **hidden fields** to hold information. While it is convenient, sensitive data should not be easily modified, and even though the hidden fields may be outside of the bounds of most users, malicious hackers will quickly discover these fields will exploit their accessibility. Hidden field manipulation attacks will potentially expose important, proprietary business data to the public and open up an online store to significant losses.

Q: An attacker posts a message containing malicious code to a newsgroup site. When other users view his message, their browser interprets the code, executes it, and enables the attacker to control the users' systems. What is this attack called?

a. Code injection attack
b. Buffer-overflow attack
c. Cross-site scripting attack
d. Replay attack

Solution: The correct answer is C.

Breakdown: In a **cross-site scripting attack**, the attacker will input malicious data into an otherwise trusted and safe website. The attacker exploits the web application to transmit malicious code, generally in the form of a browser side script, to other users. Users may be unaware that these scripts are dangerous, and will therefore accept and execute it. This exposes information retained by the browser for the relevant page to the attacker's whim.

Q: William is a Network Security Administrator. Helen, a coworker, approaches William to inform him that a few months ago, Helen filled in an online bank form on her work computer. Today, when she visited the bank's site, she discovered that some of her personal information was still displayed on the web page, in the forms. Which of the below cookies should William disable to solve Helen's issue?

a. Persistent
b. Temporary
c. Session
d. Secure

Solution: The correct answer is A.

Breakdown: Persistent cookies remain on a computer even when once the browser has been closed by a user. Therefore, William should disable persistent cookies so that the browser does not retain data after Helen closes it.

Q: Soon after visiting your bank institution's website, you inadvertently come across a malicious website. Your session on your bank's site may still be valid, and the malicious website transmits a form post to the previous website. Your browser transmits the authentication cookie back to that site and seems to make a request on your behalf without your authorization. What kind of attack are you suffering?

a. CSRF attack
b. Stored cross site scripting attack
c. Reflected cross site scripting attack
d. Dom based cross-site scripting attack

Solution: The correct answer is A.

Breakdown: **CSRF** exploits a website's trust in a user's browser. An attacker inputs script on a malicious site, which will then attempt to access websites already authenticated by the user. This attack abuses the vulnerabilities existing in web applications that base actions on the input of its authenticated users but fails to require users to authorize the actions themselves.

Q: Which of the below is a proxy server used to test the security of web applications?

a. cURL
b. Instant Source
c. BURP
d. BlackWidow

Solution: The correct answer is C.

Breakdown: **Burp Proxy** is a proxy server used by network professionals to test the security of web applications. It functions as a man-in-the-middle between a browser and a target application.

Q: Ron is trying to implement key countermeasures to protect a web application against the most common attacks carried out on web applications. Which of the below represents a basic code check that will protect against the entries of malicious users?

a. ESAPI locators
b. Security Misconfiguration
c. Randomizers
d. Input validation

Solution: The correct answer is D.

Breakdown: Malicious users might enter scripts in places where data or numerical variables are expected. A web application should offer **input validation** to sanitize, encode, or replace improper user inputs.

Q: Maria is an application security architect responsible for mitigating common website vulnerabilities, including cross-site scripting and SQL injection. First, she makes sure that the developers understand and follow coding practices. Second, Maria works with the network team to train them on deploying IDS/IPS utilities. Third, she implements personal firewalls and anti-virus systems throughout. What else should Maria set up to in her quest to counter common web application attacks?

a. Honeypot
b. Web application firewalls
c. VPN
d. RBAC

Solution: The correct answer is B.

A **web application firewall (WAF)**, which is an appliance, server plugin, or filter, employs a group of rules in HTTP conversations. The rules usually relate to common attacks, including cross-site scripting (XSS) and SQL injection.

A **honeypot** is a trap implemented by security professionals aimed at attracting attackers in order to counteract unauthorized use of genuine information systems. A honeypot will ordinarily include data, computers, or network sites that seem to be a part of the larger network, but in reality are monitored closely by the security team and isolated from the rest of the network to mitigate potential damage. This so-called honeypot attracts potential attackers with its low security permissions and other vulnerabilities.

Background: Lloyd is employed as an Ethical Hacker. He has been assigned a major project for security testing his company's website. When Lloyd inputs a single quote within the login page of the website, it returns the following error message:

Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'

Q: From this message, Lloyd is able to tell that the website is vulnerable to which of the below attacks?

a. A buffer overflow
b. An XSS attack

c. A Denial-of-Service attack
d. A SQL injection attack

Solution: The correct answer is D.

Background: Bob works as a Network Penetration tester. His workgroup has multiple projects for security testing the websites of several companies. Working with one of these company websites, Bob visits to the login page of the website and runs the below SQL query:

```
1. SELECT email, passwd, login_id, full_nameFROM membersWHERE email
   ='attacker@somehwere.com'; DROP TABLE members;--'
```

Q: What task will Bob's SQL query complete?

a. It will delete the members table in its entirety.
b. It will deletes rows of members table when email id is given as 'attacker@somehwere.com'
c. It will delete all databases storing this members table.
d. It will launch XSS attacks.

Solution: The correct answer is A.

Q: Which of the below characters can a tester input to discover if their application is vulnerable to SQL injection attacks?

a. Semi colon (;)
b. Single quote (')
c. Double quote (")
d. Dash (-)

Solution: The correct answer is B.

A **single quote (')** can be used to analyze potential SQL injection attacks (where an attacker attempts to launch unauthorized SQL statements).

Q: You work for a financial company. Your security department is requiring developers to shield their applications from SQL injections. Client supplied data must never be able to alter the syntax of any SQL statements. All application-required SQL statements need to be maintained within stored procedures on a database server. However, your company is concerned about the uptick in attack frequency and wants to know whether further defensive security scanning tools would be appropriate. You reply in the affirmative, and suggest one of the below tools. What would you recommend?

a. sqlninja
b. SQLIer
c. Acunetix
d. sqlmap

Solution: The correct answer is C.

Acunetix Web Vulnerability Scanner automatically monitors web applications for SQL Injections, XSS (cross-site scripting attacks), and other common vulnerabilities.

Q: The Voyager worm was posted on the Internet on October 31, 2005, and is intended to target Oracle databases. If successful, this worm will grant DBA to PUBLIC. What technique does the Voyager worm use to attack Oracle servers?

a. SQL Injection
b. Buffer Overflow
c. Code Injection attack
d. Utilization of default accounts and passwords

Solution: The correct answer is D.

Q: Each network device utilizes a distinct pre-configured Media Access Control (MAC) address. This is used to recognize the authentic device and limit access to the network. Which of the below addresses is an acceptable MAC address?

a. 132.298.1.23
b. F936.28A1.5BCD.DEFA
c. 1011-0011-1010-1110-1100-0001
d. A3-07-B9-E3-BC-F9

Solution: The correct answer is D.

The universal format for writing MAC addresses is 6 groups of 2 hexadecimal digits, dividing each with a hyphen.

Q: Which of the below wireless security features will provide the most effective security mechanism?

a. WAP
b. WEP
c. WPA with 802.1X authentication
d. WPA with Pre Shared Key

Solution: The correct answer is C.

WPA with 802.1X authentication offers the most effective mechanism for wireless security. 802.1X authentication, which is also called WPA-Enterprise, is a mechanism for securing wireless networks. 802.1X offers port-based authentication, involving communications between a supplicant, an authenticator, and an authentication server.

The initialization vector (IV) is a block of bits that that enables the execution of a stream cipher or a block cipher within any of several streaming operational methods. This produce a unique stream separate from other streams but produced through the same encryption key without the need for a re-keying process. The IV size is dependent on an encryption algorithm as well as the cryptographic protocol; it is ordinarily as large as the block size of the cipher, or as the encryption key size. The receiver of encrypted information must have the IV in order to decrypt the information.

Q: Drew is a network administrator. He has implemented a dual firewall Demilitarized Zone (DMZ) to isolate the rest of his company's network from other portions that are accessible to the public via the Internet. Which of the below security threats would be possible if an attacker launched successful DMZ protocol attacks?

Each correct answer represents a complete solution. Choose three.

a. The attacker (if he bypassed the first firewall defense) will have access to the company's internal network without breaking a second unique firewall.
b. The attacker would gain entrance onto the web server in the DMZ and could exploit the database.
c. The attacker would be able to exploit protocols to access the company's internal network or intranet.
d. The attacker would be able to launch a Zero Day attack, which would entail transmitting a malicious payload outside of the IDS/prevention systems protecting the network.

Solution: The correct answers are B, C, and D.

Q: Which of the below statements is not accurate regarding SSIDs?

Each correct answer represents a complete solution. Choose three.

a. SSIDs help identify a wireless network.
b. SSIDs utilize case in-sensitive text and numerical strings with a maximum length of 64 characters.

c. Each wireless device within a wireless network is required to use the same SSID in order to communicate with other devices in the network.
d. Setting an SSID to match Wireless Access Points (WAPs) of other networks creates a conflict.

Solution: The correct answer is B, which is false.

Background: Service Set Identifiers (**SSIDs**) are used to identify wireless networks. They are case sensitive text strings with a max length of 32 characters.

Q: Which of the below is a major benefit that a network-based IDS/IPS system will offer as compared to host-based solutions?

a. A network-based IDS/IPS is placed at the boundary between internal and external network sources.
b. A network-based IDS/IPS is easier to install and configure.
c. A network-based IDS/IPS will slow down user interfaces.
d. A network-based IDS/IPS does not use resources from the host system.

Solution: The correct answer is D.

Q: Which security strategy will require multiple and varied techniques to maintain the security of systems against attackers?

a. Overt channels
b. Three-way handshake
c. Data Loss Prevention
d. Defense in depth

Solution: The correct answer is D.

Q: Which of the below options are accurate regarding WPA?

Answer is complete. Select more than one answer if applicable.

a. WPA provides improved security over WEP.
b. WPA-PSK requires that users enter an 8- to 63-character passphrase into the wireless client.
c. WPA-PSK transforms that passphrase into a 256-bit key.
d. Shared-key WPA is highly vulnerable to password cracking attacks when feeble passphrases are chosen.

Solution: A, B, C, and D are the correct answers—all of the above.

Background: Wi-Fi Protected Access, or **WPA**, is a security standard for wireless networks. This standard provides improved security over WEP (Wired Equivalent Protection). Windows Vista will support both the WPA-PSK and WPA-EAP standards.

Q: Karen, a network security professional, is worried that an attacker discovering the wireless network of her company by passing by its office. She is concerned that attackers will be able to access the network via their wireless connection. Which of the below will not aid her in securing this wireless connection?

Each correct answer represents a complete solution. Choose two.

a. Use WEP or WPA encryption.
b. Do not broadcast the SSID.
c. Hardening the server's OS.
d. Use MAC filtering on the router.
e. Enforce strict password policies on workstations.

Solution: Answers C and E are correct.

While hardening the server's OS and enforcing strict password policies on workstations are useful, neither will affect the security of a wireless connection.

Q: One of your company's web developers wants to allow contractors working on various projects to access the Internet over a wireless connection. Because the approval process is so lengthy, the developer sets up his own wireless router, attaches it to a network port, and sets up a WAP for these contractors. Which of the below statements describes the risk this might pose to your company's systems?

a. Adding a WAP is commonplace and poses no security risks.
b. This WAP will cause traffic on the network to surge and will cause sluggishness in the overall performance of the network.
c. Hackers often use unauthorized WAPs to enter a network.
d. This router breaks protocol and evades the network's intrusion detection.

Solution: The correct answer is C.

Wireless Access Point (WAP) devices are capable of sending and receiving signals over a wireless LAN. These devices are connected to a server or possibly directly to a network or other device through standard cabled network protocols.

Q: How can a security team detect rogue WAPs and block them from entering its network?

a. Network anti-spyware software
b. Network anti-virus software
c. Site surveys
d. Protocol analyzers

Solution: The correct answer is C.

Q: Bryant has discovered what seems to be an unauthorized wireless access point on his company's network. At first, he is confused by this WAP, as its MAC address is identical to another genuine WAP, but the unauthorized WAP is broadcasting a much greater signal. What kind of attack is this?

a. DoS attack
b. WAP cloning attack
c. Bluesnarfing attack
d. The evil twin attack

Solution: The correct answer is D.

Breakdown: In the **evil twin attack**, an attacker sets up a rogue WAP with an identical MAC address as a genuine access point. This rogue WAP often then will launch a DoS attack on the genuine access point to render it unresponsive—which will cause users to be directed to the 'evil twin' WAP.

Q: Phil is worried that a hacker might use wardriving to discover his company's wireless network. What basic thing can he do that will help to mitigate the risk?

a. Do not broadcast the network's SSID.
b. Set up and configure WEP.
c. Set up and configure MAC filtering.
d. Set up and configure WPA.

Solution: The correct answer is A.

Q: Which of the below statements are accurate regarding using WLAN discovery software (NetStumbler, Kismet, or MacStumbler) to discover rogue access points when using a laptop that has an integrated, Wi-Fi compliant MiniPCI card?

Answer is complete. Select more than one answer if applicable.

a. These tools will not detect rogue access points when the victim is using data encryption.
b. These tools can discover rogue access points as long as the victim is using IEEE 802.11 frequency bands.
c. These tools can determine the rogue access point even when it is attached to a wired network.
d. These tools can determine the authorization status of an access point.

Solution: The correct answers are B and D.

Q: Which of the below tools will monitor the radio spectrum to discover rogue access points and utilization of wireless attack tools?

a. IDS
b. Snort
c. WIPS
d. Firewall

Solution: The correct answer is C.

Breakdown: **Wireless intrusion prevention system (WIPS)** will monitor the radio spectrum to discover any unauthorized, rogue access points and whether any wireless attack tools have been used. It monitors the radio spectrum used by wireless LANs, and will alert a systems administrator whenever it discovers a rogue access point.

Q: You are the administrator for a workgroup that has 143 Windows XP Professional client machines and 42 Windows 2003 Server machines. You need to install and implement a security layer of WAP designed for your company's wireless environment—this layer must provide privacy, data integrity, and authentication for client-server communications. Additionally, both the client and the server should be authenticated in order to maintain a secure, encrypted connection during transactions. Which of the below should you use to complete this task?

a. Recovery Console (RC)
b. Wired Equivalent Privacy (WEP)
c. Virtual Private Network (VPN)
d. Wireless Transport Layer Security (WTLS)

Solution: The correct answer is D.

Wireless Transport Layer Security (WTLS) is a security layer of WAP for wireless environments that offers privacy, data integrity, and authentication for client-server communications.

Q: Cate needs to set up an ad hoc wireless network over which she can transmit important files to a coworker. Which of the below protocols for wireless security should she pick for creating her ad hoc wireless network?

Each correct answer represents a complete solution. Choose two.

a. WPA-PSK
b. WPA-EAP
c. WEP
d. WPA2 -EAP

Solution: The correct answers are A and C.

Q: An executive in Mallory's company has complaints about odd behavior on her PDA. After investigation, Mallory determines that a trusted device is copying data off of the executive's PDA. The executive admits that the strange behavior began shortly after she accepted an e-business card from an unknown individual. What kind of attack does this represent?

a. Bluesnarfing
b. PDA hijacking
c. Session hijacking
d. Privilege escalation

Solution: The correct answer is A.

Bluesnarfing is a relatively rare attack where an attacker gains control of a device with Bluetooth-enabled. One method is to convince a PDA user to accept your device as a trusted device, as in the situation described above.

Q: A salesperson in Gary's company is concerned that he is frequently receiving unsolicited messages on his PDA. Gary determines that the issue occurs when the salesperson is in a crowded area—like an airport, and identifies the problem as one of the below attacks. Which is it?

a. Bluesnarfing
b. Bluejacking
c. Virus and Malware

d. Spam or Phishing

Solution: The correct answer is B.

Bluejacking is a method of using a Bluetooth device within range of the target to send the target device unsolicited messages.

Q: Gordon is a project engineer for a company that uses Windows XP machines. Gordon's computer does not use the default gateway; he is able to connect to the Internet, but cannot use e-mail unless he uses the company's intranet. Which of the below is potentially the reason for this situation?

a. Protocols other than TCP/IP are being used.
b. An IP packet filter is installed.
c. The router is blocking Gordon's machine.
d. Gordon may be using a proxy server.

Solution: The correct answer is D.

Breakdown: A proxy server operates between the client's browser and a genuine Internet server.

Q: When no genuine anomaly has occurred, but an alarm is generated in an Intrusion Detection System, the alarm is called which of the following?

a. False positive
b. False negative
c. True positive
d. True negative

Solution: The correct answer is A.

Breakdown: The following are the types of responses generated by IDS:

1. **True Positive**: Valid anomaly detected; alarm generated.
2. **True Negative**: No anomaly present; no alarm generated.
3. **False Positive**: No anomaly present; but alarm generated. When any IDS generates false positive responses at a high rate, the IDS will be ignored and fall out of use.
4. **False Negative**: Valid anomaly present; no alarm generated.

Background: Host-based IDS (HIDS) is an Intrusion Detection System that monitors only data that it is directed to, or data that originated on the system where HIDS is installed. In addition to monitoring a network's traffic to detect attacks, HIDS is also capable of monitoring other system parameters of the system (processes, file system access and integrity, and user logins). These records help in discovering and identifying malicious activity.

Q: Which of the below utilities are examples of HIDS?

Answer is complete. Select more than one answer if applicable.

a. HPing
b. Legion
c. Tripwire
d. BlackIce Defender

Solution: Answers C and D are correct.

Tripwire and BlackIce Defender are both examples of HIDS. Tripwire, an HIDS tool, will automatically calculate cryptographic hashes of all system files as well as any other file that a Network Administrator wishes to monitor for changes. Tripwire will periodically scan all monitored files and recalculate information to discover whether or not files have been modified.

Q: In your position as a Network Administrator, you implemented a network-based IDS and installed sensors at all key positions within the network. Each reports the command console. Which of the below will be key tasks of these sensors in this physical plan?

Answer is complete. Select more than one answer if applicable.

a. To analyze for known signatures.
b. To gather data from operating system logs.
c. To gather data from web servers.
d. To alert the console if any intrusions are detected.

Solution: Answers A and D are correct.

Breakdown: In such a network-based IDS, the sensors installed at key positions will function as full detection engines. These sensors will be able to sniff packets, analyze them for known signatures, and alert the console immediately upon discovering an intrusion.

Q: Adam is the Network Administrator for his company, which has a TCP/IP-based routed network. Adam recently learned about the Slammer worm, which attacked computers in 2003 and doubled the number of infected hosts every ~9 seconds. The Slammer worm

was able to infect 75,000 hosts in its first 10 minutes. Which of the below tools will you install and configure to prevent such attacks?

a. Anti-x
b. Firewall
c. Intrusion Detection Systems
d. Intrusion Prevention Systems

Solution: The correct answer is D.

An **Intrusion Prevention System (IPS)** is a tool that aims to prevent large-scale attacks on a network. This tool will detect sophisticated attacks by keeping an eye on the trends and searching for attacks that employ specific message patterns.

Q: Andrew is a Network Security Administrator and is working on the installation of a MySQL server. He wants to monitor only data that comes from or is sent to the server, as well as running processes, file system access and integrity, and user logins for detecting malicious activities. Which of the below intrusion detection methods can Andrew implement to complete his project?

a. Host-based
b. Network-based
c. Anomaly-based
d. Signature-based

Solution: The correct answer is A.

A host-based IDS (HIDS) is an IDS that runs within the monitored system. HIDS monitors only data sent to or received by the system on which HIDS was installed. It will accomplish precisely what Andrew was seeking in an IDS.

Q: Amanda is a Security Analyst for a company. She is gathering a large quantity of log data from multiple resources such as Apache log files, IIS logs, streaming servers, and FTP servers. In order to analyze these logs, Amanda decides to employ the AWStats application. Which of the below statements are true of AWStats?

Answer is complete. Select more than one answer if applicable.

a. It generates web, streaming, or mail server statistics graphically.
b. It functions solely as a CGI and shows information contained in a log.
c. It can analyze log files of server tools including Apache log files, WebStar, IIS and other web, proxy, and even some ftp servers.
d. It can work with all Web hosting providers, which allow Perl, CGI, and log access.

Solution: The correct answers are A, C, and D.

AWStats is a powerful (free) utility that can be used to generate web, streaming, and mail server statistics graphically. It works as a CGI **or** can be used from the command line. AWStats shows all possible information contained in a log, can analyze log files from almost all server tools such (Apache log files, WebStar, IIS (W3C log format) and various other Web, proxy, WAP, streaming servers, mail servers and some ftp servers). It is compatible with all web-hosting providers, which allow Perl, CGI and log access.

Reference: EC-Council Certified Security Analyst Course Manual, Contents: "Log Analysis"

Q: You are the Network Administrator for a company. Employees located in remote places connect to your company's network using the Remote Access Service (RAS). Which of the below could you use to pass or block packets from set IP addresses and ports?

a. Gateway
b. Antivirus software
c. Bridge
d. Firewall

Solution: The correct answer is D.

A **firewall** is used to protect internal networks or intranets against unauthorized access from the Internet or other outside networks. A firewall will restrict inbound and outbound access and is capable of analyzing traffic sent between an internal network and the Internet. Users can set up a firewall to either pass or block packets from specific IP addresses and ports.

Q: **Which of the below statements regarding packet filtering is correct?**

a. It is used to transmit confidential data over a public network.
b. It enables or blocks the flow of encrypted packets to provide security
c. It enables or blocks the flow of specific packets to provide security.
d. It is used to store information regarding confidential data.

Solution: The correct answer is C.

Packet filtering is a technique that enables or blocks the flow of specific types of packets to provide security. Packet filtering performs an analysis of incoming ad outgoing packets, allows them to pass, or stops them at a network interface based on source and destination addresses, ports, and/or protocols.

Q: Which areas of a network include DNS and web servers for Internet users?

a. VLAN
b. VPN
c. MMZ
d. DMZ

Solution: The correct answer is D.

The **DMZ** is the IP network segment containing the resources needed for Internet users including servers for the web, FTP, e-mail, and DNS. DMZ offers a large enterprise network (or a corporate network) the ability to use the Internet while maintaining security.

Q: Which of the below methods of cryptography does the NTFS Encrypting File System (EFS) utilize for the file-by-file encryption of data stored on a disk?

Answer is complete. Select more than one answer if applicable.

a. Digital certificates
b. RSA
c. Twofish
d. Public-key

Solution: Answers A and D are correct.

Breakdown: The **EFS** employs public-key cryptography as well as digital certificates in encrypting data stored on a disk. It does this on a file-by-file basis.

Q: What command is used to generate a binary log file through tcpdump?

a. tcpdump -w
b. tcpdump -B
c. tcpdump -d
d. tcpdump -dd

Solution: The correct answer is A.

Breakdown: **tcpdump** refers to a popular packet sniffer, which runs through the command line.

Q: Which of the below protocols is used for properly functioning Internet Relay Chat (IRC) sessions?

a. SMTP
b. IMAP
c. TCP
d. ICMP

Solution: The correct answer is C.

Q: Ned is a Network Administrator. Ned notices that the wireless AP sends 128 bytes of plaintext, and a station responds by encrypting it. The station then transmits the encrypted ciphertext using an identical key and cipher to that utilized by WEP to encrypt future network traffic. What kind of authentication mechanism is being used?

a. Open system authentication
b. Pre-shared key authentication
c. Single key authentication
d. Shared key authentication

Solution: The correct answer is D.

Background: Roger is an Ethical Hacker with the task of security testing www.rogr-forgenet.com. He initiates a port scan, which displays the below result:

Scan directed at open port:ClientServer192.168.1.90:4079 -----FIN/URG/PSH----->192.168.1.120:23rogr-forgenet.com192.168.1.90:4079 <----NO RESPONSE------192.168.1.120:23
Scan directed at the closed port:ClientServer192.168.1.90:4079 -----FIN/URG/PSH----->192.168.1.120:23192.168.1.90:4079<-----RST/ACK----------192.168.1.120:23

Q: Which type of scan has Roger initiated?

a. XMAS scan
b. RPC scan
c. IDLE scan
d. SYN scan

Solution: The correct answer is A.

Q: James is a sales manager for a company. He needs to download software from the Internet. However, the software he wants originates from a site outside of his trusted zone. To be sure that the downloaded software has not been Trojaned, he takes one of the below actions. Which action would make the most sense?

a. James will compare the downloadable version with the one published on the distribution media.
b. James will compare the file's MD5 signature with the one published on the distribution media.
c. James will compare virus signature to the one published in a distribution.
d. James will compare the software size with the one given online.

Solution: The correct answer is B.

The **MD5 algorithm** takes an entered message of arbitrary length and outputs a 128-bit fingerprint/message digest. It is thought that it is infeasible that two messages having the same message digest will be created, or that, having been given pre-specified target message digest, any message could be derived.

Background: A tool has a database containing signatures enabling security teams to detect a multitude of vulnerabilities in UNIX, Windows, and popular web CGI scripts. Plus, the database will discover DDoS zombies and Trojans.

Q: Which of the below tools is described above?

a. Nmap
b. Nessus
c. SARA
d. Anti-x

Solution: The correct answer is B.

Background: **Nessus** is a proprietary vulnerability scanning software (free for personal use only). The aim of this software is to uncover potential vulnerabilities through system testing. Nessus can check for a multitude of different vulnerabilities.

Q: Applying cryptography will defeat which of the below attacks?

a. Web ripping
b. DoS
c. Sniffing
d. Buffer overflow

Solution: The correct answer is C.

Q: Where a hostlist.txt file includes a listing of IP addresses and request.txt is the file output. Which of the below tasks will you perform by running this script?

a. Banner grabbing to the hosts provided in the IP address list.
b. Put nmap into the listen mode to the hosts provided in the IP address list.
c. Perform port scanning of the hosts provided in the IP address list.
d. Transfer the hostlist.txt file to the hosts provided in the IP address list.

Solution: The correct answer is A.

Background: Carl is a Security Administrator for a company. While monitoring the IDS, he notices that there has been a surge in ICMP Echo Reply packets received on the interface of the external gateway. On closer inspection, Carl discovers that the ICMP Echo Reply packets are originating from the Internet with no request from the internal host.

Q: What attack has most likely taken place on the company's network?

a. Land attack
b. DoS attack
c. Smurf attack
d. Fraggle attack

Solution: The correct answer is C.

Q: What are common signs that a system and its devices may be compromised and/or hacked? (Choose three)

a. New user accounts have been created.
b. Increased amount of failed logon events.
c. Consistency in usage baselines.
d. The server's hard drives will be fragmented.
e. Patterns in time gaps in system and/or event logs.
f. The system's partitions are encrypted.

Solution: The correct answer is B, C and F

Q: Which of the below is the most ideal path when dealing with security risks?

a. Ignore
b. Mitigate
c. Deny

d. Exploit

Solution: The correct answer is B.

Q: Alan is a penetration tester. Responsibility for a project has been given to him; he must employ penetration testing on his company's network. Running the test from home after downloading every security scanner he could find. Despite knowing the IP range of all systems and the exact network configuration, Alan is not able to discover any useful results from these security scanners. Why not?

Answer is complete. Select more than one answer if applicable.

a. Security scanners are not designed for testing through a firewall.
b. Security scanners cannot perform a vulnerability linkage.
c. Security scanners are only as smart as their database and cannot discover unpublished vulnerabilities.
d. Security scanners are as intelligent as their database and can discover unpublished vulnerabilities.

Solution: The correct answers are A, B, and C.

Q: Your manager has requests that you to create something that will showcase the improvement of security of your company's network over time. What is your manager expecting you to develop?

a. reports
b. metrics
c. standards
d. testing policy

Solution: The correct answer is B.

Background: Scott is a C programmer. He develops the following C program:

```
#include <stdlib.h>#include <stdio.h>#include <string.h> int buffer(char *str) { char buffer1[10]; strcpy(buffer1, str); return 1;} int main(int argc, char *argv[]) { buffer (argv[1]); printf("Executed\n"); return 1;}
```

Q: What kind attack does Scott's program have little to no protection against?

a. SQL injection
b. Cross site scripting

c. Denial-of-Service
d. Buffer overflow

Solution: The correct answer is D.

Breakdown: Scotts program copies a user-supplied string into 'buffer1', which can hold just 10 bytes of data. When a user sends over 10 bytes, it will cause a buffer overflow. A **Buffer overflow** will help an attacker in launching an attack on the target system and then the opportunity for the attacker to install backdoors on the system for future attacks.

Q: Which of the below is defined as unsolicited e-mails sent out to a large number of people?

a. Biometrics
b. Hotfix
c. Buffer overflow
d. Spam

Solution: The correct answer is D.

Breakdown: **Spam** refers to unsolicited e-mails sent to a large number of individuals.

Q: Which of the below languages are particularly susceptible to buffer overflow attacks?

Answer is complete. Select more than one answer if applicable.

a. C
b. C++
c. Java
d. Action script

Solution: The correct answers are A and B.

Breakdown: C and C++ are susceptible to buffer overflow attacks.

Q: Which of the below algorithms can be employed in verifying file integrity?

Each correct answer represents a complete solution. Choose two.

a. MD5
b. SHA
c. RSA

d. Blowfish

Solution: The correct answers are A and B.

Breakdown: Any hashing algorithm can be employed to learn whether any changes have occurred in a file. In this process, the hashing algorithm will compute the hash value of the file specified, and a sender also sends a hash value with the file. Then, a receiver will recalculate the hash value of the file and analyze whether the hashes actually match. Because MD5 and SHA are both hashing algorithms, either can be used to verify file integrity.

Functions of **SSL**: Secure Sockets Layer (SSL) is used to secure Web communications between clients and Web servers, and offers privacy, authentication, and message integrity. This protocol will allow clients and servers to communicate in a way that still protects clients from eavesdropping and tampering.

Internet Protocol Security (IPSec) is a standards-based protocol that offers the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. Note: IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

Q: Which of the below options represents the property of hash functions that ensures that it will not produce the same hashed value for two different messages?

a. Key length
b. Bit strength
c. Entropy
d. Collision resistance

Solution: The correct answer is D.

Q: You work as a network administrator and your company has a Linux-based network. You have set up and installed a VPN server for remote users to be able to connect to the company's network. Which of the below encryption types will Linux use?

a. RC2
b. MSCHAP
c. CHAP
d. 3DES

Solution: The correct answer is D.

Breakdown: For connections over VPNs, Linux will use 3DES encryption.

Q: Joel is a software developer. His workgroup's network has a web server that which hosts a company's website. Joel wants to improve the security of the Web website by implementing Secure Sockets Layer (SSL). Which of the below types of encryption does SSL use?

Each correct answer represents a complete solution. Choose two.

a. Secret
b. IPSec
c. Asymmetric
d. Symmetric

Solution: Answers C and D are correct.

SSL uses both asymmetric and symmetric encryptions to accomplish this task. Secure Sockets Layer (SSL) is a protocol used to send/receive private documents via the Internet. SSL uses a mixture of public key as well as symmetric encryption to provide communication privacy, authentication, and message integrity.

Q: Which of the below encryption algorithms is/are constructed on stream ciphers?

Answer is complete. Select more than one answer if applicable.

a. Blowfish
b. FISH
c. Twofish
d. RC4

Solution: Answers B and D are correct.

Breakdown: FISH and RC4 encryption algorithms are constructed on stream ciphers.

Q: Which of the below cryptographic algorithms represents a hashing algorithm that is vulnerable to both collision and rainbow attacks?

a. MD5
b. RC5
c. AES
d. RSA

Solution: The correct answer is A.

Q: Which of the below cryptographic algorithms is the simplest to crack?

a. SHA-1
b. RC5
c. AES
d. DES

Solution: The correct answer is B.

Q: Which of the below protocols will provide a framework for negotiation and management of security associations between peers, and also and traverses the UDP/500 port?

a. IKE
b. ESP
c. ISAKMP
d. AH

Solution: The correct answer is A.

Q: Which of the below declarations is correct about of digital signatures?

a. Digital signature is required for an e-mail message to get through a firewall.
b. Digital signature compresses the message to which it is applied.
c. Digital signature decrypts the contents of documents.
d. Digital signature confirms the identity of the individual who applies it to a document.

Solution: The correct answer is A.

Digital signature is a personal verification method based on encryption and authorization codes. It can be used for signing electronic documents. Digital signature not only validates the sender's identity, but also warrants that the content of the document(s) has not been modified.

Q: Kyle is setting up security on his website, an e-commerce site. He wants to be sure that any customer sending messages is really the customer he claims to be. Which of the below methods can Kyle take he use to certify this?

a. Packet filtering
b. Firewall
c. Digital signature

d. Authentication

Solution: The correct answer is C.

Q: In which of the below techniques does an attacker capture encrypted messages that have been encrypted using an identical encryption algorithm?

a. Chosen plaintext attack
b. Chosen ciphertext attack
c. Known plaintext attack
d. Ciphertext only attack

Solution: The correct answer is D.

Background: In a **ciphertext only attack**, the attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

- **Known plaintext attack**: In a known plaintext attack, the attacker should have both the plaintext and ciphertext of one or more messages. These two items are used to extract the cryptographic key and recover the encrypted text.
- **Ciphertext only attack**: In this attack, the attacker captures encrypted messages that encrypted using the same encryption algorithm. For example, the original version of WEP used RC4, and if sniffed long enough, the repetitions would allow a hacker to extract the WEP key. Such types of attacks do not require the attacker to have the plaintext because the statistical analysis of the sniffed log is enough.
- **Chosen plaintext attack**: In a chosen plaintext attack, the attacker somehow picks up the information to be encrypted and takes a copy of it with the encrypted data. This is used to find patterns in the cryptographic output that might uncover vulnerability or reveal a cryptographic key.
- **Chosen ciphertext attack**: In this type of attack, the attacker can choose the ciphertext to be decrypted and can then analyze the plaintext output of the event. The early versions of RSA used in SSL were actually vulnerable to this attack.

Q: As a security consultant, a company brings you in to run a vulnerability assessment on the system of this large entertainment organization. Company management wants to know how much time it will take you to get access to sensitive financial data. How would you respond to them?

a. Your best attempt should allow you access within 2-3 weeks.
b. You are running a vulnerability assessment, which does not involve pentesting (pentesting does involve getting access to sensitive data).
c. It is directly dependent on the security posture of the organization, and how well controls have been implemented.

d. It depends on the contract and which types of testing are allowed: white box testing, black box testing, etc.

Solution: The correct answer is B.

Q: Which of the below key phases in mitigating risk includes identifying vulnerabilities, assessing losses instigated by materialized threats, cost-benefit examination of countermeasures, and attacks assessments?

a. Risk assessment
b. Vulnerability management
c. Assessment, monitoring, and assurance
d. Adherence to security standards and policies for development and deployment

Solution: The correct answer is A.

Q: What tool would you use to trying to access domain name related records for a given organization?

a. Nmap
b. Traceroute
c. NSLookup
d. Neotrace

Solution: The correct answer is C.

NSLookup runs queries for Internet domain name servers and displays DNS records for IP and host names of crucial servers.

Q: What netcat command could you use to capture a password file?

a. pwdump> file.txt.
b. nc -l -p <port number> -e cmd.exe -d
c. nc -l -u -p 1111 < /etc/passwd
d. nc <ip address><port number><passwd>

Solution: The correct answer is C.

Breakdown: Netcat can be used to capture a password file. The above command is listening on port 1111 and capturing the /etc/passwd file.

Q: A fast food chain wants to improve its security posture related to IT infrastructure. Unfortunately, a lower security budget has been approved, and the company is now planning to run tests through utilities with an internal team in a concurrent fashion with the intent of replicating attacks from external attackers. When an increased budget has been approved, new assessments incorporate other areas such as security architecture and policy. Which of the below testing sequences is appropriate?

a. Gray box testing all through.
b. Manual testing, followed by automated testing.
c. Black box testing, followed by white box testing.
d. Automated testing, followed by manual testing.

Solution: The correct answer is D.

Q: Kevin M., a black hat, and secrets away some of his hacking tools by utilizing Alternate Data Streams (ADS). What must be true in this case?

a. Kevin's computer utilizes a FAT file system.
b. Kevin must be using an NTFS file system.
c. Alternate Data Streams is a baked into the Linux kernel.
d. Kevin is still running Microsoft Windows 98 if he is able to use this feature.

Solution: The correct answer is B.

Breakdown: Alternate Data Streams (ADS) is part of the NTFS file system and it allows more than a single data stream to be tied to the same filename, with the filename format "filename:streamname." Alternate streams are not listed in Windows Explorer, and their size will not included in the file size. This allows a hacker to run hacking tools or root kits without setting off any red flags.

Q: Bill is his company's backup administrator. His duties involve making backups of important data, and so he is only authorized to access this data in order to create backups. In some situations users with different roles have to access these same files. What is a secure way to manage the permissions?

a. Mandatory Access Control (MAC)
b. Discretionary Access Control (DAC)
c. Access Control List (ACL)
d. Role-Based Access Control (RBAC)

Solution: The correct answer is D.

Breakdown: **Role-based access control (RBAC)** is an access control model. In this model, a user can access resources according to his role in the organization. In this example, a backup administrator is responsible for taking backups of important data. Therefore, he is only permitted to access the files to create back ups. Sometimes users with a different kind of role will also have to access the same resources. This situation can be easily managed using the RBAC model.

Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity and permissions are granted via authorization. The metadata on the object defines the sensitivity of it. For example, if a user receives a copy of an object that is marked as "secret", the user cannot grant permission to other users to see this object unless they have the appropriate permission.

Discretionary access control (DAC) is an access policy determined by the owner of an object. The owner decides who is allowed to manage the object and what privileges they have. The use of Mandatory Access Control and Discretionary Access Control are not mutually exclusive and they may be used in conjunction with each other in order to provide more granular control over file permissions.

Q: John M. is his company's security administrator. Charles is the sales manager and is off site for a last minute sales meeting. Charles needs some restricted files sent to him on a Flash drive. John is worried that the drive may get lost in the mail or by Charles. The first thought John has is to encrypt the files, but he realizes that the encryption keys might be broken. What piece of software might he use to hide the files from prying eyes?

a. File Sniff
b. EFS
c. Snow
d. File Sneaker

Solution: The correct answer is C.

Q: Gary H. is a security administrator. He notices an inordinate amount of ICMP Echo Reply packets being received on the external gateway interface while watching the IDS. After looking into it further, he sees that the ICMP Echo Reply packets are originating from the Internet and there aren't any requests from the internal host. What kind of attacks could cause this issue?

a. DoS attack
b. Land attack
c. Fraggle attack
d. Smurf attack

Solution: The correct answer is D.

Q: What are the symptoms of a Denial of Service attack?

Answer is complete. Select more than one answer if applicable.

a. Results in an increase in the amount of spam
b. Helps services to a specific computer
c. Saturates network resources
d. Causes failure to access a Web site

Solution: The correct answers are A, C, and D.

Q: Kris H. is a professional ethical hacker. His latest project involves testing the security of www.ucertify.com. He doesn't want www.ucertify.com to know who is scanning them, but wants to discover open ports and applications that the web server is running. In order to do so he will initiate scanning with the IP address of some random third party. What technique can he use to make this happen?

a. UDP
b. RPC
c. IDLE
d. TCP SYN/ACK

Solution: The correct answer is C.

Breakdown: The **IDLE scan** is initiated with the IP address of a third party. Therefore, it is a stealth scan. Since the IDLE scan uses the IP address of a third party, it is almost impossible to detect the identity of an attacker.

Q: Eugene K. is a security administrator. He will execute an active session hijack against Secure Inc. He discovered a target machine that will allow a Telnet session. He found another active session because there is so much traffic already on the network. What should he do next?

a. Use Brutus to crack the telnet password.
b. Guess the sequence numbers.
c. Use a sniffer to listen to the network traffic.
d. Use macoff to change the MAC address.

Solution: The correct answer is B.

Q: The administrator of your network is allowing you to run some exploit code on your corporate network to test if the new IDS/IPS is able to discover and secure against the attacks. What might you use to try and bypass the IDS/IPS?

a. Metapreter
b. Payload
c. Exploit
d. Encoder

Solution: The correct answer is D**.**

An **encoder** will make the payload unreadable in order to mask an exploit. Most encoders will run parts of the payload through an algorithm. This algorithm also includes a decoder and when it reaches its target, the machine can decode the payload in order to run the exploit.

Q: When Bill G goes to check his morning news feed, he gets redirected to a site that is almost identical, however this other site is filled with malicious software. He realized his router has been compromised. What kind of attack has befallen Bill?

a. Route table poisoning
b. Hit and Run Attacks
c. Black hole attack
d. Persistent Attacks

Solution: The correct answer is A.

Routing table poisoning is one of the most common and useful kinds of attacks, and happens when an attacker alters or "poisons" a routing table. These poisoned entries in the routing table takes the victim to a destination address where malware can be injected or information can be gathered.

Q: Albert G. is a new pentester and is quickly building himself an arsenal of useful tools. What bootable Linux distro does he absolutely have to have because of the number of security tolls preloaded in the environment?

a. BackTrack (now Kali)
b. Bidiblah
c. VMware
d. botnets

Solution: The correct answer is A.

Q: If you needed to get a log message through a firewall what protocol and port number would you use?

a. SMTP - 25
b. SMNP - 161
c. Syslog – 514
d. POP3 -110

Solution: The correct answer is C.

Q: What is used to encrypt a message before it is sent using PGP?

a. receiver's private key
b. receiver's public key
c. senders private key
d. sender's public key

Solution: The correct answer is B.

Q: Which of these could be considered a preventative control measure?

a. Audits
b. Digital signatures
c. Disaster recovery plan
d. Smart cards

Solution: The correct answer is D.

Q: How do you define symmetric encryption in regards to asymmetric encryption?

a. It uses multiple keys to encrypt and decrypt data.
b. It uses sessions keys generated from each parties private key.
c. It uses the same key for encryption and decryption of data.
d. It creates a one-way hash that cannot be reversed.

Solution: The correct answer is C.

Q: After a major security audit all of the proposed changes are made, however there are still some risks of an attacker penetrating your network. What is your next move?

a. Cancel the project (go in a different direction)
b. Deny to management that there is remaining risk
c. Accept the risk if it is low enough (to management)
d. Continue to apply additional controls until all risk is eliminated

Solution: The correct answer is C.

Q: In regards to Proxy Firewalls, which of the following are true?

a. Proxy firewalls block network packets from passing in to and out of protected networks.
b. Proxy firewalls will increase the speed and functionality of a network.
c. Systems establish a connection with a proxy firewall, which then creates a new network connection for that device.
d. Firewall proxy servers decentralize all activity for an application.

Solution: The correct answer is C.

Q: If your company is hit with this kind of attack you should consider additional user training.

a. SQL injection
b. Application hardening
c. Vulnerability scanning
d. Social engineering

Solution: The correct answer is D.

Q: Which kinds of access controls are utilized by firewalls and routers?

a. Rule-based
b. Mandatory
c. Discretionary
d. Role-based

Solution: The correct answer is D.

Q: This kind of system will monitor, log, and alert you if you are being attacked, but cannot do anything to halt the attack.

a. Detective
b. Passive
c. Reactive
d. Active

Solution: The correct answer is A.

Q: The international standard for IT systems functionality is known as?

a. ITSec
b. ISO 18011
c. Common Criteria
d. Orange Book

Solution: The correct answer is C.

Key Terms – Index

J

K

L

M

N

O

P

R

S

T

U

V

W

X