Global Knowledge®

Expert Reference Series of White Papers

Hackers, Hacking, and CEHv8

Hackers, Hacking, and CEHv8

Bob Withers CEH, CEI, CISSP, Security+

There are many things my father taught me here in this room.
He taught me: keep your friends close and your friends closer.
-Michael Corleone

Introduction

Cybersecurity makes the news regularly. Whether it is the Stuxnet worm attacking the Iranian nuclear program, the Zeus botnet pillaging peoples' bank accounts, the Syrian Cyber Army taking down *The New York Times* website (or for that matter, Chinese hackers breaking into the same organization), we hear about cyber-attacks regularly in the press. Moreover, we may have been the victim of one of these attacks, including identity theft and financial fraud.

The security landscape has changed dramatically in the last 15 years, and particularly since the events of 9/11. You'll notice I said "security landscape" and that's true in general. While terrorist attacks are incredibly rare in the United States, as Bruce Schneier points out[1], he says that we tend to overemphasize the risk of the unusual[2].

This isn't to discount the threats of military, transnational, or socio-politically motivated cyber-attacks, but a bigger risk is from hacking that can be monetized: Identity theft, financial fraud, industrial espionage, theft of intellectual property, and financial disruption.

According to www.DataLossDB.org, the largest data breach in history was the theft of 152 million usernames and passwords from Adobe.com, closely followed by the Shanghai Roadway D&B Marketing hack. But, if you add up the next five largest data breaches, they add up to an astounding 531,000,000 records[3]. Apocryphally, the famous depression-era bank robber named Willie Sutton said that he robbed banks "Because that's where the money is."[4] The same question should be asked about why people hack on the internet?

Who's the Hacker and Why Do They Hack?

In US Criminal Law, a crime requires *means, motive,* and *opportunity*[5]. Unfortunately, it also requires a criminal and a victim. A weapon is required often, but not always. Cyber-crime is no different, other than having the crime occur electronically and intangibly.

The term "hacker" has a long and noble heritage. Hackney drivers, going back to the 17th century, were valued for their resourcefulness in navigating the streets of London and environs[6]. Hack writers provide the ability to produce written works (articles, news stories, fiction) on short notice[7]. In software, a hack was an elegant piece of code that accomplished its task with minimal effort[8].

At the end of the ARPANET and the dawn of the Internet, hackers were mostly explorers and experimenters. Largely because of the limitations of the computers of the era by which hackers took delight in creating the most efficient, esoteric code to optimize system performance. Curiosity drove a lot of the deliberate and accidental incidents on the nascent Internet. Hackers, such as *The Mentor,* posted manifestos to state their purpose and interests[9].

Today, the hacking landscape is far more diverse. Most hacking seems to be socio-politically or financially motivated. Sometimes, the motives are indistinguishable.

Transnational hacking and espionage are tools of modern warfare. Many countries on the planet are creating cyber armies, including the United States[10]. The North Korean Army very famously posted images of their cyber army[11].

Cyber-crime affects nearly every American. Criminals pursue personal information that can be monetized, including financial, credit, and personal information. Identity theft, as well as banking and credit fraud, have a massive cost on the US economy[12].

So, then, who are the hackers? Broadly speaking, we can describe them in a few categories:

- The ***Script-Kiddie***. These are the explorers and adventurers who probe systems on the Internet for fun, for curiosity, or exploration. Kevin Mitnik describes himself as just such an explorer[13].

- The ***Cyber-Criminal***. Organized crime costs organizations $11.56 million per year per organization that's affected[14]. According to *The Wall Street Journal*, cyber-crime and cyber-espionage cost $100 *billion* per year[15].

- The ***Cyber-Spy***. Between the Chinese government's theft of the plans for the new J20 fighter-plane[16], the failure of Solyndra[17], and Anna Chapman[18], governmental and transnational organizations are working to gain industrial and military secrets.

- The ***Cyber-Terrorist***. The threat of cyber-terrorism and related attacks against critical infrastructure, power and water systems, banking systems, financial institutions, and other related portions of our society threaten our way of life. Whether it is an attack against the power grid, as happened in the Brazilian state of Espirito Santo[19], or a patriotic hacker called th3j35t3r (The Jester)[20] taking down the website of the Taliban, denial-of-service (DoS) attacks serve to further the message and position of the political or religious cause.

- The ***Hacktivist***. Perhaps, we can combine *Hacktivism* with the category of the cyber-terrorist, but the purpose of the Hacktivist is to promote their message and support their cause. The group Anonymous, for example, launched their cyber-attacks in support of WikiLeaks and other organizations[21], and in retribution for perceived slights[22].

Labeling the hackers doesn't really describe the motive, opportunity, or weapon. The motive is to create or support power. Power may be religious, political, or financial. It may be to preserve or expand the power base. The opportunity and the weapon are closely tied. Because the world is so interdependent on networked and internetworked services, cyber-attacks provide an easy mechanism.

What Hackers Are Looking For and How They Get It

For the hacker, digital information that can be monetized is the Holy Grail. The process is rather straightforward: perform reconnaissance, break in, maintain access, and try (as best as you can) to cover over the intrusion.

Every system or computer or network is vulnerable to attack. Vulnerabilities arise because of software bugs (no software is perfect[23]), misconfigurations (both from the manufacturer and operator-induced), default configurations, and passwords. Many of these are well known, but others are unknown or unpatched by the software provider. These zero-day exploits often lead to system and network intrusions.

Fundamentally, there are four steps in just about any hack-attack:

1. Reconnaissance
2. Penetration
3. Maintaining access
4. Covering tracks

Although the last two steps aren't strictly necessary, they are helpful in providing down-the-road access and also in helping the preventing the victim from knowing that they have been victimized.

Reconnaissance is the process of gathering as much information as possible about the target/victim's environment. I'll point out that I didn't specify just the network or systems undergoing this footprinting. Reconnaissance, then, involves a holistic view of the target. We begin the investigation of any organization by looking at its footprint on the Internet. What are the company websites? Do they expose information about the company and its make-up? Who are the principal individuals in an organization and what's the corporate culture? Are email addresses and other confidential information visible?

By surfing search engines, can an attacker glean other information such as office locations, physical security, information posted about network, and system configurations? Is too much information (also called TMI) being released both through job sites, as well as social networks such as Facebook, LinkedIn, and so on?

So far, our reconnaissance has been almost completely passive. As in the physical world, stealth is critical. So, the beginning of the footprinting process interacts as little as possible with the subject of the analysis.

Passive analysis has its limits, however. We may be able to identify Internet-facing systems, for example, but not their operating systems or applications providing services. The Domain Naming System (DNS) will help us inventory systems and applications that provide services to Internet users. We may not, however, be able to identify supporting systems. For example, is there a database system supporting a website? What software and operating systems provide those data services?

To find these details, we will need to become more active in our reconnaissance. Scanning and enumeration allow us to probe deeper into an organization's infrastructure. Hackers look for live systems, the TCP and UDP ports that provide services, the applications providing those services, and they identify the operating system and computer architecture in the process, as well as any vulnerabilities that may be obvious or yield to scanning tools.

Following reconnaissance, the next step is to actually penetrate the target/victim environment. In certified ethical hacking (CEH) parlance, this is called *system hacking*. Using the handyman metaphor, hackers have many tools in their tool belt. These include:

- **Breaking passwords.** This is very often the first (and most effective) mechanism for penetrating a system or network. Passwords can be guessed, intercepted as network traffic, retrieved directly from systems, broken with various brute force, and other cracking attacks. I'll point out that passwords can be stored and transmitted openly (as with unprotected websites,) encrypted (in which case, they can be retrieved), or hashed. In the latter, systems store a digest of the password and the hacker's task is to reverse-engineer the original plain text.

- **Hacking websites**. Coming back to Willie Sutton, websites are hacked because "That's where the data is." Websites (based on application frameworks, based on web server software, based on operating systems, based on hardware connected to networks) create some of the most complex systems we have. Compounding the problem, web administrators have the mission to provide the content for their websites. They are not information-security professionals; they are technologists who have a job to do—provide the support for web content.

  Hackers attack websites at six tiers: defacement, DoS, attacking the website, attacking the web infrastructure, attacking the database underneath the web server, and attacking the web client. We will talk about DoS more broadly in a few moments.

  Whether to a spread political, religious, or social message (or "just because they can"), we see website defacement is a common problem. Usually because of misconfiguration or software bugs, defaced websites often display messages related to the cause of the attacker.

  Because websites facing the Internet are often in protected zones, breaking into the web server can lead to further attacks within the network. Internet-facing websites usually reside within screened or protected subnets, often called DMZs. Breaking into a web server can lead to further attacks within the DMZ or into the corporate networks behind them.

  The web infrastructure provides support connecting the website and the underlying services. Challenging the web infrastructure may provide the same level of access to the database system or to the DMZ.

  Databases underneath web servers provide a wealth of personally identifiable information (PII), including email addresses, contact information, and (often) credit card or other information that can be used for identity theft.

  Finally, the trust between the web server and the web client can be violated. With both cross-site scripting (XSS) and cross-site request forgery (CSRF), the web browser can be manipulated to perform actions such as information theft, redirecting the client to a new website, delivery of malware, and attacks against other web servers.

- **Malware**. Commonly, malware is defined as malicious software. Originally from French, *mal*, means sick, ill, or bad. We can look at four different types of malware, understanding that there is a large overlap between them. *Trojans*, named for the story of the Trojan horse from the Homeric poems about the Peloponnesian wars, are ways of maintaining remote control. Aside from providing access to the network over time (more about that, later), these also allow large-scale remote control of systems in the eponymously named botnets. Other kinds of malware include *viruses* and *worms*, which are self-propagating software often used to carry Trojans, and *rootkits*, which mask the presence of malware.

- **Network Interception**. Often called *sniffing*, network interception involves eavesdropping on network communications to allow the gathering of data. The three principal purposes of sniffing are to steal passwords and other access information, usurp someone else's network access (*session hijack*), and generally observe and record network communications. Wireless networks often provide the simplest media to sniff, but encryption will complicate the attack. Much like password-cracking, web cracking often involves retrieving the password or passphrase to a network. Other network interception often involves penetrating the network and insinuating a network-tap in appropriate locations.

- **Denial of Service**. Most commonly, we associate DoS with attacks on websites or other related services. The primary purpose of a DoS attack is to render a service unusable on the Internet. Whether for social, religious, governmental, political purposes, or "just for the fun of it"—DoS attacks have been in the news over the last few years. A style of attack, using botnets, allows the attack to be spread across (potentially) millions of systems to render networks and systems inoperable. These distributed denial of service (DDoS) attacks have brought down major networks. *DDoS* attacks can also be used to mask another attack or set of attacks.

Once a system or network has been penetrated, that may be enough. Consider the case of the thief who makes off with millions of credit cards from a website. More often, hackers require continuous access to a network in order to perpetrate their crime. Maintaining access is the process continuing control of the victim network or systems. Trojans and other malware, including those propagated by viruses and worms, provide this remote-access and remote-control.

The late science fiction author, Robert Heinlein, famously said "The only crime is getting caught." Covering tracks is the process of attempting to erase tracks of the intrusion and the actions of the attacker. Dr. Clifford Stoll's 1988 book, *The Cuckoo's Egg*, describes one of the earliest excursions into the hacker underground.

Ethical Hacking

Hackers are continually attacking networks and systems. Whether these attacks are motivated by financial goals (such as stealing personal or banking and credit information), social and political goals (the so-called *hacktivists*), exploration, mischief, or just curiosity, there are really only two purposes: to steal information or to execute a DoS attack.

When one performs the same acts as the attacker, but for defensive purposes, the security professional is looking to identify the vulnerabilities and take advantage of them. This is in the same way that the hackers are systematically attacking a business' network.

When a security professional hacks their own networks or is hired to do this on behalf of a client, we call this *ethical hacking*. There are other names for the activity, as well: penetration testing, red-teaming, tiger-teaming, and security testing. Regardless of the name, the goals are to identify and exploit system and network vulnerabilities. Unlike the attacker, the purpose of the exercise is to identify the flaws so they can be fixed. In ethical hacking, remediation is crucial to enhancing an organization's security posture.

The ethical hacker, with the emphasis on ethics, is a computer and network security professional who brings the same skills and methodology as the attacker to bear on a system and network. The goal of the ethical hacker is to strengthen the security of the environment.

There are several dimensions to conducting a security analysis using the ethical hacking methodology. First is the level of intrusiveness. A security analysis may scale from a simple scan of vulnerabilities, using industry-standard tools, to a complete break-in in a full-blown penetration test.

Secondly, the attack may come solely from the outside (called a black-box test), completely from the inside (white-box), or from the position of a malicious-but-unknowing insider (gray-box) test. Black-box tests are often performed without the knowledge of the maintainers of a network. White-box tests, on the other hand, are designed to be interactive with the network security infrastructure and have the goal of seeing how a network responds to a security test. Lastly, since a large portion of security violations come from inside any network's firewalls, gray-box tests pose as a malicious insider.

One of the key factors of an ethical hack is abiding by the statement of work (SOW), which defines the scope of the allowable and disallowed actions. An ethical hack's work does not exceed the constraints of the project. If a particular test is not allowed, the security professional should avoid it.

Any discussion of ethical hacking would be lacking without a discussion of the risks. Whether performing a relatively passive vulnerability scan or a fully intrusive penetration test, there are the risks of causing damage. Network scans can flood networks and other activity can become a DoS attack. Anyone performing a security analysis should be aware that they can inflict the damage that they are trying to avoid.

What is CEH?

Jay Bavisi and Haja Mohideen (the founders of EC-Council and the creators of the *Certified Ethical Hacking and Countermeasures* program after September 11th, 2001[24]), built the CEH program as a new kind of security program that was based on offensive security.

CEH is different from most other cybersecurity training programs in that it emphasizes the tactical aspects of cyber-defense. Most cybersecurity classes teach the *traditional* aspects of protecting systems. They include limiting the functions of a system, hardening the infrastructure and services, patching, policy-and-procedure. Instead, CEH teaches about penetration testing and the tools and techniques to conduct a red-team exercise.

The program teaches the fundamentals of hacking. The *ethical* part of CEH comes from what one does with the knowledge gained. The skills we teach in the CEH class include: password cracking, privilege escalation, use of malware (such as Trojans, worms-and-viruses, and rootkits), session hijack, exploitation of vulnerabilities (such as buffer overflows), and web hacking.

Mirroring the hacking cycle, the purpose of CEH is to teach our students the essential skills required to emulate and replicate the attacks on a network and systems. By performing the same exploits as the attacker on the Internet, defenders can (hopefully) discover the holes in their networks before the adversaries.

If system defenders can identify the vulnerabilities, then they can define the defenses. But, without that knowledge, they merely remain vulnerable to attack.

Who Is This For?

Admittedly, the idea of being taught to hack is appealing, at both an intellectual and visceral level. Many people will think about the appeal of the illicit nature of hacking. On the other hand, ethical hacking requires discipline and methodology. Any penetration test is a formal project with a statement of work, timeframes, deliverables, and defined outputs.

Obviously, the CEH program is for individuals employed in cyber-defense. Cyber-operations employees, as well as those employed in network and security operations centers, are ideal students for the CEH program. They of course can, however, be a benefit to systems administrators, network managers, and application programmers. Information technology auditors can also benefit because they gain the skills necessary for understanding the recommendations they make—how to conform to "best practices" and why.

Network support and management personnel face the challenge of maintaining and monitoring their networks. They also have the responsibilities for repairing abnormal situations and for incident response. Since network hacks are commonplace, network support and operations groups can learn from the experiences of attacking the networks they defend. Wired network and wireless hacking are of particular interest to this audience.

Attacks, such as web defacement and SQL injection, make the news because of website defacements or the theft of financial and personal information from Internet-facing servers. Additionally, organizations are rightly concerned with Internet-based attacks such as DoS and their distributed cousins. Web and database administrators have to deal with higher layers of complexity as they support web servers, application platforms and frameworks, and home-grown sites on top of all of the rest of the infrastructure. Over 25% of the content in the CEHv8 class directly addresses web attacks and related services. This makes the course essential for web and database administrators.

It has been said that, "The difference between hardware and software is that hardware breaks; software comes broken." Developers (whether application, mobile, web, or database) can benefit from the hacking and analysis skills that are taught in class. The aspects of the class related to network and infrastructure security directly affect application development because that is the environment where the software runs.

Security operations centers, policy analysts, and specialists in incidence response use the CEHv8 to learn what hackers are trying to do to their networks and systems. The class samples hacking techniques and tools, and demonstrates their effects. After all, the first step in incidence response is figuring out that something unusual happened. After that, the classification and remediation of the incident require an understanding of the event and the consequences.

Global Knowledge offers most of their classes as public sessions and onsite to businesses, governments, or other organizations. I had the pleasure of teaching a CEH class to a group of IT auditors at a major East Coast accounting firm. The room was filled with senior auditors, investigators, and so forth. They were all seasoned IT professionals. During lunch, the lead auditor took me aside and said, "You know, Bob, we've been telling our customer which practices to follow and which behaviors to avoid. But, we never knew why they were considered best practices. You've been showing us all week why we say what we do!" In other words, audit and control specialists and Information Assurance professionals are natural candidates for the class.

What's New in CEHv8

The CEHv8 course contains 20 modules, compared to 19 with the previous class version (7). The new module covers mobile devices, mobile threats, and cellular hacking. In addition, each of the other modules has been updated to reflect the latest tools, techniques, and threats.

There are also 20 additional labs in the course. These labs focus on modern attacks, including dedicated websites for web hacking and a selection of tools that operate in modern environments.

Each student receives courseware with color copies of all the presentation slides. These materials have a similar look-and-feel to Microsoft's tile-like presentation in Windows 8.Additionally, each student who receives a printed-copy of the courseware also gets access to an electronic copy of the student text. While the printed courseware contains the slides (and the labs,) the electronic courseware includes a discussion of each topic for more in-depth understanding.

Lastly, the DVD tools distribution has been updated and refined, with each section of tools matching the courseware modules and labs.

Complete Outline

The CEHv8 class covers the range of hacking and cyber-security topics, from the foundational to advanced topics, including the need for security to buffer overflows and web hacking. In the course the chapters are:

- **Introduction to Ethical Hacking:**
  Offensive security differs from traditional practices in that the latter depends on implementation of best practices, system hardening, and responding to threats while Ethical Hacking looks to exploit vulnerabilities with the purpose of remediating the problems. This module introduces current security issues, the hacking cycle, the reasons for implementing security, and provides an overview of vulnerability analysis.

- **Footprinting and Reconnaissance:**
  Any attack on a network, whether malicious or for defensive purposes, must start with reconnaissance. This is the process of identifying networks, identifying the systems within those networks, finding the services on those systems and the underlying operating systems and applications which serve those capabilities. Additionally, other reconnaissance includes identification of physical security, identifying web presences, and understanding the individuals within an organization. *Footprinting* is the process of performing passive reconnaissance, including web searches, using online resources (such as social networking and business intelligence sites), and people searches to build a profile of an organization and individuals.

  80–90% of the effort to exploit systems comes from the reconnaissance phase and footprinting provides a wealth of information. The important aspect of footprinting is that it is almost completely passive. The person performing the reconnaissance takes great pains to avoid any action that would warn the target that they are being reconnoitered. Use of web services, proxies, and Internet-based services form the basis of footprinting.

- **Scanning Networks:**
  Footprinting has significant limitations when one is identifying Internet-facing systems. First, we cannot find systems that are not published to the Internet through mechanisms such as the DNS. Secondly, we may not be able to identify the applications providing the services we've found, the operating systems, and platform architectures, because finding that information requires interacting with the target systems.

  Scanning is the process of using tools to identify all of these characteristics, as well as misconfigurations, unpatched systems, and other vulnerabilities. These activities can generate significant network noise, so the ethical hacker must take pains to perform these tests as stealthily as possible. In hacker parlance, we want to avoid "rattling the doorknobs."

- **Enumeration:**
  We complete the reconnaissance phase by finding other information that can be used to complete the attack. *Enumeration* is the process of discovering network-shared resources, distributed applications, user names and user groups, and (if possible) security settings.

- **System Hacking:**
  Traditionally, the skills in this module are those most commonly associated with hacking—both malicious and defensive. The first step is system penetration. Next, we escalate our privileges to become administrators on the target system. Administrator privilege allows us to install programs including several varieties of malware and to cover our tracks to avoid detection. The goals of the malware are to provide continued remote access, log keystrokes, and hide the presence of the malware.

- **Trojans and Backdoors:**
  In system hacking, we use the actions of the hacker to plant remote access software. This software is often known as a *RAT* or *Remote Access Trojan*. RATs, as well as other spyware, allow us to re-enter the network or to propagate access throughout the victim network.

- **Viruses and Worms:**
  Self-propagating software used to be the fodder of science fiction. But, beginning about 25 years ago, that changed as malicious software made its presence known on the Internet. Both viruses and worms are self-propagating, but the former needs to attach itself to a host application or part of the system. The virus executes when the carrier mechanism executes and it attaches itself to the host. As systems reboot or infected applications run, the viral code is invoked and runs and often propagates itself. Worms operate similarly with the exception that they run autonomously and do not need a host application or service.

  Viruses and worms are often used for destructive purposes. More often, however, they carry Trojans to extend cyber-criminals' access to victim systems. Botnets, specialized version of the Trojan, can be widespread infections. These bots are most commonly used to either send secure spam email for criminal purposes or to launch DoS attacks.

- **Sniffers:**
  Another tool hackers use to steal data is a *sniffer*, whose purpose is to intercept network traffic. Many network protocols send their data in the open, without any encryption. When a cyber-criminal uses a sniffer, they can capture the information, modify it in flight, or replay and re-inject it. On wired networks, this may require subverting the switching infrastructure. Wireless networks, however, are subject to easy sniffing if there is not encryption.

- **Social Engineering:**
  Donn Parker, in his seminal book[25], talks about the human factor being the weakest link in the security chain. Social engineering is often called *hacking the human*. This module explains the various techniques including using phishing email, use of intimidation and reputation, and the tools to facilitate social engineering.

- **Denial of Service:**
  We traditionally associate DoS with groups attacking websites for social, political, or religious causes. These so-called "hacktivists" will either deface websites or they will make Internet services unavailable for legitimate use. The attacks of "Anonymous[26] in support of WikiLeaks or against government websites are examples of this type of activity.

  The other purpose for DoS attacks is to be diversionary. If the defenders are kept busy, the hackers may be executing another simultaneous attack. This module covers DoS attacks and their siblings, DDoS hacks. We also talk about botnets and their command-and-control systems.

- **Hacking Web Servers:**
  The CEHv8 class divides web hacking into three portions: Hacking web servers, web applications, and attacking the underlying databases behind the web servers. Web servers and their applications are intrinsically more complex than other environments because we have the underlying network-system-and-operating-system. On top of that, the web server is also a large, complex application whereupon developers use pre-built frameworks to implement the customer-facing web application.

  In this module, we examine the impact of differing web server architectures, exploiting vulnerabilities of these platforms, and server hardening. We also take an in-depth look at patch-management and its effects on system security.

- **Hacking Web Applications:**
  Web applications have become much more complex over the last several years. With the advent of the so-called Web 2.0 services (as well as mobile applications), the opportunities for attack expand with the complexity of the environment.

  In this module, we examine the advanced web technologies such as SOAP, AJAX, and JAVA, as well as the infrastructures that provide content-and-media-rich websites. Beyond attacking the Web2.0 services, we also look at violating the trust between the web client and server with both XSS and XSRF. In this module, we exploit a specifically designed website to demonstrate the concepts of attacking web applications.

- **SQL Injection:**
  Databases underlie most modern websites. They provide services such as a storage location for a web server's web pages, information about how the pages are to be presented, and are facilitators for interacting with the site itself. Often, websites will have login mechanisms and even the ability to post comments or reply to surveys.

  All of this information is stored in the database servers that support the web server and its applications. Injection attacks allow the hacker to interact with the systems behind the web presence. SQL injection allows a hacker to bypass login mechanisms and to interact directly with the database management system (DBMS). In this module, we examine the ways to use the Structured Query Language (SQL) to proxy through web servers to directly command the DBMS. This may be to steal the stored data (such as usernames, passwords, credit card or social security numbers, or other personally-identifiable-data), modify existing information such as bank accounts, or to destroy the data in the database and executing a DoS attack.

  Like the lab in the Web Application module, we use specially crafted websites to demonstrate the tools and techniques for SQL injection.

- **Hacking Wireless Networks:**
  The advantage of wireless networks is that there are no wires. The disadvantage of wireless networks is that there are no wires. Intrinsically, wired and switched networks provide some protection against sniffing the network. That protection doesn't exist in a broadcast radio environment using WiFi. Wireless networks are then susceptible to eavesdropping, data modification, and spoofing (or faking) client or access point information. Wireless encryption provides some protection, but even that can be attacked.

  In this module, we examine the benefits and risks of wireless networks, the attacks against these networks, and how to hack the systems attached to wireless environments. We also examine the process of breaking the encryption used to protect the on-air signals for these services. As part of this module, we also look at the risks and protections for Bluetooth devices when they are connected to the network infrastructure or mobile devices.

- **Mobile Device Hacking:**
  This past year, tablets outsold traditional PCs[27]. In the third quarter of 2013, the Android operating system made up 80% of all new mobile phone sales. Industry buzz says we are in the post-PC era[28]. The threats to mobile devices from traditional sources (such as theft and malware) extend from the traditional security environment. There are two significant differences, however. First, is the mobile nature of the victim. BYOD is taken to mean "Bring Your Own Device." Many employees would rather use their own PCs, tablets, or phones instead of the ones issued by their employers. Employers benefit from the cost saving of moving the work to the employees' devices. However, without proper security, the mobile risks often exceed the benefits.

  In other words, BYOD can also mean "Bring Your Own *Destruction*." This module examines the mobile landscape and hack attacks against the devices and the data upon them.

- **Evading IDS, Firewalls, and Honeypots:**
  The purpose of an ethical hack is to identify weaknesses in the network. By using the same techniques as the attackers, the penetration tester finds and exploits the target's vulnerabilities. One significant difference is that the person hacking for defensive purposes recommends solutions to the exploits they find.

  A key aspect of this is the hacker's identification of defensive systems and being able to successfully evade them. In this module, we look at the use and implementation of intrusion detection systems (IDS), network firewall systems, and honeypot servers. A honeypot is a specifically instrumented computer system whose purpose is to trigger alarms when probed by hackers.

  In this module, we examine the role of these systems, and detection and evasion techniques. The goal of this module is to provide the network defenders with information about how hackers are circumventing the network defenses.

- **Buffer Overflows:**
  Looking at software development, programmers write buggy code. This is simply a fact of life. The best code, or even the simplest, will have flaws because of the programmer's errors or faults in the underlying supporting operating system and infrastructure. After all, an operating system on a computer is just another computer program whose role is to control the machine. One of the earliest names for an operating system was the Master Control Program (MCP)—with due reference to the movie *TRON*.

  Hackers will exploit these failings in software systems through a variety of mechanisms and tools. The Metasploit Framework, for example, allows both hackers and defenders to exploit bugs in the software.

  Using buffer overflows, the attacker sends specifically malcrafted input data to a program. This data includes the text representation of computer instructions which overwrite legitimate program code and sufficient padding to position the new instructions at the correct location in an application's system memory. Using buffer overflows, the hacker attempts to subvert the running application or the underling operating system to their own purposes.

- **Cryptography:**
  For more than 3,000 years, people have worried about eavesdroppers intercepting communications. This includes personal communications, military and diplomatic communiqués, and other confidential information. Encryption and the use of other ciphers and data-hiding techniques have helped protect the confidentiality of these communications. Generally speaking, cryptography can be viewed as code-making and cryptology as code-breaking.[29] This module examines the use of cryptography, cryptographic techniques, and the ways of breaking cryptographically encoded information. Because defenders need to protect their data in flight and at rest, and because hackers want to intercept that information, cryptography is foundational to strong security mechanisms. In this module, we review the principles of cryptography and then learn about applying cryptology to crack the protected information.

- **Penetration Testing:**
  We return to the key question of ethical hacking—why are we doing this? When we posit that the defenders have to win all the battles, but the attacker needs only one, then defensive security is merely a holding action. Using the same techniques that the attackers use to find vulnerabilities and exploit them, the ethical hacker seeks out vulnerabilities and exploits them to see if an intrusion can be successful. Other names for the process include red-teaming, tiger-teaming, or penetration-testing.

  Beyond being able to successfully exploit weaknesses in system and network defenses, the purpose of penetration testing is to produce actionable results that will help the defenders strengthen their defenses. The end result of a penetration test is a report, with clear issues and actions that can be used to strengthen the security of the target environment.

  Penetration testing is the formalized action of putting the work to use in protecting the client's environment. The CEHv8 class covers the tools and techniques to perform an ethical hack. Following this, the EC Council ECSA/LPT program implements the formal testing and reporting methodologies.

The CEHv8 Exam

EC-Council, through the CEHv8 exam has achieved ANSI 17024 Certification. The criteria for Personnel Certification Accreditation, demonstrates that the certification process "…is conducted in a consistent, comparable, and reliable manner." Through ANSI's review process, ANSI has certified EC-Council's quality process.[30]

This process, along with US Department of Defense Directive 8570 endorsement, speaks to the quality and rigor of the certification.

With 125 questions and a passing score of 70%, this four-hour exam measures the skills needed to perform the duties that this class teaches. Students who attend Global Knowledge CEHv8 classes automatically receive a test voucher to take the exam at VUE testing centers.

Exam Objectives

From the EC-Council website[31], the CEHv8 exam tests the following areas:

- Background (5 questions, 4%): Networking, web and system technologies, communications protocols, malware operations, mobile operations, telecommunications, and backup and archiving

- Analysis/Assessment (16 questions, 13%): Data and systems analysis, risk assessments and technical assessment methods

- Security (31 questions, 25%): Systems security controls, application/fileserver, firewalls, cryptography, network and physical security, threat modeling, verification procedures, social engineering, vulnerability scanners, privacy/confidentiality, biometrics, wireless technology, trusted networks, and vulnerabilities

- Tools/Systems/Program (40 questions, 32%): Network/host based intrusion, network/wireless sniffers, access control mechanisms. cryptography techniques, programming and scripting languages, boundary protection applications. subnetting, port scanning, domain name system, routes/switches/modems, vulnerability scanners, operating environments, antivirus, log analysis tools, security models, exploitation tools, and database structures

- Procedures/Methodology (25 questions, 20%): Cryptography, public key infrastructure, security architecture, service oriented architecture, information security incident response, n-tier application design, TCP/IP networking, and security testing methodology

- Regulation/policy (5 questions, 4%): Security policy, and compliance regulations

- Ethics (3 questions, 2%): Professional code of conduct, appropriateness of hacking activities

How to Proceed from Here?

Audiences for the CEHv8 class range from working security professionals, to software developers, to website administrators, to systems engineers, to operations and network managers. Unlike other training programs and certifications, the CEHv8 program focuses on offensive security: how to hack and how to respond to the hacking incident. The CEHv8 course and exam are appropriate for the individual and group whose responsibilities include cyber-defense and incidence response. The program teaches the offensive security skills needed to respond to the changes in the security landscape.

According to the warrior-general *Sun Tzu*:

> *Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.*

These words, from *The Art of War*, describe how an understanding of your enemy ensures your success against them in battle. Our battleground is not a field with opposing warriors, but rather, opposing cyber-forces. In this conflict, both the defenders and attackers must use the same tools to gain the same advantages. You can only successfully defend when you understand your opponent, their techniques, and how they use their weapons.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training. Global Knowledge offers a comprehensive menu of cybersecurity courses, including:

Certified Ethical Hacker v8

Cybersecurity Foundations

CompTIA Advanced Security Practitioner (CASP) Prep Course

RSA Threat Intelligence

Cyber Security Compliance & Mobility Course (CSCMC)

IBM Security Systems Courses

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Bob Withers is a Principal Consultant with BWA, Inc., a cybersecurity training and consulting company specializing in healthcare security. He is also a Master Trainer for Global Knowledge, teaching both cybersecurity and Microsoft curricula. Bob holds the CISSP certification from ISC^2, C|EH, E|CSA/LPT, C|HFI, and C|EI certifications from EC Council, MCSE, and MCT accreditation from Microsoft, and many other industry-standard certifications. With more than 30 years of information technology and cybersecurity experience, Bob is also an author and speaker at security conferences across North America.

Endnotes

[1] https://www.schneier.com/blog/archives/2013/02/jared_diamond_o.html

[2] https://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html

[3] http://datalossdb.org/ as of 10/21/13

[4] http://en.wikipedia.org/wiki/Willie_Sutton

[5] http://en.wikipedia.org/wiki/Means,_motive,_and_opportunity

[6] http://en.wikipedia.org/wiki/Hackney_carriage#Etymology

[7] http://en.wikipedia.org/wiki/Hack_writer

[8] http://quotes.cat-v.org/programming/

[9] http://www.mithral.com/~beberg/manifesto.html, 1986

[10] http://www.stratcom.mil/factsheets/Cyber_Command/

[11] http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10239283/North-Korea-builds-online-troll-army-of-3000.html

[12] http://www.infolawgroup.com/2013/04/articles/information-security/2013-dbir/

[13] http://www.cbsnews.com/video/watch/?id=7380240n

[14] http://www.internetnews.com/security/report-cybercrime-costs-11-56-million-per-organization.html

[15] http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990

[16] http://www.dailymail.co.uk/sciencetech/article-2146283/Chinas-stealth-jet-goes-strength-strength-U-S-air-technology-falters-just-Chinese-rip-off.html

[17] http://www.technologyreview.com/view/429625/solyndra-files-suit-against-chinese-solar-cartel/

[18] http://gizmodo.com/5621350/russian-numbers-station-changes-broadcast#

[19] http://www.huffingtonpost.com/2009/11/07/cyber-attacks-caused-braz_n_349530.html

[20] http://www.youtube.com/watch?v=WeO44IWlkfU

[21] http://arstechnica.com/tech-policy/2011/01/fbi-goes-after-anonymous-for-pro-wikileaks-ddos-attacks/

[22] http://dailylounge.com/the-daily/entry/things-that-will-end-badly-company-trademarks-anonymous-logo

[23] http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=all

[24] http://www.cisse.info/news/24-speakers/128-jay-bavisi

[25] Donn Parker, *Fighting Computer Crime: A New Framework for Protecting Information*

[26] Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*

[27] http://www.bbc.co.uk/news/technology-20052118

[28] http://en.wikipedia.org/wiki/Post-PC_era

[29] http://www.ciphermysteries.com/2009/02/03/cryptography-vs-cryptanalysis-vs-cryptology

[30] http://www.eccouncil.org/ec-council-achieves-ansi-17024

[31] https://www.eccouncil.org/Certification/exam-information/ceh-exam-312-50