MODULO VI
Detección de Intrusos

PROGRAMA

1. Sistemas detectores de intrusos: basados en host y basados en red
2. Técnicas de detección de intrusiones
3. Verificación de integridad
4. Análisis de tráfico
5. Sistemas actuales de detección de intrusos
6. Detección activa. *Honeypots*.
7. Respuesta a incidentes
8. Técnicas de informática forense
9. Recursos

Terminología

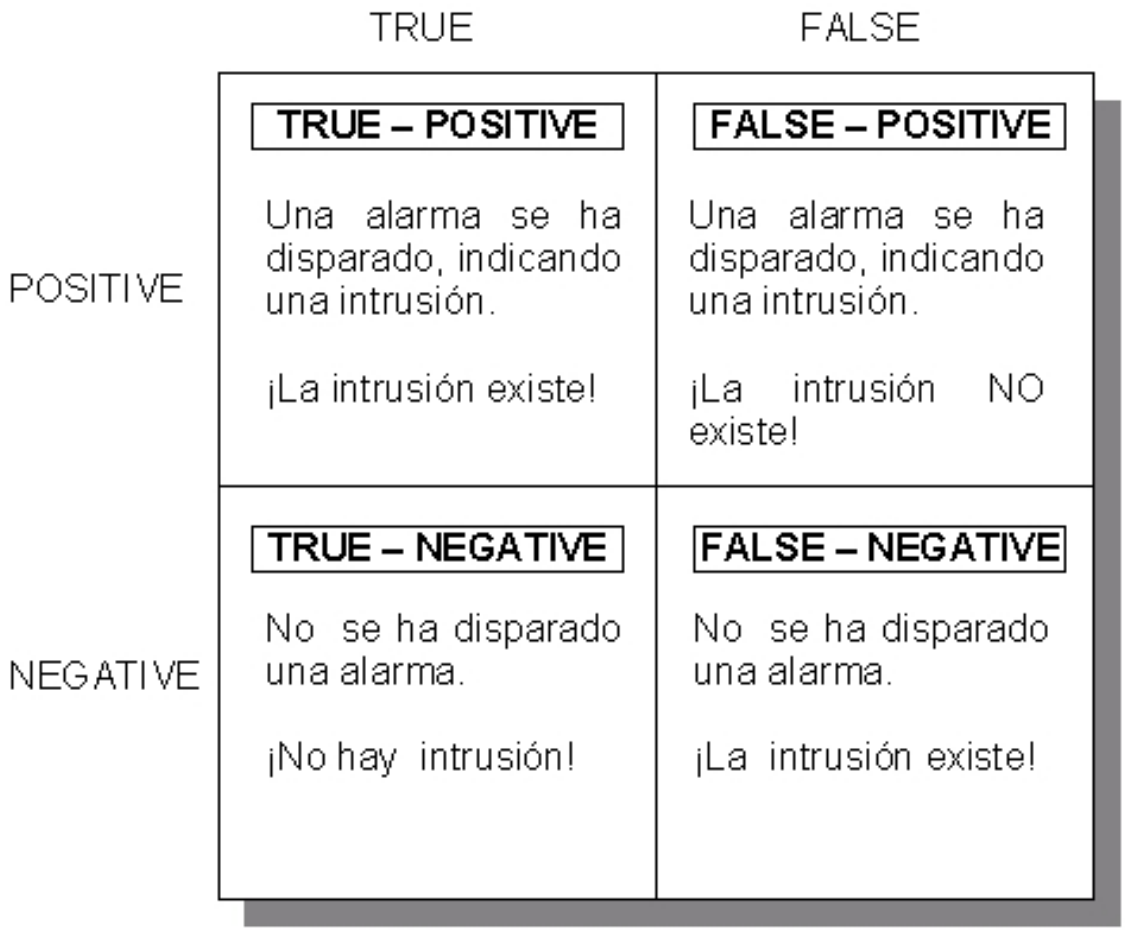
- Detección de intrusos

  - Es el proceso de detectar acceso, o intentos de acceso, no autorizado a los recursos de cómputo de una organización.

  - Es el arte de detectar actividad incorrecta, inapropiada, maliciosa o anómala en los equipos de cómputo o red de una organización.

  - El proceso de detección de intrusos puede ocuparse de la atención de ataques originados desde el exterior de la organización, o de ataques generados en el interior de la propia organización *(misuse detection).*

Matriz de IDS



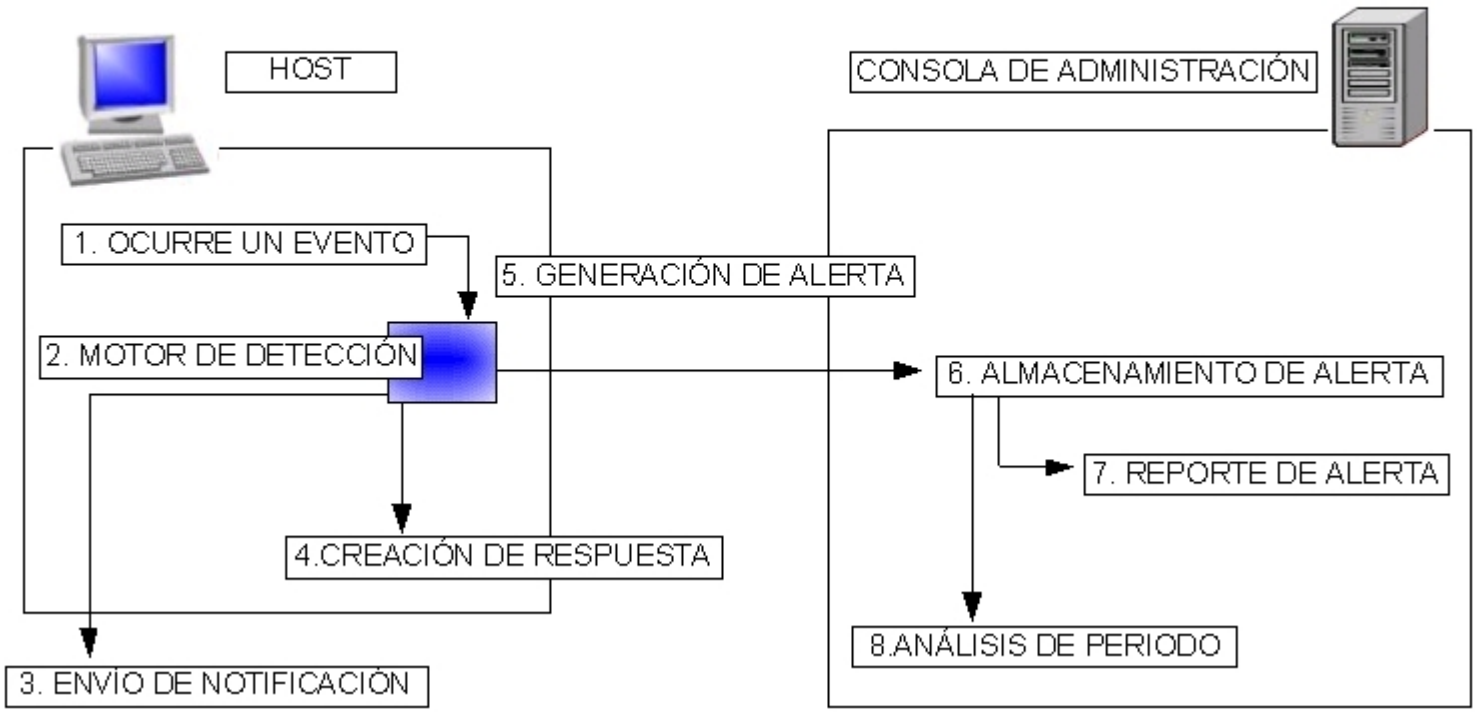
Capacidades de los IDSs

- Un IDS efectúa una o más de las siguientes actividades para realizar la detección de intrusos:
  - Reconocimiento de patrones asociados con ataques conocidos
  - Análisis estadístico de patrones anormales de tráfico
  - Verificación de integridad de archivos específicos
  - Monitoreo y análisis de actividad del sistema
  - Monitoreo y análisis de actividad de los usuarios
  - Análisis de tráfico de red
  - Análisis de bitácoras de eventos

Implantación de IDSs

- IDS basado en host (HIDS)
  - Los datos que serán analizados son generados por los equipos de la red
  - Los datos a analizar pueden ser:
    - recopilados de las bitácoras de las aplicaciones o las bitácoras del sistema operativo *(Logfile surveillance)*
    - *Obtenidos a partir de la verificación de la integridad de los archivos (File system integrity checking)*
  - Un sistema basado en host permite rastrear más fácilmente casos de uso inapropiado de recursos
  - Permite determinar con mayor facilidad si la intrusión fue exitosa

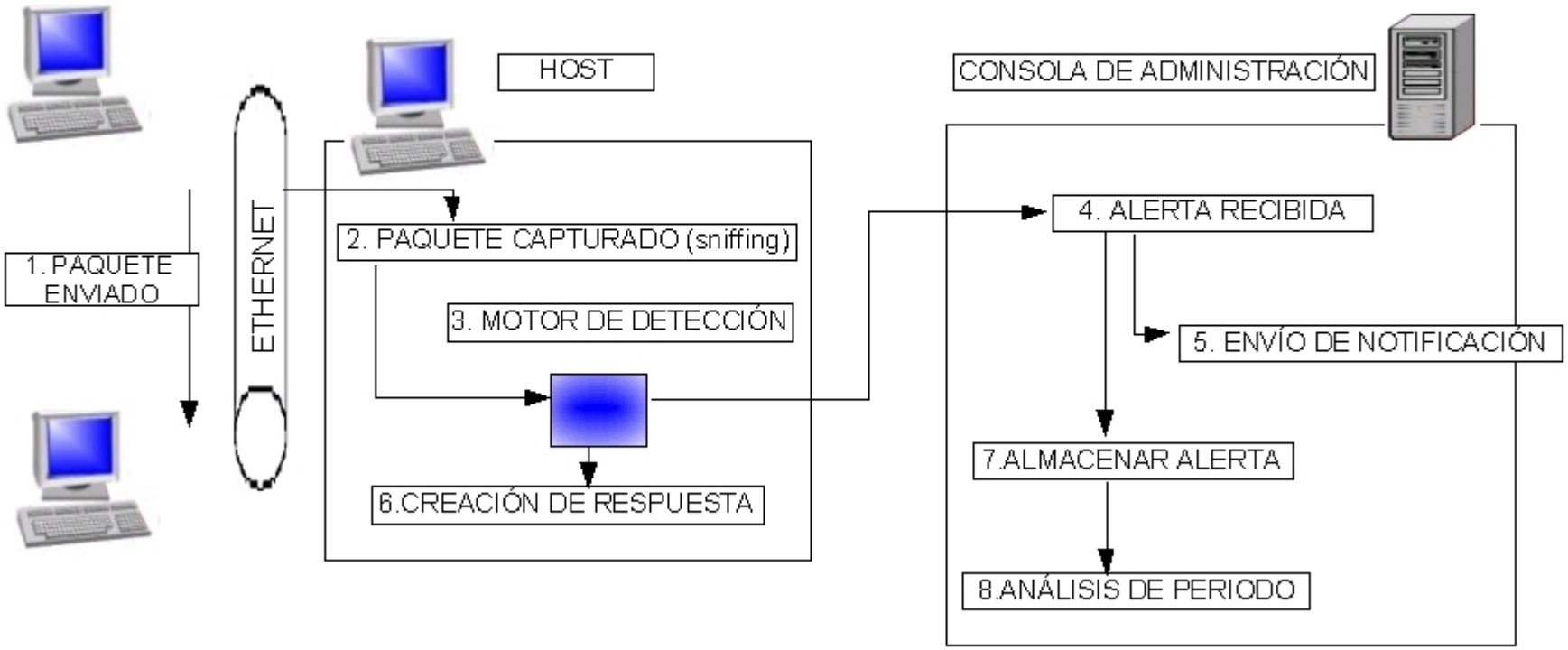
IDS basado en host



Implantación de IDSs (cont.)

- IDS basado en red (NIDS)
  - Se analiza el tráfico que fluye a través de un segmento de red, por medio de un sensor configurado en modo promiscuo *(sniffing)*.
  - Los sensores se instalan en posiciones estratégicas dentro de la organización. Usualmente se coloca uno en cada segmento crítico.
  - Un IDS basado en red no siempre permite determinar con exactitud si la intrusión fue exitosa

IDS basado en red



Implantación de IDSs (cont.)

- IDS basado en stack
  - También conocido como NNIDS *(Network Node IDS)*.
  - Similar a un *firewall* personal
  - Una variante de HIDS, que permite protección como la de un NIDS, en la cual el monitoreo se hace en la pila TCP/IP, permitiendo analizar los paquetes conforme fluyen en las diferentes capas.
  - Esto permite que los paquetes sean analizados por el IDS antes de que sean procesados por el kernel o por las aplicaciones

Implantación de IDSs (cont.)

- IDSs basados en host:
  - Tripwire (www.tripwire.org)
  - AIDE (*Advanced intrusion detection environment,* http://www.cs.tut.fi/~rammer/aide.html)

- ***IDSs basados en red:***
  - Dragon (www.enterasys.com)
  - Snort (www.snort.org)
  - ISS Real Secure (www.iss.net)

- IDSs basados en stack
  - Real Secure Desktop/Server (www.iss.net)
  - Tiny Firewall (www.tinysoftware.com)

Métodos de Análisis de ID-1

¿Cuándo analizar?

- *Análisis basado en intervalos*
  - Los eventos son recolectados y registrados en bitácoras (particulares o del sistema operativo)
  - Los datos son analizados en períodos de tiempo determinados
  - Se privilegia la exactitud de la información recopilada, sobre la velocidad de respuesta
  - Al no ser en tiempo real, no existe un gran impacto en el desempeño de los equipos en que residen los sensores
  - Los incidentes son detectados tiempo después de que han ocurrido.
  - Muy difícil responder a los incidentes

Métodos de Análisis de ID-2

¿Cuándo analizar? (continuación)

- *Análisis en tiempo real*
  - Los datos son analizados conforme son recolectados
  - El objetivo es que un ataque pueda ser bloqueado antes de sea completado y la víctima sea comprometida.
    - El equipo de seguridad puede atender el incidente mientras está ocurriendo
    - Pueden establecerse respuestas automatizadas para ataques conocidos
  - Se requieren recursos adicionales de procesamiento y memoria
  - La configuración es crucial, ya que una respuesta automática a un falso-positivo puede resultar costosa

Métodos de Análisis de ID-3

¿Cómo analizar?

- *Análisis de firmas*
  - El proceso de verificar la coincidencia de firmas de ataques conocidos contra los datos recolectados
  - Firma
    - Un evento o patrón de eventos que corresponde a un ataque conocido
    - Ejemplos: Una inundación de paquetes ICMP, una secuencia de bytes utilizada por un gusano
  - *Debe existir la firma en el IDS para que un ataque pueda ser detectado*
  - *Al encontrar una coincidencia, se genera una alarma indicando una intrusión (o actividad maliciosa).*
  - *Comunmente implantado en los IDSs comerciales*

Métodos de Análisis de ID-4

¿Cómo analizar? (continuación)

- *Análisis de Anomalías*
  - También conocido como *behavioral or statistical analysis*
  - El IDS crea perfiles de comportamiento de cada usuario (horarios de conexión, duración de sesiones en la red, ancho de banda utilizado, etc.)
  - El objetivo es encontrar una desviación a un patrón o comportamiento conocido.
  - Al encontrar una desviación se genera una alarma indicando una posible intrusión.
  - *No es incorporado comunmente en los IDSs comerciales*

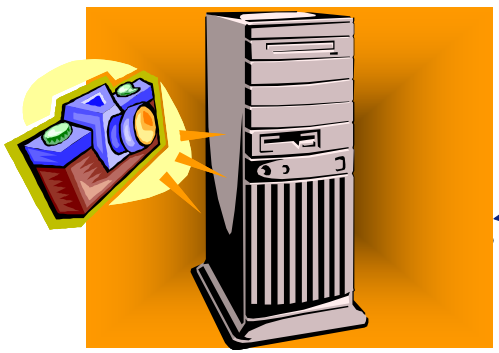
Verificación de Integridad

- La verificación de integridad de sistemas de archivos es una técnica que permite:
  - Determinar si se han modificado, eliminado o añadido archivos, con referencia en un estado anterior.
  - *Detectar y reparar fácilmente un sistema modificado intencional o accidentalmente*

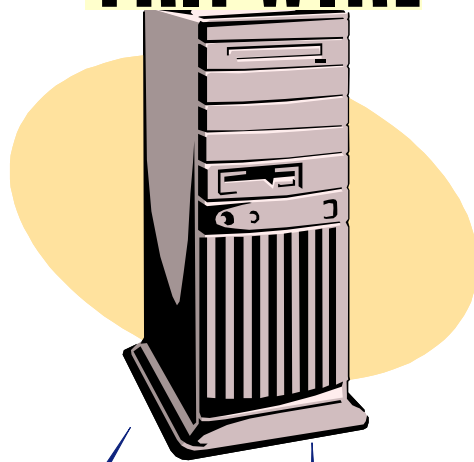
- *Herramientas de verificación de integridad*
  - *Algoritmos de digestión: MD5, SHA1*
  - *Firma digital: PGP, GPG*
  - *Tripwire (Unix, Windows)*
  - *AIDE (UNIX)*

Tripwire for Servers

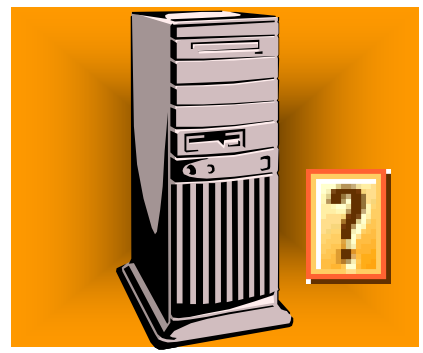
1. Tomar una foto digital de los archivos existentes



TRIPWIRE



2. Tomar una segunda foto, para comparar



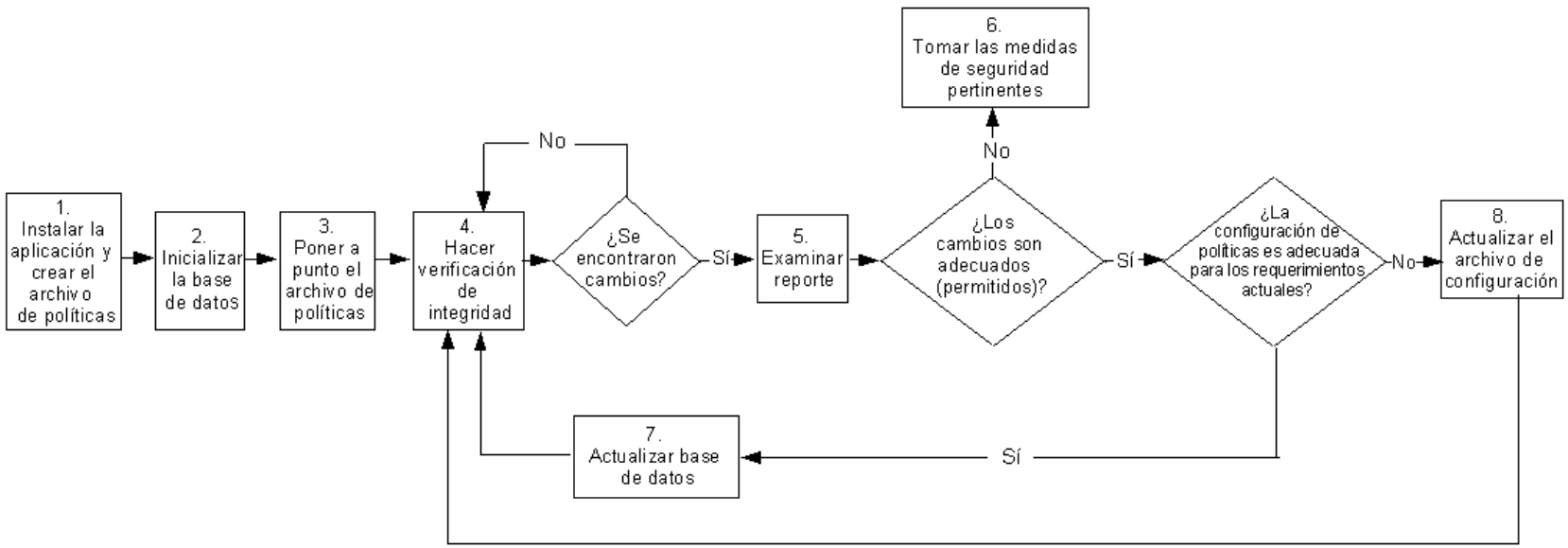
3. Las violaciones de integridad son registradas

SSL

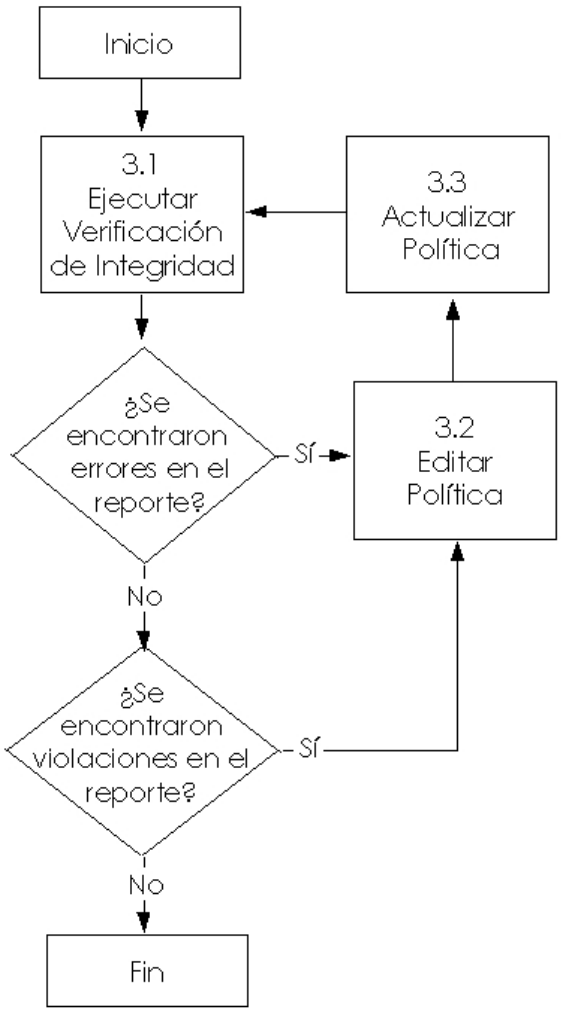
Componentes Tripwire

- *Política definida por el usuario*
  - ***Especifica los objetos en el sistema y los atributos de dichos objetos que serán verificados***
  - ***Es almacenada cifrada y firmada para prevenir cambios no autorizados (El Gammal, 1024 bits)***
- *Base de datos de estado*
  - ***Se construye con base en la política definida por el usuario.***
  - ***Se usa como base para determinar si han ocurrido cambios en el sistema***
  - ***Es almacenada cifrada y firmada para prevenir cambios no autorizados***
- *Llaves criptográficas*
  - ***Site key: protege las políticas y archivos de configuración que pueden utilizarse a lo largo de la organización.***
  - ***Local key: protege la base de datos y reportes de una máquina en particular***

Verificación de Integridad con Tripwire



Puesta a punto de políticas



Comandos de Tripwire

- ***twadmin***
  - ***Crear archivos de configuración y de políticas***
  - ***Realizar operaciones criptográficas a los archivos de Tripwire***
- ***tripwire***
  - ***Crear la base de datos***
  - ***Verificar integridad***
  - ***Actualizar la base de datos y las políticas***
- ***twprint***
  - **Presentar los reportes y la base de datos en texto plano**
- ***siggen***
  - **Generar e imprimir *hashes* de archivos**

Comando *twadmin*

- ***Crear y firmar el archivo de configuración de Tripwire a partir de un archivo de texto***

twadmin--create-cfgfile --site-keyfile /etc/tripwire/site.key /etc/tripwire/twcfg.txt

twadmin -m F -S /etc/tripwire/site.key /etc/tripwire/twcfg.txt

- ***Crear la política de Tripwire a partir de un archivo de texto***

twadmin--create-polfile /etc/tripwire/twpol.txt

twadmin -m P /etc/tripwire/twpol.txt

Comando *tripwire*

- ***Crear e Inicializar la base de datos con base en la política de Tripwire***

tripwire --init

tripwire -m I

- ***Verificar la integridad de los objetos, según la política***

tripwire --check

tripwire -m c

- ***Verificar la integridad de los objetos, según la política. Al término de la verificación, realizar interactivamente la actualización de la BD***

tripwire --check --interactive

tripwire -m c -I

Comando *tripwire (cont.)*

- ***Verificar la integridad de los objetos, según la política y enviar un reporte vía email***

tripwire --check --email-report [--email-report-level { 0|1|2|3|4 }]

tripwire -m c -M [-t { 0|1|2|3|4 }]

- ***Actualizar la base de datos de estado con base en un reporte de verificación previo***

tripwire --update --twrfile /pathto/reporte.twr

tripwire -m u - r /pathto/reporte.twr

- ***Actualizar la política de Tripwire a partir de un archivo de texto y sincronizar la base de datos de Tripwire con esta nueva política***

tripwire --update-policy /etc/tripwire/policy.txt

tripwire -m p /etc/tripwire/policy.txt

Comando *twprint*

- ***Imprimir un reporte en texto plano a la pantalla***

twprint --print-report --twrfile /pathto/reporte.twr [--report-level { 0|1|2|3|4 }]

twprint -m r -r /pathto/reporte.twr [-t { 0|1|2|3|4 }]

- ***Imprimir el contenido de la base de datos de estado a la pantalla***

twprint --print-dbfile

twprint -m d

Configuración de Políticas – 1

- ***Comentarios***
  - ***Permiten incluir explicaciones, instrucciones y otros textos en el archivo de configuración de la política con objeto de hacerla más clara***
  - ***# Este es un comentario***
  - ***objeto -> propiedades; # También este es un comentario***
- ***Reglas***
  - ***Especifican los objetos del sistema que serán verificados por la aplicación: archivos, directorios, llaves del registro de windows***
  - ***Especifican también las propiedades que serán modificadas***
  - ***Cada objeto puede estar en una sola regla***
  - ***objeto -> propiedades [atributos];***

Configuración de Políticas – 2

- ***Reglas (continuación)***
  - ***Ejemplo en Unix***

    /etc/home -> pinugs; # Objeto y propiedades son case-sensitive
  - ***Ejemplo en Windows***

    c:\winnt -> &size &sha1; # Objeto no es case-sensitive

    # propiedades son case-sensitive

- ***Propiedades de reglas***
  - ***Especifícan las características del objeto que serán verificadas.***
  - ***Para incluir una o varias propiedades, debe establecerse un caracter + antecediendo a una serie de propiedades (si no se especifica, por omisión se considera el caracter +)***
  - ***Para excluir una o varias propiedades, debe establerse un caracter – antecediendo a una serie de propiedades***

/mnt -> +pinu;

/mnt -> +pns -s; &size;

c:\winnt -> +&access &size;

c:\winnt -> &access &size -

Configuración de Políticas – 3

SEKUREIT CONSULTORES EN SEGURIDAD INFORMATICA

- ***Propiedades de sistema de archivos para objetos de UNIX***

p	Permisos de archivo
i	Número de ínodo
n	Número de enlaces
u	User ID del propietario
g	Group ID del propietario
t	Tipo de archivo
s	Tamaño
d	Número de dispositivo del disco en que el ínodo del archivo está almacenado
r	Número del dispositivo al que apunta el ínodo (sólo para dispositivos)
b	Número de bloques asignados
m	Estampa de tiempo de modificación
c	Estampa de tiempo de creación/modificación del ínodo
l	Cambio en el tamaño del archivo. Se espera que el archivo sea mayor que el último tamaño registrado
a	Estampa de tiempo de acceso
C	CRC-32
M	MD5
S	SHA
H	HAVAL

Configuración de Políticas – 4

- ***Atributos de las reglas***
  - ***Permiten extender la funcionalidad de Tripwire indicando cómo debe ejecutarse una regla o cómo debe reportarse una violación***
  - ***rulename***
    objeto -> propiedades (rulename=”archivos criticos”);
  - ***severity***
    - ***Valores posibles: 0 – 1'000,000***

    objeto -> propiedades (severity=150);
  - ***recurse***
    - ***Valores posibles: true|false ; 0 – 1'000,000***

    objeto -> propiedades (recurse=true);
    objeto2 -> propiedades2 (recurse=3);
  - ***emailto***
    objeto -> propiedades (emailto=usuario@dominio.com);

Configuración de Políticas – 5

- ***Bloques de reglas para aplicación de atributos***

```
(atributo1=valor, atributo2=valor, atributo3=valor)
{  regla;
   regla;
   ...
}
```

Ejemplo:

```
(rulename="bitacoras", emailto=administrador@dominio.com,
    severity=80)
{ /etc/passwd -> pinugst;
  /etc/shadow -> pinugst-s (emailto=cuentas@dominio.com);
  /bin/bash -> pinugstmbcM (severity=100);
}
```

Configuración de Políticas – 6

- ***Variables***
  - ***Permiten sustituir elementos predefinidos en las reglas de la política de seguridad***
  - ***La sustitución de la variable se hace usando el caracter $, seguido por el nombre de la variable entre paréntesis***
  - ***Ejemplos:***

```
ROOT=/etc;
$(ROOT) -> pin;

ROOT=c:\winnt;
$(ROOT) -> &sha ;

PROP_CRIT=pinugtsdbmcSM;
/temp -> $(PROP_CRIT);
```

Configuración de Políticas – 7

- ***Variables Predefinidas***

  ReadOnly

  - ***Conjunto de propiedades apropiadas para archivos con autorización lectura, disponibles a múltiples usuarios, pero que no deben ser modificados.***
  - ***Equivale a: +pinugsmtdbCM -racISH***
  - ***/bin/bash -> $(ReadOnly);***

  Dynamic

  - ***Conjunto de propiedades apropiadas para archivos y directorios que cambian frecuentemente.***
  - ***Equivale a: +pinugtd -rsacmblCMSH***
  - ***/etc/syslog.conf -> $(Dynamic);***

Configuración de Políticas – 8

- ***Variables Predefinidas (continuación)***

  Growing

  - ***Conjunto de propiedades apropiadas para archivos que normalmente crecen (tales como las bitácoras).***
  - ***Equivale a: +pinugtdl -rsacmbCMSH***
  - ***/var/log/syslog -> $(Growing);***

  IgnoreNone

  - ***Incluye todas las propiedades de un objeto***
  - ***Usarla siempre con -ar***
  - ***Equivale a: +pinusgamctdrbCMSH -I***
  - ***/var/lib/sendmail -> $(IgnoreNone) -ar;***

Configuración de Políticas – 9

- ***Stop Points***
  - ***Especifican objetos que serán excluidos en una verificación de integridad.***
  - ***El stop point se establece anteponiendo un caracter ! al nombre del objeto***
  - ***Util en el caso de verificación recursiva de directorios***

  - ***Ejemplo:***

    /var/lib/tripwire -> $(IgnoreNone) -ar;
    !/var/lib/tripwire/reports;

Configuración de Políticas – 10

- ***Directivas***
  - ***Permiten seccionar y establecer cierta lógica condicional en el archivo de políticas***
  - ***Las directivas inician con @@ seguido por el nombre de la directiva***

  @@section {GLOBAL|FS|NTFS|NTREG}
    - ***Esta directiva permite diferenciar diversos tipos de objetos de regla en el archivo de política***
    - ***@@section GLOBAL se utiliza para definir variables globales que pueden ser utilizadas en subsecuentes secciones de la política***
    - ***@@section FS se usa para definir las reglas de un sistema de archivos UNIX***
    - ***@@section NTFS se usa para definir las reglas de un sistema de archivos de Windows***
    - ***@@section NTREG se utiliza para definir reglas para el registro de windows***

Configuración de Políticas – 11

- ***Directivas (continuación)***

@@ifhost hostname [\|\| hostame2 \|\| ...]
@@else
@@endif

  - ***Permiten aplicar diferentes reglas a diferentes máquinas usando un sólo archivo de configuración.***
  - ***No pueden ser utilizadas dentro de un bloque de reglas***

Ejemplo:

```
@@ifhost aldonza||carrasco
    /etc/passwd -> $(Growing);
@@else
    /etc/passwd -> $(ReadOnly);
@@endif
```

Configuración de Políticas – 12

- ***Directivas (continuación)***

  @@end
  - ***Esta directiva marca el final lógico de un archivo de política***

  @@print "mensaje de texto"
  - ***Permite hacer debug de una política enviando una cadena de texto a stdout***

  @@error "mensaje de texto"
  - ***Permite hacer debug de una política enviando una cadena de texto a stdout.***
  - ***La aplicación termina y sale con un status de 1***

AIDE

- *Una alternativa no comercial a Tripwire*
- *Limitado en mecanismos de reporte de violaciones*
- *Incorpora algoritmos de hash adicionales para verificación de integridad*
- *Exclusiva para ambientes UNIX*
  - *Solaris*
  - *AIX*
  - *TRU64*
  - *Linux*
  - *BSDi*
  - *OpenBSD*
  - *FreeBSD*

AIDE (continuación)

p	Permisos
i	Inodo
n	Número de ligas
u	Usuario
g	Grupo
s	Tamaño
b	Número de bloques asignados
m	mtime
a	atime
c	ctime
S	Tamaño creciente
md5	MD5
sha1	SHA1
rmd160	RMD160
tiger	Tiger
>	p+u+g+i+n+S (Archivos de bitácora)
R	p+i+n+u+g+s+m+c+md5
L	p+i+n+u+g
E	Empty group

Configuración de AIDE

- ***Archivo de configuración***
  - ***/usr/local/etc/aide.conf***

- ***Reglas***

objeto propiedad1 + propiedad2 + propiedad3 + ...

```
/etc            p+i+u+g          #Verificar para archivos del directorio etc
/usr/bin/p      R                # Archivos que inician con p dentro de
   /usr/bin
/bin/vi$        p+i+n+u+g+s      # El archivo /bin/vi

 /var                            # Verificar el directorio /var
!/var/log/.*                     #  Excepto los archivo del directorio /var/log
```

Uso de AIDE

- ***Iniciar la base de datos***

  aide -c /usr/local/etc/aide.conf --init

  La base de datos recién creada e inicializada queda en /usr/local/etc/aide.db.new

- ***Verificar la integridad***

  Mover la base de datos /usr/local/etc/aide.db.new a /usr/local/etc/aide.db

  aide -c /usr/local/etc/aide.conf --check

- ***Actualizar la base de datos***

  aide -c /usr/local/etc/aide.conf --update

  La base de datos actualizada queda en /usr/local/etc/aide.db.new

Snort

- ***Un IDS basado en red con las siguientes características:***

  - ***Baja utilización de recursos***
  - ***Capaz de examinar todo el paquete, no sólo los encabezados (payload inspection).***
  - ***Tres modos de operación:***
    - ***Sniffer***
    - ***Packet logger***
    - ***NIDS***

      En este modo snort utiliza un conjunto de reglas que definen el tráfico que será considerado para la emisión de alertas.

Reglas de Snort -1

- ***Una regla se compone de dos partes:***
  - ***Encabezado***
    - ***Acción***
    - ***Protocolo***
    - ***IP origen/máscara***
    - ***Puerto origen***
    - ***IP destino/máscara***
    - ***Puerto destino***
  - ***Opciones***
    - ***Formato: (opción1: argumento1; opción2: argumento2; ...)***
    - ***Especifican el mensaje de alerta que será emitido***
    - ***Especifican qué parte del paquete es verificada en busca de una coincidencia***

alert tcp any any -> any 80 (content: "adult"; msg "Contenido para adultos";)

encabezado (opciones)

Reglas de Snort -2

- ***Encabezado***
  - ***Acción***

    alert ***Generar una alerta y registrar el paquete en la bitácora***

    log ***Registrar el paquete en la bitácora***

    pass ***Ignorar el paquete***

    activate ***Generar una alerta y activar otra regla dinámica***

    dynamic ***Permanecer ocioso hasta ser activado por una regla activate, después comportarse como una regla log.***

  - ***Protocolo***

    tcp

    udp

    icmp

    ip

Reglas de Snort -3

- ***Encabezado (continuación)***
  - ***IP origen/máscara, IP destino/máscara***

any	*Cualquier dirección IP*
10.1.1.0/24	*Red clase C: 10.1.1.0*
172.17.25.34/32	*Host 172.17.25.34*
[192.168.1.0/24,172.25.0.0/16]	*Una lista de redes*
!172.16.1.0/24	*Cualquier red, excepto 172.16.1.0/24*

  - ***Puerto origen, Puerto destino***

any	*Cualquier puerto*
80	*El puerto 80*
1:1024	*Rango de puertos 1 a 1024 inclusive*
:1024	*Cualquier puerto menor o igual a 1024*
500:	*Cualquier puerto igual o mayor a 500*
!12345	*Cualquier puerto, excepto el 12345*

Reglas de Snort -4

- ***Encabezado (continuación)***
  - ***Operador de dirección***
    - **->** *Origen a la izquierda, destino a la derecha*
    - **<>** *Considerar los pares de direcciones/puertos en cualquier dirección. Util para registrar sesiones completas.*

  - ***Puerto origen, Puerto destino***

any	*Cualquier puerto*
80	*El puerto 80*
1:1024	*Rango de puertos 1 a 1024 inclusive*
:1024	*Cualquier puerto menor o igual a 1024*
500:	*Cualquier puerto igual o mayor a 500*
!12345	*Cualquier puerto, excepto el 12345*

Reglas de Snort -5

- ***Opciones***

msg *Imprimir un mensaje en alertas y registros de bitácora*
msg: "Texto del mensaje";

ttl *Evaluar el valor del campo TTL del encabezado IP*
ttl: 128;
ttl: >220;

id *Evaluar el valor del campo Fragment ID del encabezado IP*
id: 39426;

content *Buscar la coincidencia de un contenido específico en el payload de un paquete. El caracter pipe (|) delimita datos binarios.*
content: "|0d0a5b52504c5d3030320d0a|"; #Firma de Sub7
content: "public";

Reglas de Snort -6

- ***Opciones (continuación)***

nocase *Desactivar case sensivity en la opción content*

content: "USER root"; nocase;

flags *Evaluar las banderas TCP de un paquete*

Banderas: F (fin), S (syn), R (rst), P (psh), A (ack), U (urg)

2 (bit reservado 2), 1 (bit reservado 1), 0 (banderas apagadas)

Operadores lógicos:

+ Todas las banderas especificadas hacen match (default)

** Alguna(s) de las banderas especificadas hace(n) match*

! Hace match si ninguna de las banderas especificadas está

encendida en el paquete

flags: A+; ***flags: 0;*** ***flags: SA*;***

flags: SF; ***flags: SRAFPU12;*** ***flags: S!***

Reglas de Snort -7

- ***Opciones (continuación)***

ack *Evaluar el valor de reconocimiento del protocolo TCP*

ack: 0;

sid *Especificar un número de identificación único de la regla*

sid: 983;

rev *Especificar el número de revisión de la regla*

sid: 983; rev: 2;

session: *Extraer los datos de aplicación de una sesión TCP*

session: printable; #Sólo lo que el usuario normalemente teclea o ve

session: all; # Toda la sesión. Caracteres no imprimibles se sustituyen por su equivalente hexadecimal.

Reglas de Snort -8

- ***Opciones (continuación)***

  flow ***Permite la inspección de paquetes basada en estados (en conjunción con TCP stream reassembly preprocessor). Adicionalmente, permite dar cierto contexto a las reglas.***

  from_client ***Hace match en solicitudes de "nuestro" cliente a un servidor "externo"***

  to_client ***Hace match en respuestas de un servidor "externo" a "nuestro" cliente***

  to_server ***Hace match en una solicitud hacia "nuestro" servidor por parte de un cliente "externo"***

  from_server ***Hace match en respuestas de "nuestro" servidor a un cliente "externo"***

  established ***Hace match si el paquete es parte de una conexión TCP establecida***

  stateless ***Hace match sin importar el estado de la conexión***

Reglas de Snort -9

- ***Opciones (continuación)***

  classtype ***Categoriza las alertas en tipos de ataques***
  El administrador puede especificar una prioridad a cada categoría (classification.config)

  classtype: attempted-admin;
  classtype: web-application-attack;
  classtype: trojan-acttivity;

Archivo classification.config

...
config classification: attempted-admin, Attempted Administrator Privilege Gain, 1
config classification: not-suspicious, Not Supicious Traffic, 3
...

Ejemplos de Reglas de Snort

- ***Captura del tráfico intercambiado en sesiones POP3***

  log tcp any any -> any 110 (session:printable;)

- ***Detección y registro de posibles contraseñas intercambiadas en texto plano*** ***alert tcp any any -> any any (content: "pass"; nocase; session: printable; ***

  msg: "Posible transferencia de password en texto plano";)

- ***Detección de escrutinio TCP NULL a la red 10.1.1.0/24***

  alert tcp any any -> 10.1.1.0/24 any (msg: "Detección de NULL scan"; flags: 0;)

- ***Intento de enumeración de usuarios a través de FINGER***

  ***alert tcp $EXTERNAL_NET $HTTP_PORT -> $HOME_NET 79 ***

  ***(msg:"Intento de enumeracion de cuentas con FINGER"; ***

  ***flow: to-server,established; content "a b c d e f"; nocase; ***

  classtype: attempted-recon; sid 321; rev: 5;)

Recursos

- ***Initial TTL values***

  http://members.cox.net/~ndav1/self_published/TTL_values.html

- ***Remote OS Detection***

  http://www.astalavista.com/library/os/misc/detection.shtml

- ***ICMP usage in scanning***

  http://www.sys-security.com/html/projects/icmp.html

- ***Artículos sobre IDSs (Securityfocus)***

  http://www.securityfocus.com/infocus/ids

Detección activa (Honeypots y Honeynets)

- ***Honeypot***
  - ***Un sistema, colocado en un ambiente de red real, diseñado para atraer y ser comprometido por atacantes***
  - ***Sus objetivos son:***
    - ***Mantener a los atacantes alejados de los equipos críticos, manteniéndolos ocupados con el honeypot***
    - ***Ser un mecanismo de alerta en el caso de un ataque***
    - ***Registrar la actividad del atacante***
    - ***Aprender, para incrementar la capacidad de detección y respuesta a incidentes del equipo de seguridad***

Detección activa (Honeypots y Honeynets)

- ***Honeypot de baja interacción***
  - ***Ofrece un nivel de actividad limitado al atacante.***
  - ***Normalmente emula servicios y sistemas operativos, de modo que el atacante no tenga interacción con sistemas operativos reales, pudiendo dañar a otros sitios***
  - ***Fáciles de implantar y mantener***
  - ***Ejemplo: Honeyd***

- ***Honeypot de alta interacción***
  - ***Sistemas operativos y aplicacione reales***
  - ***Es posible registrar ataques hasta ahora desconocidos.***
  - ***Implantación compleja***
  - ***Riesgo de que el honeypot pueda ser usado para atacar otros***

- ***Honeynet***
  - ***Una red completa diseñada específicamente para atraer y ser comprometida por atacantes***
  - ***Su diseño debe ser tal que los atacantes piensen que es un ambiente productivo real***
  - ***Características:***
    - **Un cortafuegos, dónde se controla y captura todo el tráfico generado por el atacante**
    - ***Honeypots de alta interacción de diversos tipos: Windows NT, Windows 2000, switches Cisco , Linux, Solaris, HP-UX***
    - ***Sistemas y servicios reales, no emulaciones.***
    - ***Nada se hace para disminuir o incrementar la seguridad de los componentes.***

Recursos

- ***Honeypots, Definitions and Value of Honeypots***

  http://www.tracking-hackers.com/papers/honeypots.html

- ***The Honeynet Project***

  http://www.honeynet.org

- ***Honeyd***

  http://www.honeyd.org

  http://www.securityprofiling.com/honeyd/honeyd.shtml

- ***Deception Toolkit***

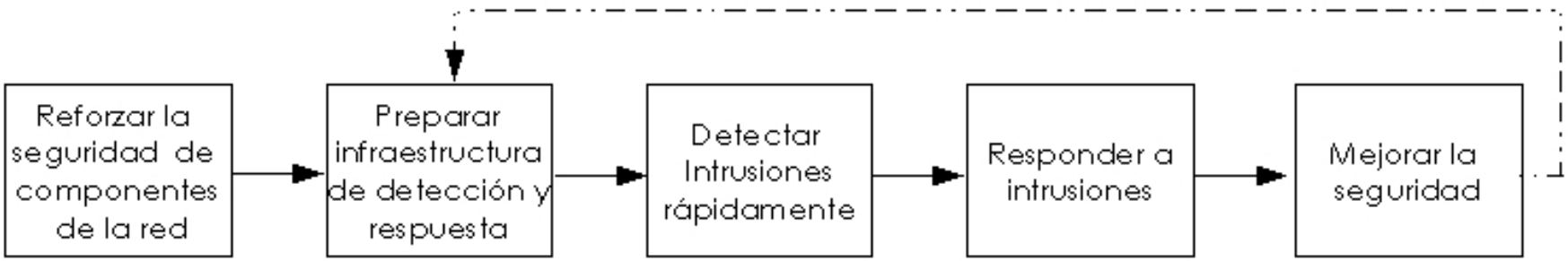
  http://www.all.net/dtk/index.html

Respuesta a Incidentes

- ***Incidente***
  - ***El acto de violar una política de seguridad explícita o implícita.***
  - ***Ejemplos de Incidentes:***
    - ***Intentos (fallidos o exitosos) para obtener acceso no autorizado a un sistema o a sus datos.***
    - ***Denegación de servicios***
    - ***El uso no autorizado de un sistema para procesar o almacenar datos***
    - ***Cambios al hardware, firmware o software de un sistema sin el conocimiento, autorización o consentimiento del propietario***

SkiP

SKiP Method
Security Knowledge In Practice
http://www.cert.org/security-improvement/skip.html



Asegurar componentes de la red

- ***Actividades***
  - ***Definición de Política de Uso Adecuado de Recursos***
  - ***Establecimiento de los mecanismos seleccionados para la seguridad física***
  - ***Aseguramiento de SO de servidores y clientes***
  - ***Actualización aplicaciones y servicios***
  - ***Instalación de parches existentes***
  - ***Establecimiento de mecanismos de autenticación***
  - ***Respaldo de sistemas de archivos***
  - ***Establecimiento de mecanismos de auditoría***
  - ***Implantación de solución antivirus***
  - ***Diseño e implantación de cortafuegos y DMZ***

Preparar infraestructura detección/respuesta

- ***Actividades***
  - ***Definición de Política de IDSs***
  - ***Etiquetar activos***
  - ***Establecimiento de mecanismos seleccionados para la detección de intrusiones que permitan monitorear, inspeccionar y auditar:***
    - ***Tráfico y carga de la red***
    - ***Bitácoras de aplicaciones, sistemas operativos, etc.***
    - ***Actividades de los usuarios***
    - ***Virus***
    - ***Integridad de archivos y datos***
    - ***Vulnerabilidades***
    - ***Procesos y servicios***
    - ***Dispositivos***

Preparar infraestructura detección/respuesta (cont.)

- ***Establecimiento de mecanismos de respuesta útiles en el proceso de respuesta:***
  - ***Disponer de pruebas de la integridad de datos, configuraciones y respaldos***
  - ***Desarrollar y tener disponible un kit de herramientas y dispositivos para la atención de incidentes***
  - ***Disponer de un entorno aislado para probar los elementos encontrados***
  - ***Disponer de discos de arranque e instalación de sistemas operativos y aplicaciones***
  - ***Disponer de parches necesarios para sistemas operativos y aplicaciones***
  - ***Desarrollar y validar procedimientos de respaldo y restauración***
  - ***Desarrollar y validar un plan de pruebas a un equipo restaurado, para su ejecución previo al retorno al ambiente productivo***
  - ***Disponer de una base de datos de contactos***
  - ***Desarrollar y validar procedimientos de comunicación durante el incidente***

Detectar intrusiones

- ***Utilizando sólo herramientas confiables en cuanto a su origen e integridad:***
  - ***Monitorear la red***
    - ***Variaciones de carga***
    - ***Tráfico de sitios inesperados***
    - ***Repetidos intentos de conexión fallidos***
    - ***Paquetes mal formados***
    - ***Conexiones en horarios inusuales***
    - ***Escrutinios de puertos***
    - ***Tráfico de exploits, virus, gusanos o troyanos conocidos.***
  - ***Monitorear el sistema***
    - ***Cambios de desempeño en el sistema: CPU, memoria, disco***
    - ***Actividades de los usuarios***
      - ***Login/logout***
      - ***Autenticación***
      - ***Procesos ejecutados***
      - ***Archivos accedidos***

Detectar intrusiones (cont.)

- ***Monitorear el sistema (continuación)***
  - ***Errores del sistema***
  - ***Estado de los procesos***
  - ***Escrutinio periódico de vulnerabilidades con herramientas especializadas***
- ***Monitorear sistemas de archivos***
  - ***Verificación de integridad de archivos y directorios con base en una periodicidad establecidad***
  - ***Detectar:***
    - ***Creación o eliminación de archivos y directorios***
    - ***Cambios en los atributos de los archivos***
    - ***Cambios en los archivos de configuración***
    - ***Violaciones a la integridad de las bitácoras***
- ***Auditar componentes de red***
  - ***Identificar dispositivos y sistemas no autorizados, conectados a la red.***

Responder a la intrusión

- ***Responder a la intrusión significa:***
  - ***Analizar la información disponible para caracterizar la intrusión, con objeto de determinar:***
    - ***¿Qué ataques fueron utilizados para ganar acceso?***
    - ***¿Qué datos y sistemas fueron accedidos por el intruso?***
    - ***¿Qué hizo el intruso después de obtener acceso?***
    - ***¿Qué está haciendo actualmente el intruso?***

Acciones Preliminares

1. ***Registrar en una bitácora todas las acciones relacionadas con la respuesta a la intrusión***
2. ***Cumplir las políticas de comunicación de incidentes***

Responder a la intrusión (cont.)

Acciones de respuesta

3. ***Capturar toda la información que puede perderse o no ser capturada por un respaldo, esta información incluye:***
   - ***Conexiones de red establecidas***
   - ***Procesos en ejecución***
   - ***Usuarios conectados***
   - ***Archivos abiertos***
4. ***Hacer una imagen completa del sistema comprometido, protegiéndola contra escritura***
5. ***Aplicar mecanismos para contener la intrusión temporalmente***
6. ***Analizar el sistema comprometido en un entorno aislado***
7. ***Buscar signos de intrusión en otros sistemas***
8. ***Examinar bitácoras de cortafuegos, IDSs y ruteadores. ¡ La sincronización de relojes es crucial !***
9. ***Identificar el ataque, a partir de la información recolectada***

Responder a la intrusión (cont.)

SEKUREIT CONSULTORES EN SEGURIDAD INFORMATICA

Acciones de respuesta (continuación)

10. ***Identificar las acciones del atacante luego de obtener acceso:***
    - ***Analizar bitácoras***
    - ***Verificar cambios en los sistemas de archivos***
    - ***Buscar información eliminada***
11. ***Antes de restaurar el sistema, eliminar cualquier medio de acceso del atacante:***
    - ***Cambiar todas las contraseñas a los sistemas que el atacante podría haber tenido acceso***
    - ***Si la preparación fue insuficiente, resintalar el sistema totalmente***
    - ***Eliminar las puertas de entrada del atacante identificadas***
    - ***Restaurar aplicaciones y servicios a partir de medios originales***
    - ***Verificar la configuración del sistema, aplicaciones y servicios***
    - ***Identificar y corregir otras vulnerabilidades que pudiera tener el sistema***
    - ***En caso necesario, mejorar los mecanismos de defensa y los mecanismos de detección***
12. ***Restaurar los sistemas a su operación normal***

Mejorar la seguridad

Luego de una intrusión o un intento de intrusión, es necesario:

- ***Evaluar la eficacia de las medidas de preparación para la ocurrencia de un incidente.***
- ***Evaluar la eficacia de las herramientas de detección***
- ***Determinar qué mecanismos podrían ayudar a mejorar el proceso de respuesta***
- ***Determinar el costo de la intrusión con objeto de utilizarlo como referencia en posteriores análisis de riesgos.***
- ***Elaborar un reporte del incidente para la Dirección***
- ***Determinar la necesidad de realizar un nuevo análisis de riesgos***
- ***Documentar las lecciones aprendidas y mejorar las políticas de seguridad y procedimientos.***
- ***Tomar las acciones legales pertinentes.***