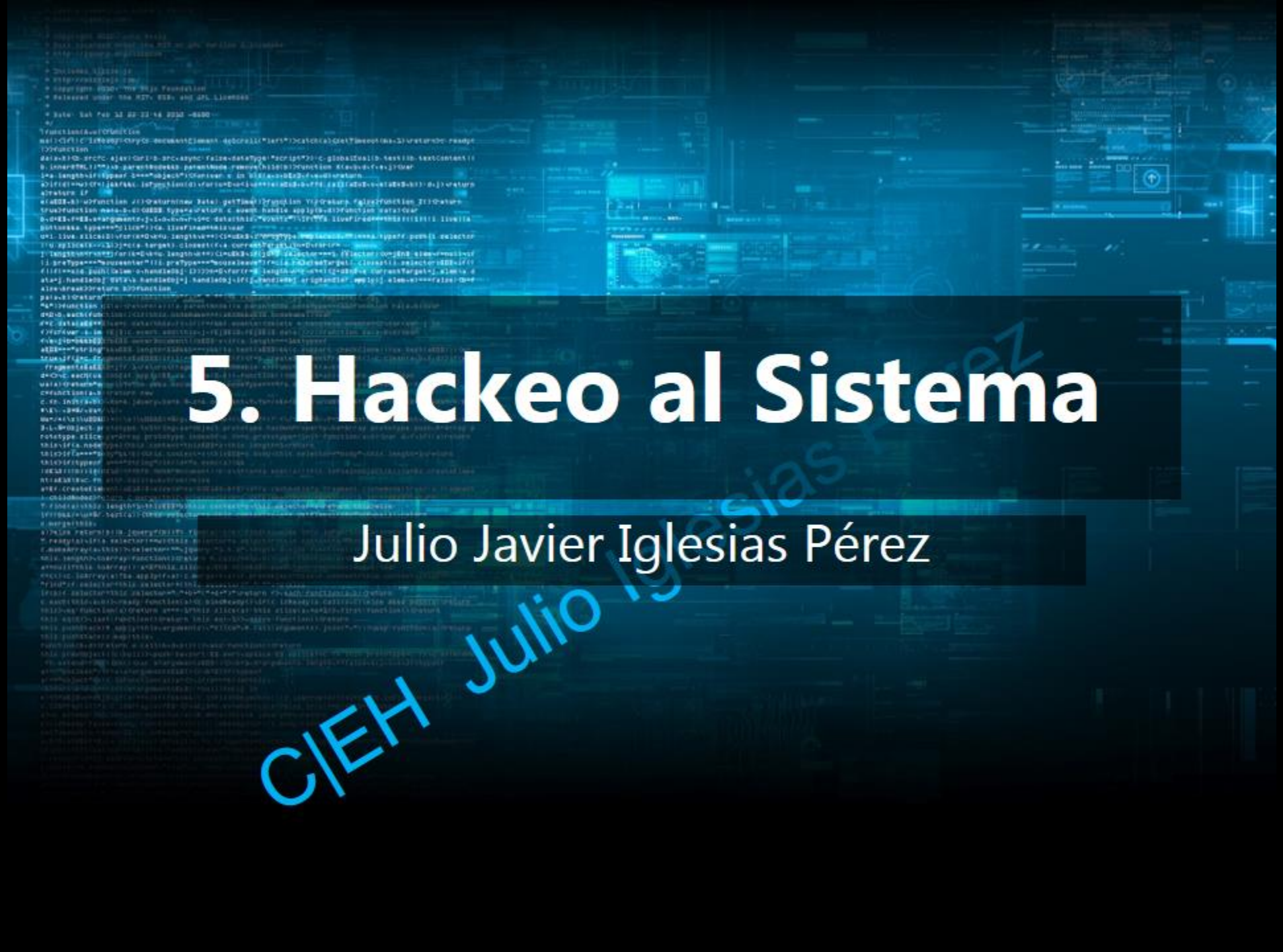

5. Hackeo al Sistema
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Metas

- Obtener Acceso. Para colectar información para obtención de acceso, utilizando password eavesdropping y fuerza bruta
- Escalar privilegios. Para crear una cuenta de usuario administrativa, utilizando password cracking y exploits.
- Ejecutar aplicaciones. Para crear y mantener acceso backdoor, utilizando troyanos.
- Esconder archivos. Para esconder los archivos maliciosos, utilizando rootkits.
- Escondiendo huellas. Para esconder la presencia, limpiando huellas.

Las contraseñas pueden contener:

- Solo letras: HIJKLLKDF
- Solo números: 9238647
- Solo caracteres especiales: $/"()
- Letras y números: lkjd2947
- Letras y caracteres especiales: P@sswo(#
- caracteres especiales y números: /("3413$@
- Letras, caracteres especiales y números: C0ontr@se/&"a

Técnicas de crackeo de contraseñas

- Ataques de diccionario: Un archivo diccionario es cargado dentro de la aplicación cracking, se ejecuta contra las cuentas de usuario.
- Ataques fuerza bruta: El programa intenta cada combinación posible de caracteres hasta que la contraseña es descubierta.
- Ataque híbrido: Funciona similar al ataque de diccionario, pero agrega algunos números y símbolos a las palabras e intenta descubrir la contraseña.
- Ataque de sílaba: Es una combinación de fuerza bruta con diccionario.
- Ataque basado en reglas: Es utilizado cuando el atacante obtiene algo de información acerca de la contraseña.

Tipos de ataque a las contraseñas

- Passive Online Attacks: Wire Sniffing. Los atacantes ejecutan herramientas sniffer en la LAN.
- Man-In-the-Middle and Replay Attacks. El atacante accede en medio del cana de comunicación entre la victima y el servidor para extraer información.
  Es difícil de realizar.

Tipos de ataque a las contraseñas

- Password Sniffing. difícil porque el atacante conoce el nombre de usuario pero tendría que “adivinar” la contraseña.
- Active Online Attack: Password guessing Intentar adivinar el pass utilizando un diccionario de palabras y letras e intentar todas las combinaciones posibles. Toma mucho tiempo. Necesita mucho ancho de banda y es fácilmente detectable.

Tipos de ataque a las contraseñas

- Otros son Troyanos, Spywares y Keyloggers.
- Hash Injection Attack: Permite al atacante inyectar un hash comprometido en una sesión local y utilizar el hash para validar recursos de la red. El atacante encuentra y extrae un hash de un administrador del dominio que esté con la sesión iniciada. El atacante utiliza el hash extraído para iniciar sesión en el controlador del dominio.

Tipos de ataque a las contraseñas

Cuando un administrador establece una conexión remota en S.O. Microsoft, se crea un token en la memoria, hay una aplicación llamada Pass the Hash e involucra dos programas, who is there y I am; who is there realiza consultas de todos los tokens del equipo y I am permite declarar que las credenciales que estamos utilizando son las nuestras. Es bastante poderoso.

Rainbow attacks: Pre-Computed Hash

- Convierte enormes cantidades de palabras como archivos de diccionario y fuerza bruta en las listas de hashes de contraseñas que utilizan técnicas tales como las Rainbow Tables
- Ejemplo:

Contraseña	Hash
1qazwed	425cc3499c530b28zf225d668590

- Del hash sale la contraseña, las raibow contiene los hashes

Distributed Network Attack (DNA)

- DNA Manager es instalado en una locación central donde las maquinas DNA clientes puedan acceder desde la red.
- DNA Manager coordina el ataque y asigna pequeñas porciones de la llave a los equipos que están distribuidos por la red.
- Los clientes DNA ejecutan en background y consumen solo el tiempo del procesador que está sin uso.
- El programa combina la capacidad de procesamiento de los clientes de la red y utiliza el trabajo en conjunto para descifrar.
- Ejemplo: elcomsoft distributed password recovery

Contraseñas por defecto

Recordar buscar en internet los default passwords en sitios como:

- www.phenoelit-us.org
- www.defaultpassword.com
- cirt.net
- default-password.info
- defaultpassword.us
- passwordsdatabase.com

Robar passwords utilizando USB

Robar passwords utilizando USB

1. Necesitaremos una hacking tool
2. Copiar los archivos en la USB
3. Crear un autorun.inf

```
[autorun]
en=launch.bat
```

4. El contenido de launch.bat

```
start pspv.exe /stext pspv.txt
```

5. Insertar la USB y la autorun se ejecutara
6. Password2 es ejecutado en segundo plano y los password serán almacenados en un archivo .txt en la USB

Autenticación Microsoft

La autenticación NTLM (NT LAN Manager) es un protocolo de autenticación de Windows NT 4.0/2000. Microsoft actualizó este protocolo de autenticación a Kerberos, el cual se considera más seguro que NTLM.

El hash LM ha sido deshabilitado en Windows Vista para adelante.

El archivo SAM está ubicado en: C:\Windows\system32\config\SAM

LM Hash

LM Hash es muy inseguro. Microsoft lo utiliza para almacenar password de menos de 15 caracteres. Cuando el pass es encriptado por este algoritmo, primero todas las letras son convertidas a mayúsculas, ej: 123456QWERTY. Luego se agrega caracteres nulos al final para hacerlo de 14 caracteres. 123456QWERTY__. Antes de cifrarlo, el pass es dividido en dos 123456Q y WERTY__ y es individualmente encriptado.

LM Hash

123456Q=6BF11E04AFAB197F

WERTY__=F1E9FFDCC75575B15

El hash de este pass seria:
6BF11E04AFAB197FF1E9FFDCC75575B15

Los primeros 8 bytes son derivados de los primeros 7 caracteres de la contraseña y los 8 segundos son derivados desde el carácter 8 al 14.

Si la contraseña tiene menos de 7 caracteres, la segunda mitad siempre será: 0XAAD3B435B51404EE

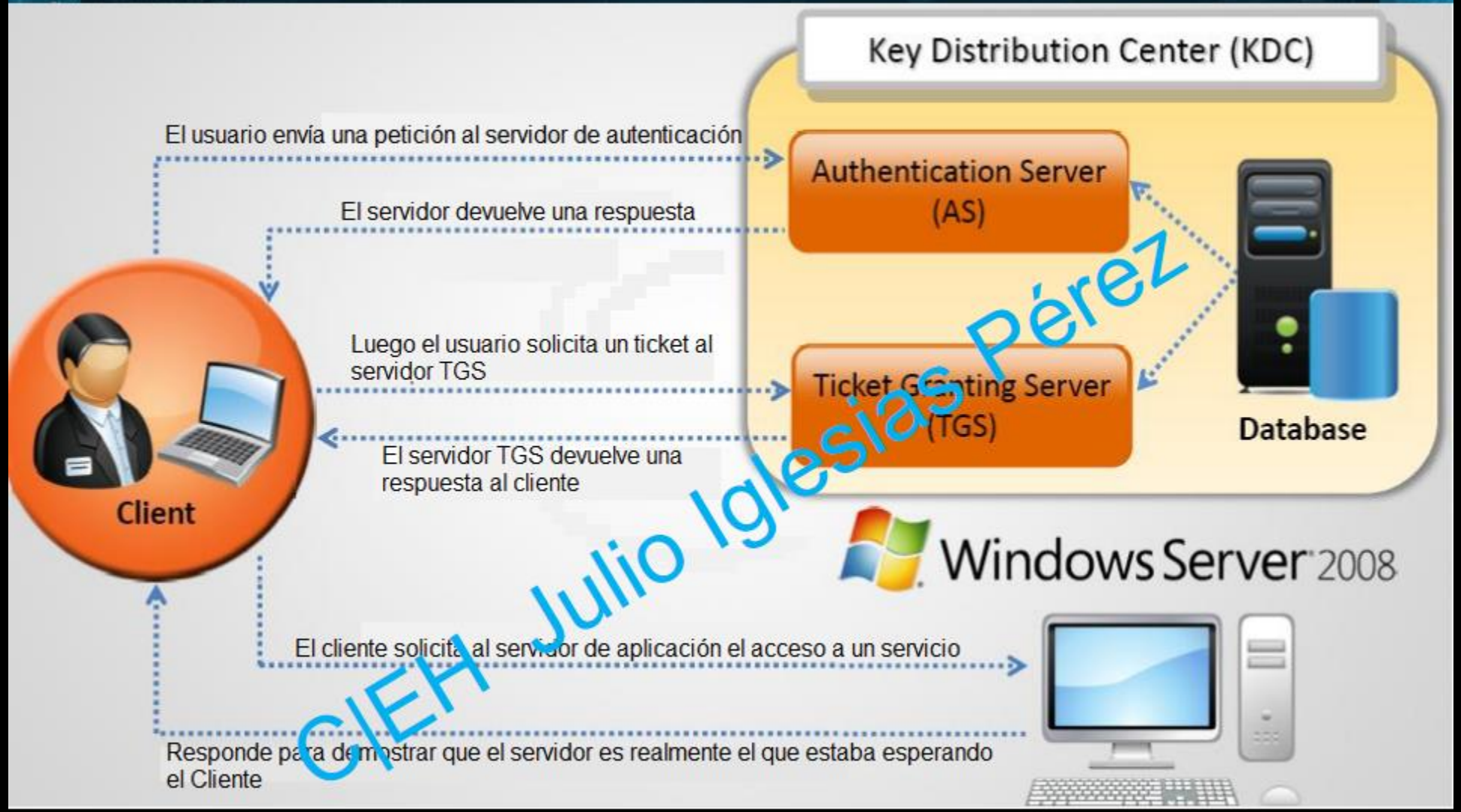
NTLMv2

NTLMv2 es una protocolo de autenticación challenge/response que mejora la seguridad sobre LM.

Autenticación Kerberos

El usuario y la contraseña nunca salen del sistema. Trabaja con Tickets, si el TGT (Ticket Granting Ticket) es descifrado de manera correcta, probamos que tenemos el password.

Trabaja de la siguiente manera:


Key Distribution Center (KDC)
El usuario envía una petición al servidor de autenticación
Authentication Server (AS)
El servidor devuelve una respuesta
Luego el usuario solicita un ticket al servidor TGS
Ticket Granting Server (TGS)
El servidor TGS devuelve una respuesta al cliente
Client
Database
Windows Server 2008
El cliente solicita al servidor de aplicación el acceso a un servicio
Responde para demostrar que el servidor es realmente el que estaba esperando el Cliente
CIEH Julio Iglesias Pérez

Crackeadores

- L0phtCrack es el primer crackeador de contraseñas de Windows y el mas conocido.
- Ophcrack es un boot cd que también crackea contraseñas
- Cain&Abel es una excelente herramienta entre las que cuenta cracking passwords.
- RainbowCrack genera las rainbowtables.
- KerbCrack intenta obtener los tickets de Kerberos capturándolos.

Directiva NOLMHash

LM Hash puede ser deshabilitado utilizando la directiva NoLMHash, o por registro o utilizando contraseñas de mas de 15 caracteres de longitud.

Sugerencia para contraseñas

Las contraseñas se sugieren que sean de 8 a 12 alfanuméricas combinando con símbolos. No utilizar las mismas contraseñas para varias cosas. Cambiar las contraseñas al menos cada 30 días. etc.

Escalada de Privilegios

Si un atacante obtiene acceso a la red utilizando una cuenta no administrativa, el próximo paso será obtener privilegios administrativos. A esto se lo denomina escalar privilegios.

StickyKeys

StickyKeys es una característica de accesibilidad para Windows. Si presionamos 5 veces la tecla SHIFT aparecerá esta característica que se encuentra en c:\Windows\system32\sethc.exe

Si remplazamos este archivo con cmd y lo renombramos nuevamente a sethc.exe y presionamos 5 veces la tecla shift, aparecerá una consola con privilegios administrativos.

Microsoft la corrigió

Admin User

Si creamos un usuario: net user Juggyboy Password y luego vamos al registro hasta HEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Special Accounts\Userlist

Creamos un nuevo DWORD value, escribimos el nombre del valor "Juggyboy" y cerramos el editor.

Juggyboy será un usuario con privilegios administrativos.

Usuario del dominio

1. El atacante infecta el equipo local de la víctima con un keylogger.
2. La víctima inicia sesión con sus credenciales del dominio.
3. El keylogger envía las credenciales al atacante.
4. El atacante obtiene acceso al dominio.

¿Cómo defenderse contra la escalada de privilegios?

Para protegernos de la escalada de privilegios podemos utilizar técnicas de encriptación, parchar los sistemas regularmente, correr los servicios con cuentas sin privilegio, implementar autenticación y autorización milti-factor, ejecutar las aplicaciones con privilegios mínimos, restringir los inicios de sesión con privilegios.

Ejecutando aplicaciones

Los atacantes ejecutan aplicaciones maliciosas para "adueñarse" del sistema.

Alchemy Remote Excecutor es un sistema de administración que permite ejecutar programas en equipos remotos, se ejecuta en múltiples equipos simultáneamente.

Otros: RemoteExec, Execute This!

Keylogger

Son programas o dispositivos de hardware que monitorean cada pulsación de tecla que el usuario realiza en el teclado; luego registra dicha actividad en archivos o los transmite a localidades remotas.

Wifi keyloggers, bluetooth, dentro del teclado, etc.

Spywares

Reducen el rendimiento del sistema, conecta a sitios porno remotos, accesos remotos maliciosos, roba información del usuario, monitorea la actividad del usuario, redirige a webs, cambia el sitio por defecto del usuario y evita que el usuario lo restaure, agrega múltiples marcadores a los navegadores, hace un decremento en el rendimiento general del sistema.

Tipos de spyware: Celulares, gps, audio, usb, salvapantallas, escritorio, mail, child monitoring, video, print.

Un ejemplo de Spyware de escritorio es el: Activity Monitor

"Child Monitoring"Spyware

Controla y supervisa como su hijo utiliza la PC e Internet. Bloquea cualquier web inapropiada utilizando keywords. Monitorea actividades. Graba actividades.

"Child Monitoring"Spyware

- Los video spyware graba no solo la pantalla si no también desde la webcam
- Los print spyware monitorea archivos a ser impresos en impresoras remotas.
- Los Telephone y Cellphone Spyware. los atacantes lo instalan en los dispositivos y estos envían secretamente datos al atacante como sms o mails.
- GPS spyware determina la locación de una persona o vehículo.

Cómo protegerse de los spywares

- Ajustar las opciones de configuración del navegador a medio.
- Mejorar el nivel de seguridad del equipo.
- Sospechar de correos y sitios.
- Instalar antispywares.
- Realizar navegación segura.
- Actualizar software con regularidad.
- Actualizar las definiciones de los antivirus.

Herramientas antispyware

- Spyware Doctor
- CounterSpy
- SpyHunter
- Kaspersky Internet Security
- Etc.

Rootkits

Puede remplazar archivos, intercepta las llamadas del S.O. por ej. en Linux podría dar acceso root.

En Windows podría hacerse pasar por controladores.

Estos mantienen el acceso al sistema a los atacantes.

Tipos de Rootkits

- Hypervisor Level: Modifica la secuencia boot para cargarse a si mismos en cuenta de un equipo virtual
- Kernel Level: Agrega código malicioso al Kernel.
- Application Level: Remplaza la aplicación con un troyano o modifica el comportamiento de una aplicación existente.

Tipos de Rootkits

- Hardware/Firmware: Se esconde en dispositivos o firmwares donde no se inspecciona el código.
- Boot Loader Level: Remplaza el boot original con uno controlador remotamente por un atacante.
- Library Level: Remplaza las llamadas originales del sistema con falsas para esconder información acerca del atacante.

¿Cómo defenderse contra Rootkits?

- Reinstalar la aplicación o S.O. desde una fuente segura.
- Tener procedimientos documentados de instalación automatizada.
- Instalar firewalls.
- Utilizar autenticación fuerte.
- etc.

Anti Rootkits

- RootkitRevealer
- McAfee Rootkit Detective
- Sophos Anti-Rootkit
- F-Secure BackLight
- Etc.

Flujo de datos NTFS alternativos

Son flujos escondidos que contienen metadatos.

Estos archivos son detectados por los antivirus pero no por el ojo humano.

Para crear NTFS Streams notepad archivo.txt:tigre.txt

Luego ejecutar notepad archivo.txt:tigre.txt modificar el archivo y luego de guardarlo apreciará que el archivo archivo.txt está en

blanco, para poder verlo habría que abrir el archivo con toda la cadena.

Manipulación de flujo de datos NTFS

Se pueden manipular los contenidos, por ej:

type c:\trojan.exe > c:\Readme.txt:Trojan.exe

Para ejecutarlo: c:\start c:\Readme.txt:Trojan.exe

Para extraerlo: cat c:\Readme.txt:Trojan.exe > trojan.exe

Nota: cat es un recurso de Windows Server 2003

¿Cómo defenderse contra los NTFS Data Stream?

- Al mover a particiones FAT los streams se borran.
- También utilizar LSN.exe para detectarlos.

Esteganografía

Consiste en esconder un archivo dentro de otro, generalmente uno muy pequeño dentro de uno grande, y luego extraerlo.

Tipos: imágenes, documentos, carpetas, video, audio, web, mail, dvd, txt, etc.

Un ejemplo de Stegano es la herramienta Invisible Secrets 4 para esconder archivos dentro de imágenes.

Para detectar se puede utilizar el Stegdetect.

Esteganografía

- Aunque no es un algoritmo de cifrado en sí, la esteganografía es una gran manera de enviar mensajes de ida y vuelta a otros sin siquiera darse cuenta. Es la práctica de esconder un mensaje dentro de otro medio (como otro archivo o una imagen) de tal manera que sólo el remitente y el destinatario siquiera saben de su existencia.

Ejemplo de uso

gifshuffle [-CQS1] [-p passwd] [-f archivo | -m mensaje] [infile.gif [outfile.gif]]

gifshuffle -C -m "Soy Ethical Hacker" -p Pa$$w0rd CEH.gif hacker.gif

- Para extraer

gifshuffe -C -p Pa$$w0rd hacker.gif

http://www.darkside.com/gifshuffle/index.html

Herramientas estenográficas de imagen

- SNOW
- Hermetic Stego
- ImageHide
- QuickStego
- gifshuffle
- OutGuess
- Etc.

Herramientas estenográficas de video

- Masker
- Max File Encryption
- Xiao Steganography
- Etc.

Herramientas estenográficas de documentos

- wbStego
- Merge Streams
- Office XML
- Etc.

Herramientas estenográficas de audio

- Mp3stegz
- MAXA Security Tools
- Stealth Files
- Audiostegano
- Etc.

Herramientas estenográficas de directorios

- Invisible Secrets 4
- StegoStick
- QuickyCrypto
- Max Folder Secure
- Etc.

Detección de Esteganografía

- Stegdetect
- Xstegsecret
- Stego Watch
- StegAlyzerAS
- Etc.

Escondiendo Huellas

La idea es volver al sistema. Hay que manipular los archivos de registro (logs)

1. SECEVENT.EVT (security). Logins fallidos, acceso a archivos sin privilegios
2. SYSEVENT.EVT (system). Falla de drivers, cosas que no operan correctamente
3. APPEVENT.EVT (applications). El atacante no querrá borrar todo el log, solo manipularlo.

Borrando las pistas online

Borrar la MRU (Most Recently Used). Borrar cookies, cache, deshabilitar autocompletar, borrar las barras de herramientas de los navegadores.

Deshabilitando la auditoría

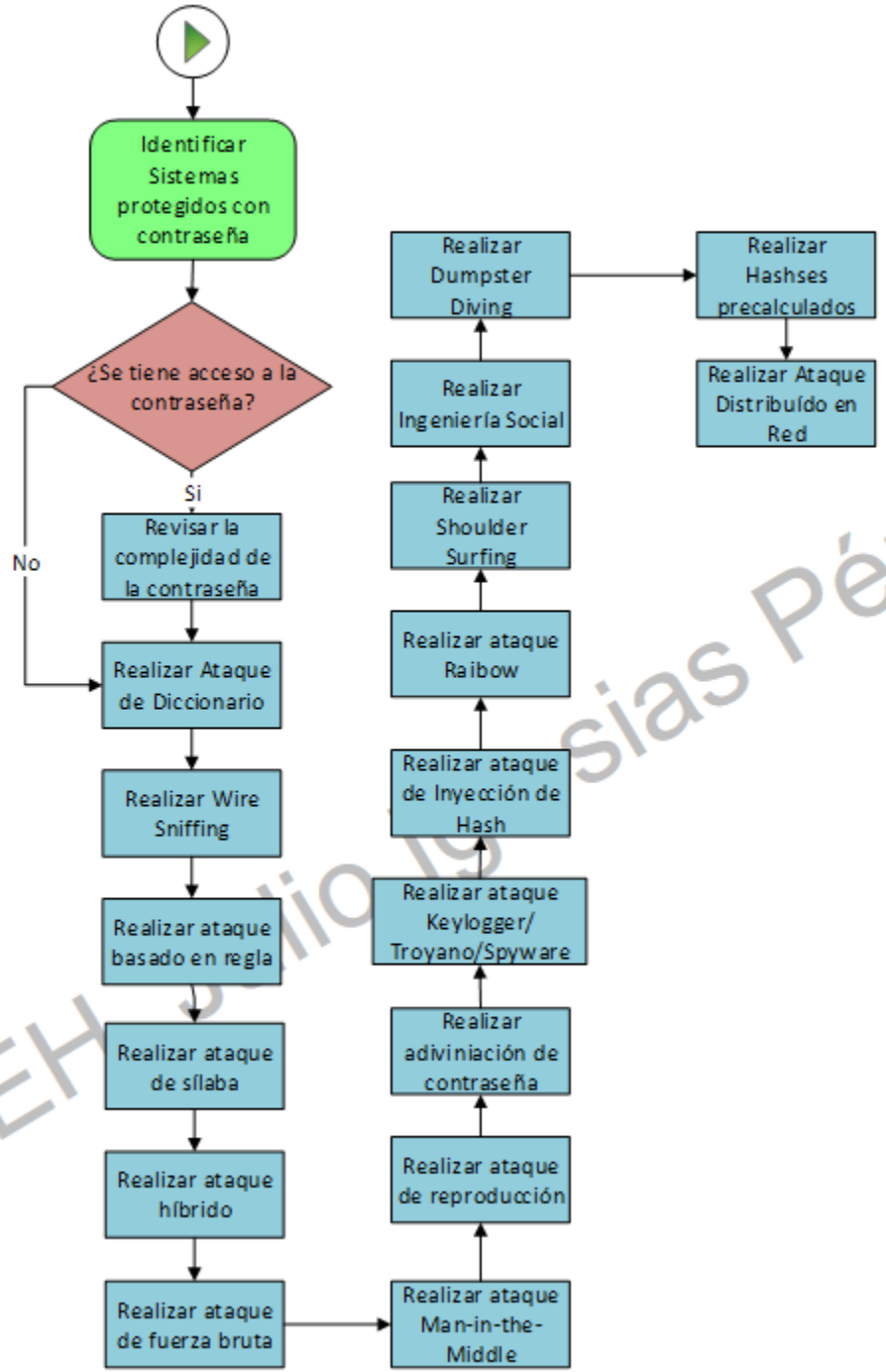
Los intrusos deshabilitaran la auditoria inmedíatamente después de obtener acceso administrativo. Luego de su estadía, la volverán a encender.

auditpol.exe /enable | /disable

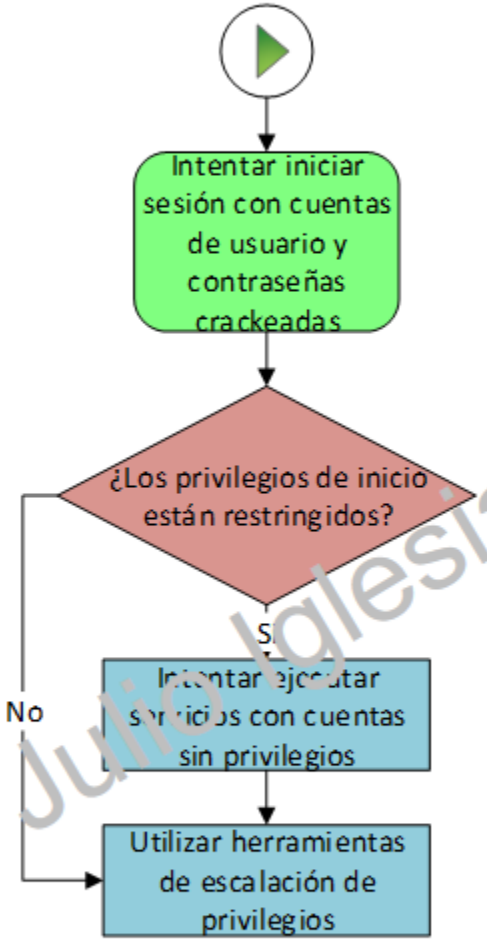
Herramientas para esconder huellas

- Window Washer
- Tracks Eraser Pro
- Evidence Eliminator
- Armor Tools
- Clear My History
- Etc.

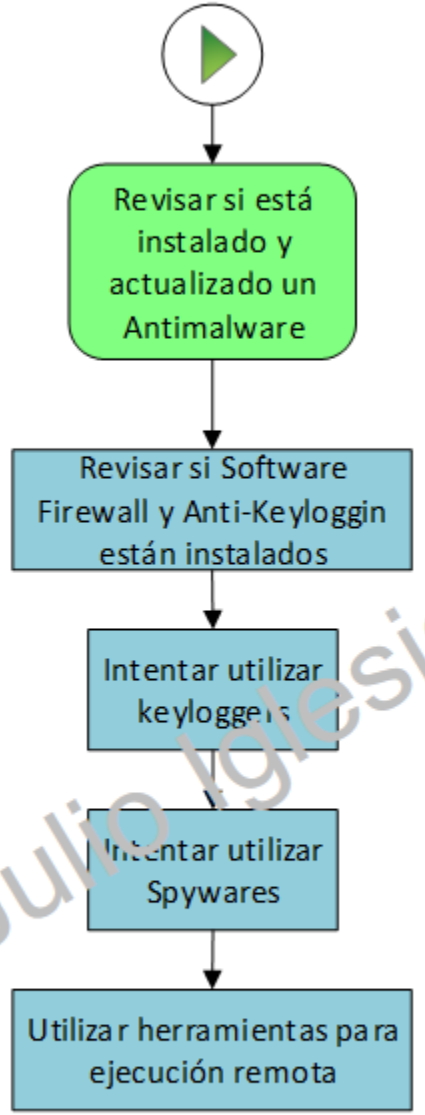

Test de Intrusión Password Cracking
C|EH
Julio



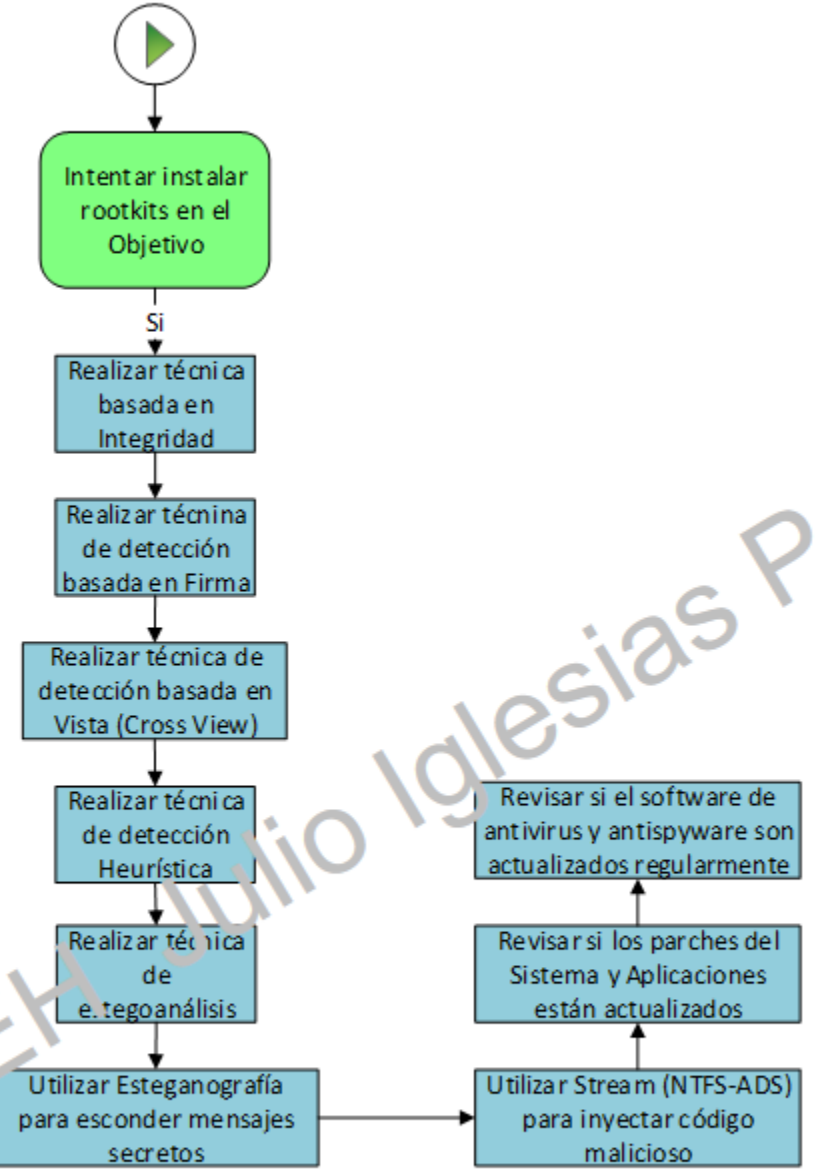

Test de Intrusión para
Escalada de Privilegios

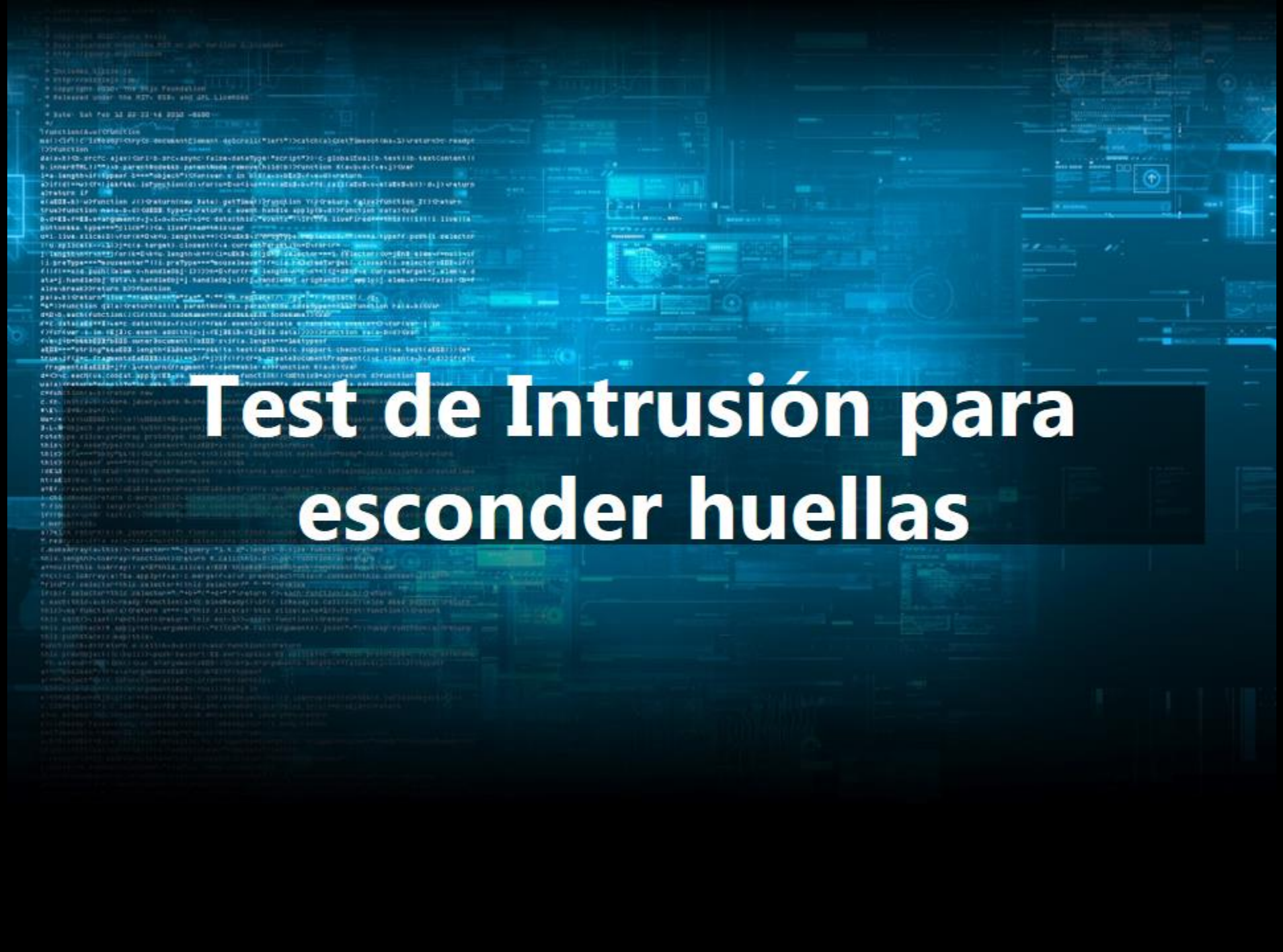


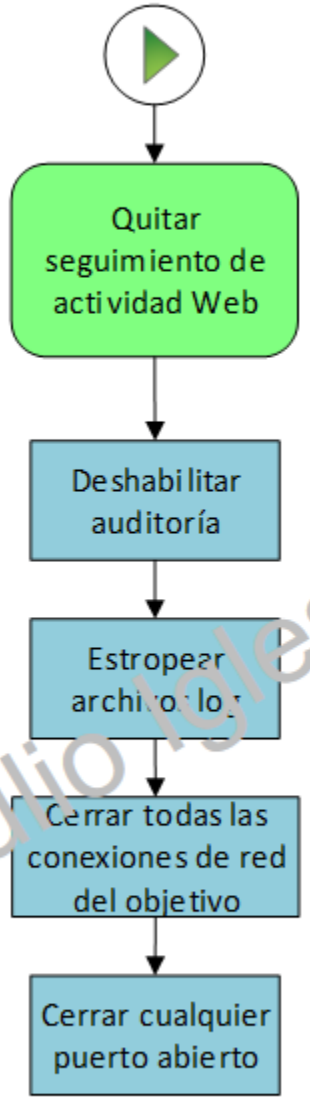
Test de Intrusión para ejecución de aplicaciones




Test de Intrusión para
esconder archivos




Test de Intrusión para
esconder huellas




¡Muchas Gracias!
C|EH Julio Iglesias Perez