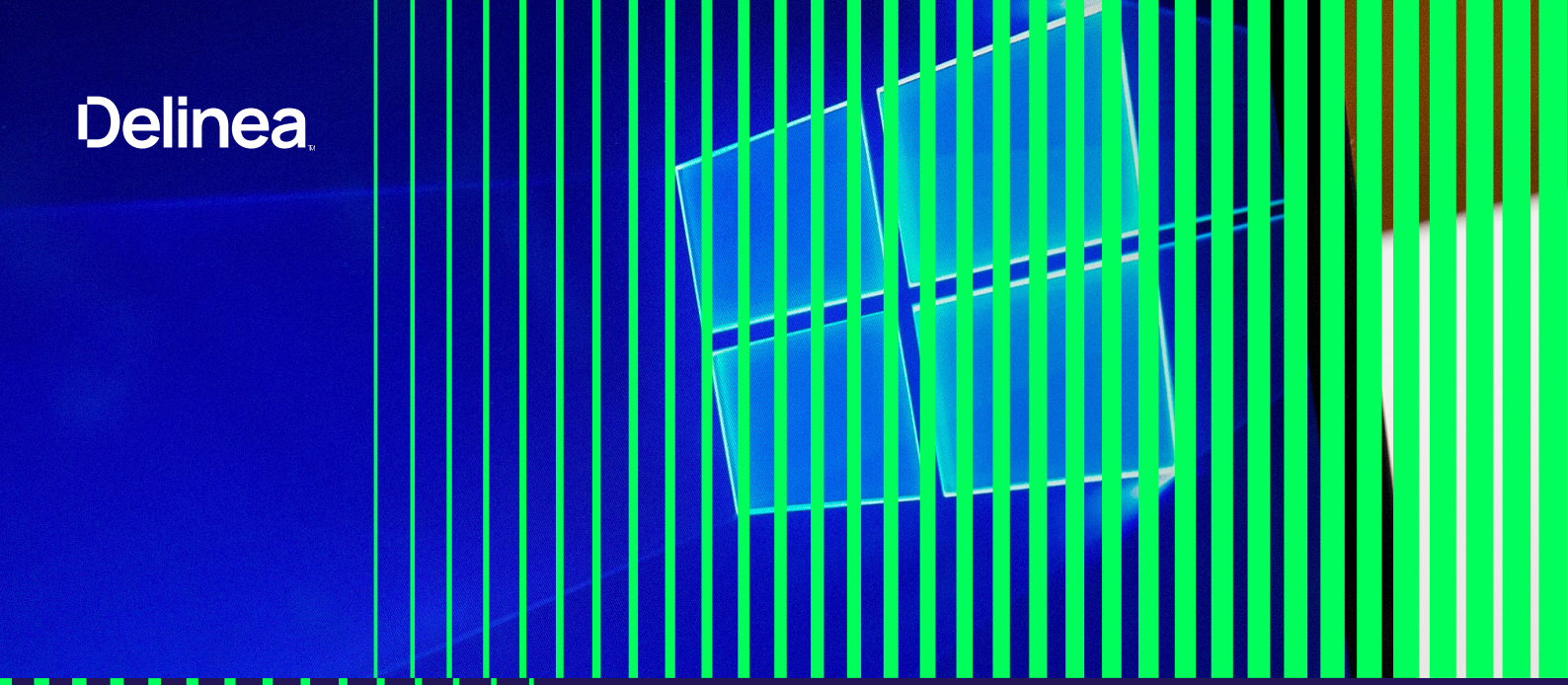
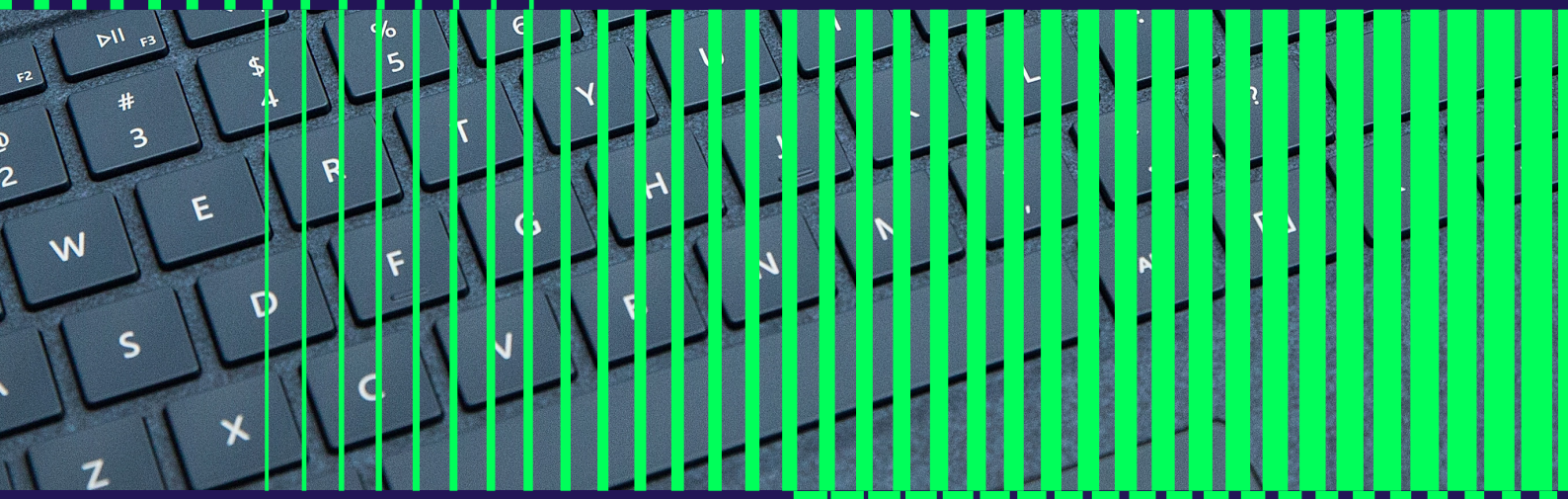
Delinea



¿Cómo de seguros son tus endpoints?

Guía del hacker ético para la protección de equipos Windows



DOCUMENTO TÉCNICO

¿Cómo de seguros son tus endpoints?

Guía del hacker ético para la protección de equipos Windows

Para proteger los equipos Windows contra ataques informaticos, es útil pensar como un ciberdelincuente. Los hackers malintencionados buscan la forma más barata, rápida y sigilosa de lograr sus objetivos. Los equipos Windows brindan muchas oportunidades para obtener acceso a entornos de TI e información confidencial.

La comunidad de hacking ético ha creado numerosas herramientas y técnicas para ayudar a las organizaciones a proteger mejor sus entornos Windows.

En este documento, aprenderás estrategias y recursos que los hackers éticos utilizan en cada etapa de un ataque:

Armado con este conocimiento, podrás realizar un ataque ético para probar las defensas de tu propia organización. Lo más importante es que también aprenderás estrategias de seguridad de endpoints que impiden que los hackers malintencionados alcancen sus objetivos.

PASO 0 | Actividad previa

El primer paso en un hack ético es determinar los objetivos, el objetivo y el alcance de las actividades. Debes asegurarte siempre de no causar daños. Asegúrate de que tu plan cumpla con un código ético y se mantenga dentro de los límites legales.

Confirma que tienes permiso de la organización para ejecutar cualquier herramienta de piratería que vayas a utilizar. ¿Se te permite establecer a empleados como objetivos, o solo a sistemas y aplicaciones? Por lo general, esto depende del nivel de simulación buscado con respecto a un ataque real.

Si tu organización tiene un entorno de laboratorio, prueba allí tu conjunto de herramientas antes de comenzar el hackeo activo. Si tus acciones activan alguna alarma, sabrás que los controles de seguridad están haciendo su trabajo. De lo contrario, puede haber errores de configuración.

PASO 1 | Reconocimiento pasivo

El siguiente paso es crear tu ruta de ataque. Es increíble cuánto reconocimiento pasivo se puede hacer con información disponible públicamente.

La inteligencia de código abierto (OSINT) es fundamental para cualquier evaluación de riesgos de la seguridad de una empresa, especialmente para el bastionado de sistemas y dispositivos. Con OSINT, un ciberdelincuente puede obtener información disponible públicamente para obtener acceso. Cuanta más información recopiles, mejor preparado estarás.

Durante OSINT, el reconocimiento pasivo utiliza dos pasos:

- **Reconocimiento físico.** Esto podría significar permanecer cerca de la oficina del objetivo o mirar por las ventanas, tratando de recopilar información sobre controles de seguridad, vigilantes, lectores de credenciales, vallas y cualquier otro control físico de seguridad. Puedes intentar identificar la información de los empleados, como nombres, cargos, tipos de credenciales, modelos de teléfonos, modelos de portátiles y, tal vez, incluso intentar tomar una foto de alta definición.
- **Reconocimiento en línea, mediante investigación e ingeniería social.**
  Puedes crear un organigrama de una estructura organizativa a partir de las redes sociales. Las ofertas de trabajo que incluyen las habilidades requeridas pueden revelar las herramientas que utiliza la empresa, como versiones de sistemas operativos, aplicaciones e incluso soluciones de seguridad. También puedes recopilar logotipos, formatos de correo electrónico, plantillas corporativas, pies de página/firmas de correo electrónico y números de teléfono a través de información disponible públicamente.

Herramientas comunes para reconocimiento pasivo

WHOIS: búsqueda de nombres de dominio

Way Back Machine: archivo de Internet

Shodan: motor de búsqueda de dispositivos conectados a Internet

theHarvester: herramientas OSINT para correos electrónicos, nombres, subdominios, IP y URL

DIG: consulta DNS

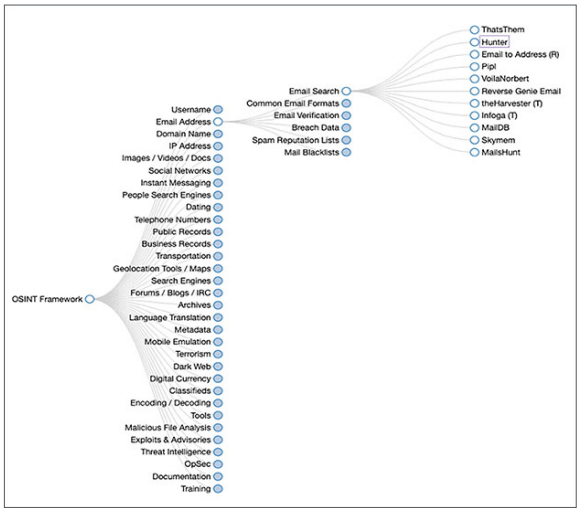
dnsenum: script de enumeración de dominios

nslookup: búsqueda de servidor de nombres para consultar DNS

Algunos recursos increíbles de ingeniería social y OSINT incluyen:

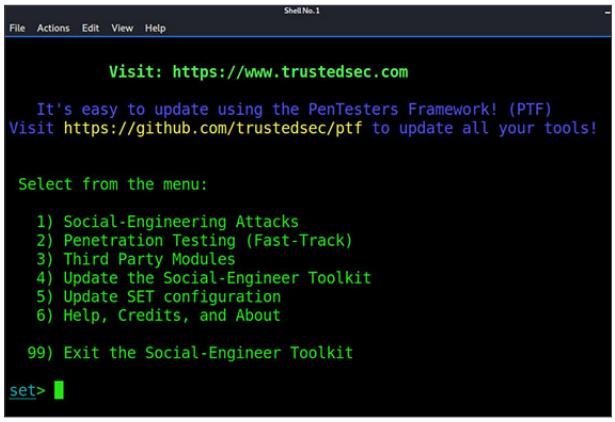
Marco OSINT, centrado en recopilar información de herramientas o recursos gratuitos.

Figura 1 - Marco OSINT



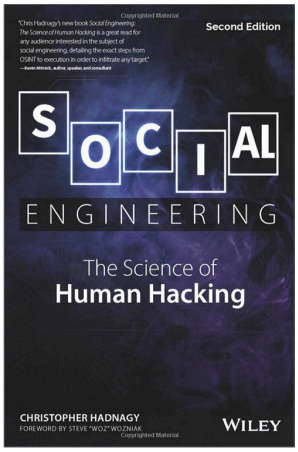
The Social-Engineer Toolkit (SET), de Dave Kennedy, fundador de TrustedSec.

Figura 2 - Conjunto de herramientas de ingeniería social de TrustedSec



Ingeniería social: la ciencia del hacking humano, 2.a edición, por Christopher Hadnagy.

Figura 3 - Ingeniería social: la ciencia del hackeo humano



Antes de continuar, compruebe siempre los nombres de host, los nombres de dominio, las direcciones IP y todo lo demás que haya recopilado durante la determinación del alcance o OSINT. ¡Lo último que desearía es realizar un hackeo ético contra la empresa equivocada (lo cual, sinceramente, no es ético)!

CONSEJOS: Cómo protegerse contra OSINT

Mira tu organización a través de la lente de la inteligencia de código abierto para bloquear o desviar a los atacantes.

- **Limita la información pública.** Asegúrate de que tu equipo de talento no divulgue información, como el software de seguridad que utiliza, en un sitio web público. Si es necesario, deben ser lo menos precisos posible y solo revelar los proveedores o los datos de la versión durante una entrevista en persona.
- **Coloca trampas.** Deja rutas de navegación, como direcciones de correo electrónico divulgadas intencionalmente. El uso de honeypots o tecnologías de engaño puede alertarte sobre intentos de OSINT.
- **Trabaja con probadores abiertos externos.** Realiza ingeniería social y recopilación de OSINT.
- **Forma a los empleados.** Los empleados están en la primera línea de la protección de tu organización. Enséñales a protegerse en el trabajo y en su vida personal. Por ejemplo, es habitual que los empleados se hagan un selfie mientras almuerzan o se reúnen con el equipo. Asegúrate de que sepan verificar lo que hay en segundo plano, como contraseñas en pizarras, información confidencial, ID de reuniones de Zoom e información de credenciales.
- **Capacita a los empleados.** Los empleados no deben tener miedo de informar sobre incidentes o pedir consejo. Cuanto más se comuniquen, antes podrás identificar posibles ataques.

PASO 2 | Reconocimiento activo

Esta fase también se conoce como «tocar puertas y ventanas». Esas puertas y ventanas pueden ser servidores públicos, aplicaciones, servidores web, endpoints de Windows y empleados. Busca vulnerabilidades y configuraciones incorrectas para lograr un punto de apoyo inicial.

Escaneo y enumeración de puertos

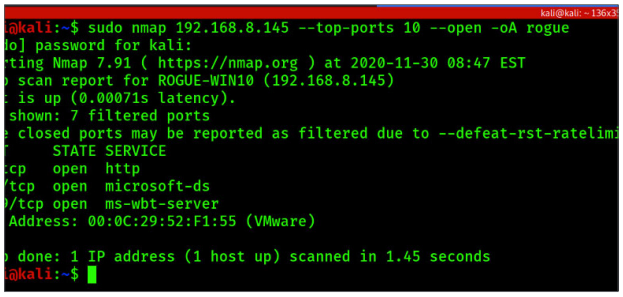
Una de las herramientas de enumeración de puertos y escaneo más populares es nmap, también conocida como Network Mapper. Nmap es extremadamente poderosa. Esta utilidad gratuita de código abierto se utiliza para escanear, descubrir redes y realizar auditorías de seguridad.

A continuación, se muestran ejemplos de opciones de enumeración de puertos y escaneo predeterminadas.

El escaneo de puertos rápido

nmap <ip> –top-ports 10 –open -oA <host>

- <ip> = dirección IP o rango de IP de los objetivos para escanear
- –top-ports <número> = introduce el número de puertos más comunes para escanear
- –open = solo muestra puertos abiertos en la salida
- -oA = genera todos los formatos
- <host> = nombre del archivo para la salida

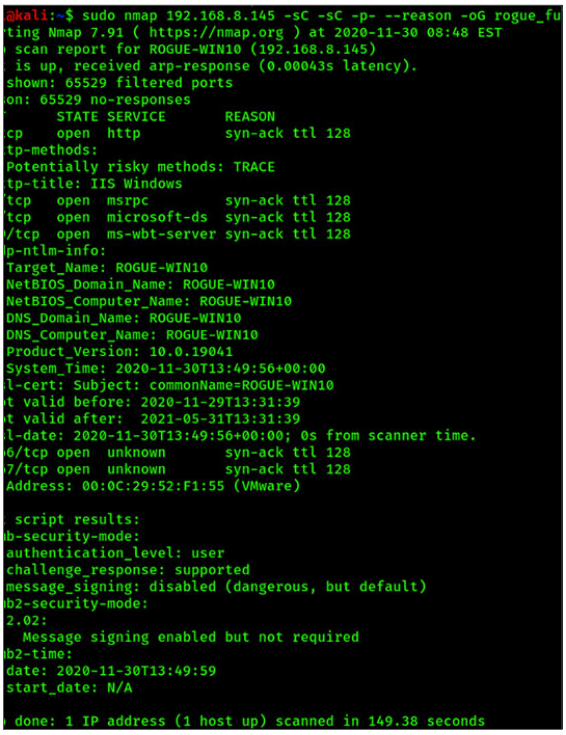


El escaneo de puertos completo

Esto puede tardar algún tiempo en ejecutarse. No olvide también los puertos UDP.

nmap <ip> -sV -sC -p- –reason -oG <host_full>

- <ip> = dirección IP o rango de IP de los objetivos para escanear
- -sV = sondea puertos para determinar información de servicio/versión
- -sC = ejecuta scripts predeterminados (consulta la guía de referencia de nmap)
- -p- = escanea todos los puertos
- –reason = muestra el motivo de la salida del puerto
- -oG = salida solo en formato greppable
- <host_full> = nombre del archivo para la salida



Otras opciones comunes:

- -T4 = plantilla de sincronización para usar T<0-5> (cuanto más alto, más rápido)
- -A = habilita la detección de sistema operativo, versión, escaneo de scripts y traceroute
- -O = detección del sistema operativo
- -sU = escaneo UDP
- -sS = escaneo TCP SYN

Otras herramientas comunes de recopilación, escaneo y enumeración de información incluyen:

- Netdiscover: herramienta de reconocimiento de arp activo/pasivo
- Zenmap: GUI para nmap
- Netcat: herramienta de red
- Masscan: el escáner de puertos de Internet más rápido
- Legion: reconocimiento y escáner automatizados con cientos de integraciones
- Dmitry, también conocido como herramienta de recopilación de información Deepmagic

A partir del escaneo inicial y la enumeración de puertos en los ejemplos anteriores, puedes determinar lo siguiente:

- Es un sistema operativo Windows.
- Ttl en 128 confirma que es Windows.
- Es una máquina virtual que se ejecuta en VMWare según la dirección MAC.
- El nombre del host es ROGUE-WIN10, lo que podría significar que es una versión de Windows 10.
- Escritorio remoto está disponible.
- RDP confirma la versión de Windows 10.0.19041.
- Tiene versión SMB 2.

También tienes información sobre puertos:

- Puerto 80: endpoint de Windows que ejecuta un servidor web
- Puerto 135: RPC de Windows
- Port 445 – Server Message Block (SMB)
- Puerto 3389: Microsoft Terminal Server (RDP) registrado oficialmente como terminal basado en Windows (WBT)

Esta información muestra algunas áreas potenciales de riesgo. El endpoint ejecuta un servidor web, lo que podría significar sitios web potencialmente mal configurados. Tiene SMB habilitado, que, si no está parcheado, podría estar expuesto al exploit Eternal Blue. El puerto RDP 3389 podría permitir a un atacante utilizar fuerza bruta si el usuario utiliza una contraseña conocida o débil. El Protocolo de escritorio remoto (RDP) que se ejecuta en el puerto 3389 permite una conexión gráfica remota al endpoint de Windows, que anteriormente se sabía que tenía vulnerabilidades como BlueKeep (CVE-2019-0708).

Durante la pandemia, se ha producido un aumento en el número de puertos RDP descubiertos. Con el aumento de empleados que trabajan de forma remota, los endpoints de Windows que nunca habrían salido de la oficina ahora son de dominio público, también conocido como el Internet salvaje de las cosas conectadas. En la oficina, los endpoints normalmente estarían protegidos por el firewall corporativo. Cuando se trasladan a la Internet pública, esos puertos quedan expuestos. Si esos endpoints no tienen un firewall basado en host, lo más probable es que estén siendo escaneados activamente en busca de puertos abiertos utilizando los métodos anteriores.

CONSEJOS: Cómo protegerse contra el reconocimiento

- **Aplica parches y actualizaciones.** Concéntrate en la ejecución remota de código o CVE de alto riesgo para priorizar los parches.

  La gestión de parches suele ser una historia interminable que suele verse así:

  - Martes de parches
  - Miércoles de pruebas
  - Jueves piloto
  - Viernes de despliegue
  - Sábado de dolores
  - Domingo de reversión
  - Lunes de reaplicación de parches
  - Martes de parches

- **Desinstala o deshabilita aplicaciones y puertos no utilizados.** Cuantas menos aplicaciones y servicios se ejecuten en endpoints de Windows, menos objetivos habrá. Con menos cosas que revisar, más difícil es el proceso para un atacante y más riesgos está dispuesto a asumir, lo que aumenta la posibilidad de descubrimiento.

  Utiliza una autenticación fuerte. Utiliza frases de contraseña seguras, autenticación multifactor y seguridad en accesos privilegiados. Nunca permitas que una contraseña sea la única seguridad entre un atacante y tus endpoints de Windows.

- **Conoce qué puertos se están ejecutando.** Escucha las conexiones en tu entorno. Escanea y comprende activamente los riesgos de cada una de ellas.

PASO 3 | Enumeración del servicio

En este punto del proceso de piratería, ya tienes una idea de qué se está ejecutando en el sistema Windows; ahora quieres confirmar y ver si algo sirve como punto de apoyo inicial. Elabora un plano detallado sobre el objetivo y el entorno.

El primer puerto que hay que verificar es el puerto 80, el servidor web IIS. Para hacer esto, ejecuta curl en la dirección IP:

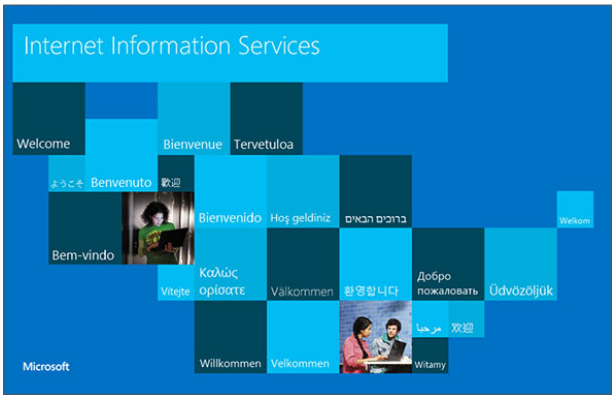
-i = incluir la respuesta del protocolo en el encabezado

```
i@kali:~$ curl -i 192.168.8.145
P/1.1 200 OK
tent-Type: text/html
t-Modified: Mon, 30 Nov 2020 13:45:48 GMT
ept-Ranges: bytes
g: "80c7321c1fc7d61:0"
ver: Microsoft-IIS/10.0
e: Mon, 30 Nov 2020 14:16:38 GMT
tent-Length: 696

OCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dt
ml xmlns="http://www.w3.org/1999/xhtml">
ad>
ta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
tle>IIS Windows</title>
yle type="text/css">
-
y {
    color:#000000;
    background-color:#0072C6;
    margin:0;
```

La respuesta muestra que la versión es IIS/10.0, lo que confirma que se trata de un endpoint de Windows 10. La respuesta también es típica de la página web predeterminada de IIS, que se puede mostrar a continuación. Esto indica que:

- El sistema acaba de ser aprovisionado y debe ser un servidor web, pero aún no se ha configurado.
- Estaba malconfigurado.
- Se ha eliminado un sitio web.
- También podría estar ejecutándose en otro puerto.



Algunas de las herramientas de enumeración de servicios más comunes incluyen:

- rpcclient : herramienta para ejecutar funciones MS-RPC del lado del cliente
- netcat: potente herramienta de red
- nbtscan: herramienta para escanear NetBIOS y encontrar recursos compartidos abiertos
- smbclient: cliente para comunicarse con servidores SMB/CIFS
- Metasploit: marco de pruebas de penetración
- WFUZZ: Fuzzer de aplicaciones web
- DIRB: escáner de contenido web
- GOBUSTER: escáner de objetos web
- NIKTO: escáner de vulnerabilidad web

Investigación de vulnerabilidades

Determina las mejores opciones para tu ruta de ataque, basándote en:

- No causar daños
- Velocidad
- Sigilo
- Recursos
- Tiempo
- Coste
- Disponibilidad

Algunas herramientas que te ayudarán a investigar las opciones son:

- Google-Fu
- exploit-db
- Common Vulnerabilities and Exposures (CVE)
- Searchsploit
- MITRE ATT&CK®

Determina la ruta de acceso inicial, como por ejemplo:

- Vulnerabilidades de hardware, sistema operativo o aplicaciones de acceso público
- Suplantación de identidad
- USB drops
- Cadena de suministro y terceros
- Credenciales débiles o predeterminadas
- A través de Wi-Fi

CONSEJOS: Cómo reducir tu superficie de ataque

- **Configura la protección antivirus y contra malware.** Esto puede proteger a los usuarios de amenazas conocidas.
- **Ejecuta análisis de vulnerabilidades.** Los análisis periódicos ayudan a encontrar configuraciones incorrectas en aplicaciones, sistemas y software sin parches. Integra tu escáner de vulnerabilidades en una solución PAM para asegurarte de tener credenciales para escanear los sistemas por completo y obtener una visión completa de tu superficie de ataque. Asegúrate de que todos los dispositivos USB estén escaneados correctamente.
- **Crea varias capas de red y segmentación.** Las estrategias de defensa en profundidad limitan la capacidad del atacante para moverse. Crea bloqueadores entre diferentes redes para aplicaciones, servicios, servidores de producción, almacenes seguros de datos, sistemas operativos, dispositivos de los empleados tanto administrados como personales (BYOD). BYOD, que hoy en día se parece más a llevarse la casa a cuestas que un simple dispositivo, a veces, es la receta para el desastre.
- **Forma a los usuarios.** Documenta y comparte políticas de seguridad. Realiza formaciones periódicas en materia de seguridad enfocadas a amenazas concretas.
- **Contraseñas seguras.** Acostumbra a los empleados a utilizar una solución PAM. Reduce una de las principales causas de la fatiga cibernética automatizando la creación y rotación de contraseñas. Garantiza la complejidad de las contraseñas y la integración con SSO y MFA.
- **Controla el acceso de la cadena de suministro y de terceros.** Adopta un enfoque de privilegios mínimos y confianza cero para el acceso de terceros. Obliga a terceros a acceder a través de una solución PAM para saber quiénes son, qué harán y qué aprobaciones se requieren antes de que se les permita el acceso.

PASO 4 | Vulnerabilidad del acceso

Hay muchas posibles rutas de ataque. Los dos más populares son los errores en el sistema operativo o las aplicaciones de Windows y las personas.

Errores en los sistemas operativos y aplicaciones de Windows

El software tiene errores. Los hackers éticos que participan en programas de recompensas por errores son recompensados por descubrirlos, y algunas empresas hacen negocio con su venta. Hay errores del kernel en los sistemas operativos y errores de aplicaciones que permiten a los atacantes utilizar el software de forma no deseada para obtener acceso inicial.

Con la transición digital a la virtualización, la computación en la nube y DevOps, ha habido un aumento en las configuraciones erróneas (generalmente debido a la seguridad no habilitada de manera predeterminada) que deja el acceso abierto para todos. Los mismos viejos métodos de seguridad que utilizas para las herramientas locales tradicionales ya no son suficientes.

Las mejoras significativas en la seguridad, el proceso de aplicación de parches y las vulnerabilidades menos frecuentes del kernel han hecho que Windows sea más difícil de explotar. Sin embargo, una vez que presenta usuarios y aplicaciones, la seguridad se debilita.

El mayor riesgo de seguridad para los endpoints de Windows es el uso de versiones heredadas. Si utilizas Windows 7/8, XP o todavía tienes Windows NT o Vista, tu seguridad es como un caramelo a la puerta de un colegio.

Al igual que los sistemas operativos, las aplicaciones tienen diferentes tipos y riesgos de seguridad. Muchos propietarios de aplicaciones tienden a instalar la predeterminada con todo marcado, lo que probablemente introduzca muchas funciones y errores.

Casi todos los exploits contra sistemas operativos y aplicaciones implican al menos uno de los siguientes elementos:

- SO heredado con exploits conocidos existentes
- Sistema sin parches con exploits conocidos existentes
- Credenciales débiles: SO y aplicaciones
- Credenciales predeterminadas: SO y aplicaciones
- Sistema mal configurado
- Sistema sin parches con exploits conocidos existentes
- Aplicación mal configurada
- Seguridad no habilitada

Para aplicaciones web, el OWASP Top Ten proporciona priorización de las vulnerabilidades más comunes:

1. Inyección
2. Autenticación rota
3. Exposición de datos confidenciales
4. Entidades externas XML
5. Control de acceso roto
6. Configuraciones erróneas de seguridad
7. Secuencias de comandos entre sitios (XSS)
8. Deserialización insegura
9. Uso de componentes con vulnerabilidades conocidas
10. Registro y supervisión insuficientes

Además, consulte las 25 debilidades de software más peligrosas CWE 2020 de MITRE.

Personas

Los usuarios están en primera línea. Están bajo el ataque de innumerables ciberdelincuentes. Simplemente decirles a los usuarios que «hagan clic en menos cosas malas» los deja solos ante las amenazas cibernéticas. Debemos trabajar juntos para hacer del factor humano un vínculo fuerte en la defensa de la ciberseguridad.

Los ciberdelincuentes intentan abusar de la confianza de las personas ofreciendo servicios aparentemente legítimos. Un clic en un hipervínculo podría instalar malware o ransomware. Una contraseña compartida podría proporcionar información y credenciales personales.

Si no puedes obtener acceso a través de un sistema operativo o una aplicación, recurre a los usuarios. Hay muchas maneras de hacer esto:

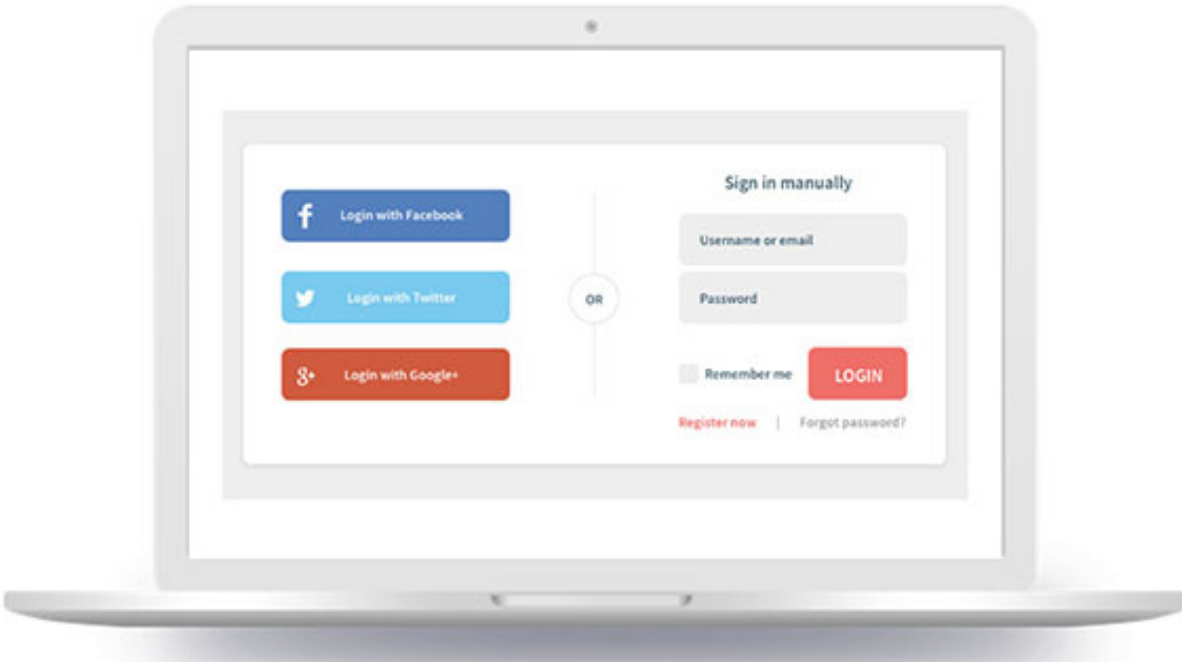
- Solicitar cortésmente la contraseña a los usuarios; algunos incluso la entregarán.
- Solicitar asistencia técnica para restablecer la cuenta de un usuario (es posible que Twitter/X la recuerde)
- Phishing por teléfono, también conocido como Vishing
- Phishing, fingiendo ser un servicio de Internet legítimo
- Conseguir que los usuarios instalen una actualización de software, también conocida como RAT (herramienta de acceso remoto)
- Portátiles desatendidos, especialmente si están conectados
- Ataque de hombre/mujer en el medio
- Usar una red o Wi-Fi no segura
- Contraseñas reutilizadas o débiles

Las campañas de phishing con éxito se aprovechan del miedo de las personas a perder dinero o tiempo. Por ejemplo, podría animar a las personas a hacer clic o iniciar sesión para ver:

- Multas por exceso de velocidad
- Multas de estacionamiento
- Seguro médico
- Información de salud
- Encuestas de TI
- Botones para cancelar suscripciones

Simplemente mostrar a las personas una pantalla de inicio de sesión les hace querer introducir sus credenciales.

El peor de los casos es cuando los usuarios se ejecutan como administrador local en sus endpoints de Windows. Entonces, el juego casi ha llegado a su fin.



CONSEJOS: Cómo protegerse contra la vulnerabilidad del acceso

No se lo pongas fácil a los atacantes. Las siguientes prácticas de refuerzo de Windows reducen el riesgo.

- **Aplica parches y actualizaciones de los endpoints y las aplicaciones de Windows con regularidad.** Elimina el software no utilizado y deshazte de tus sistemas operativos y aplicaciones heredadas. Si no puedes deshacerte de los sistemas heredadas, protégelos bien mediante el acceso a la red y controles de acceso privilegiados.
- **Utiliza protección antivirus y contra malware.** Da a los usuarios una oportunidad protegiéndolos de amenazas conocidas.
- **Contraseñas seguras.** Utiliza administradores de contraseñas y soluciones PAM.
- **Practica el principio de privilegios mínimos.** Asegúrate de que los usuarios no tengan privilegios excesivos. No permitas que los usuarios ejecuten sus sesiones como administradores locales en endpoints de Windows.
- **Usa el control de aplicaciones.** Permite únicamente que se ejecuten aplicaciones fiables. Evita que se ejecute software no deseado con privilegios elevados.

PASO 5 | Ampliación de privilegios

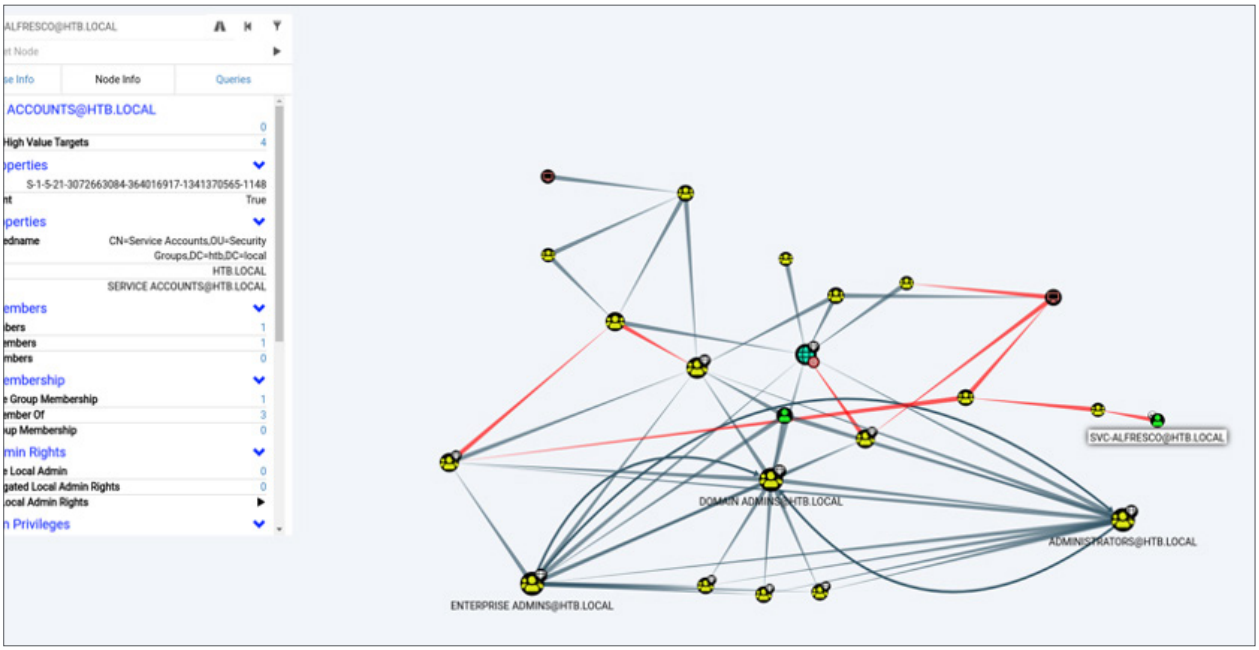
Todos los atacantes buscan cuentas privilegiadas. Estas cuentas les permiten entrar y salir cuando quieran mientras permanecen ocultos detrás de servicios y credenciales que parecen legítimos.

Los endpoints de Windows vienen con varios tipos de control de acceso: cuentas de usuario, cuentas de servicio y grupos. Cada uno de estos está delegado en una lista de control de acceso (ACL), que determina el acceso a los recursos del sistema, como archivos, carpetas, registros y servicios. Las cuentas más buscadas son las de administrador de dominio, administrador local, cuentas de servicio y cualquier cuenta incluida en el grupo Dominio local.

Para obtener acceso a cuentas privilegiadas, el siguiente paso en el proceso de hackeo es repetir la enumeración, esta vez como usuario interno en un endpoint de Windows. A continuación, se muestran herramientas para recopilar una enumeración de posibles escaladas de privilegios o movimientos laterales.

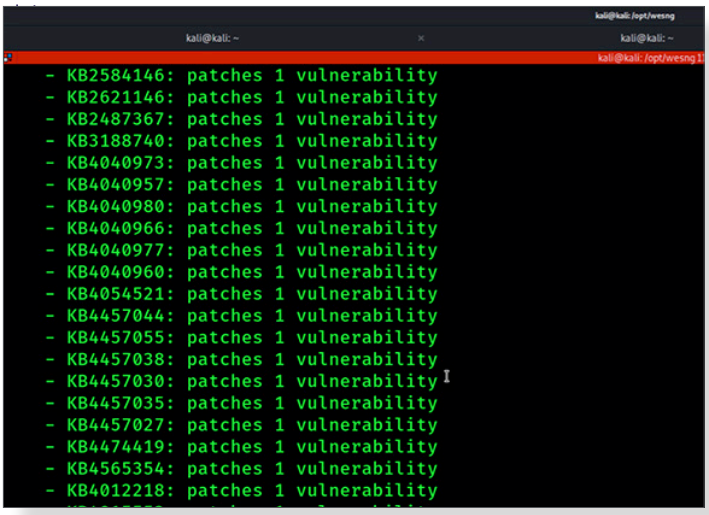
Bloodhound. BloodHound es una aplicación web Javascript de una sola página, desarrollada sobre Linkurious, compilada con Electron, con una base de datos Neo4j alimentada por un recolector de datos C#. Utiliza la teoría de grafos para revelar relaciones ocultas y, a menudo, no deseadas dentro de un entorno de Active Directory. Los atacantes pueden utilizar BloodHound para identificar fácilmente rutas de ataque altamente complejas que de otro modo serían imposibles de encontrar. Los defensores pueden utilizar BloodHound para identificar y eliminar esas mismas rutas. Tanto el equipo azul como el rojo pueden utilizar BloodHound para obtener fácilmente una comprensión más profunda de las relaciones de privilegios en un entorno de Active Directory.

Figura 4 - Ejemplo de Bloodhound de Hackthebox



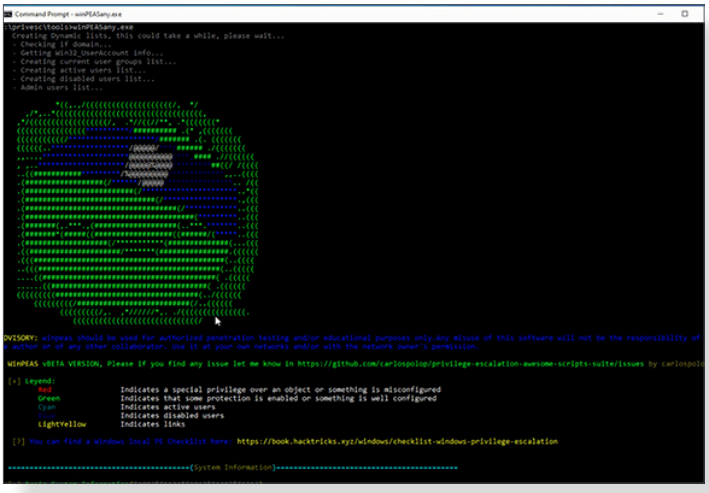
Sugerencia de vulnerabilidades de Windows: próxima generación (WES-NG). WES-NG es una herramienta basada en el resultado de la utilidad systeminfo de Windows. Proporciona la lista de vulnerabilidades a las que es vulnerable el sistema operativo, incluido cualquier exploit para estas vulnerabilidades. Se admiten todos los sistemas operativos Windows entre Windows XP y Windows 10, incluidos sus homólogos de Windows Server.

Figura 5 - WES-NG ejecutándose en Windows 10, Información del



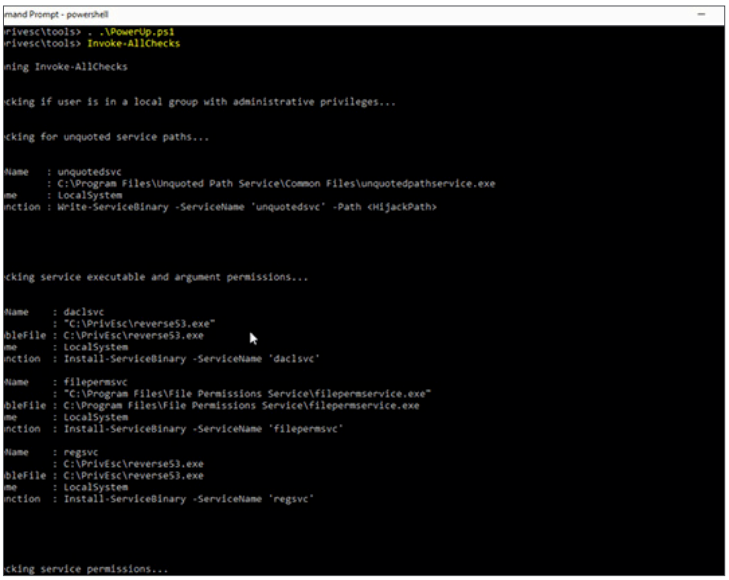
Scripts impresionantes de escalada de privilegios de Windows (WinPEAS). WinPEAS es una compilación de scripts locales de escalada de privilegios de Windows para verificar credenciales almacenadas en caché, cuentas de usuario, controles de acceso, archivos interesantes, permisos de registro, cuentas de servicios, niveles de parches, posibles configuraciones incorrectas y mucho más. WinPEAS es útil porque incluye sugerencias sobre dónde se debe centrar la atención.

Figura 6: WinPEAS ejecutándose en el endpoint de Windows 10



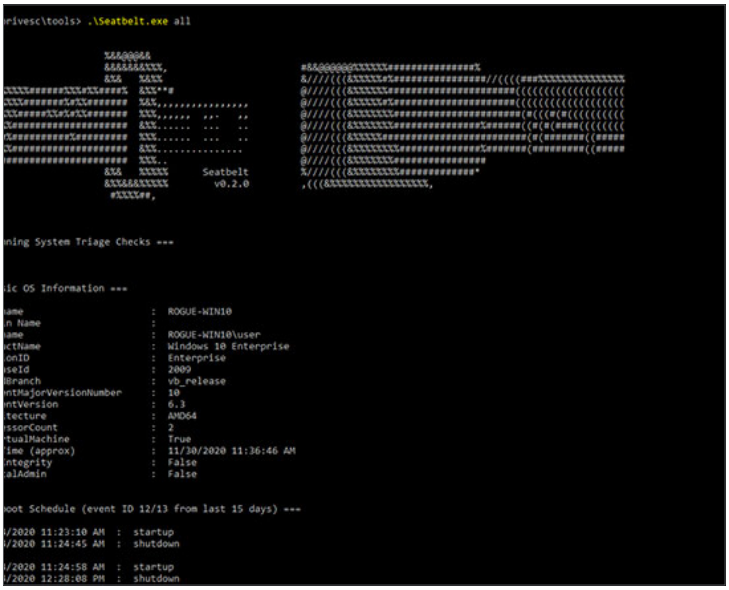
PowerUp. PowerUp es un conjunto de scripts de PowerShell para encontrar vectores comunes de escalada de privilegios de Windows que dependen de configuraciones incorrectas. La ejecución de comprobaciones de Invoke-All busca configuraciones erróneas comunes en los endpoints de Windows.

Figura 7: PowerUp ejecutándose en un endpoint de Windows



Seatbelt. Seatbelt es un proyecto de C# que realiza «comprobaciones de seguridad» de encuestas de host orientadas a la seguridad, relevantes desde perspectivas de seguridad tanto ofensivas como defensivas. Simplemente, Seatbelt es una herramienta de enumeración para mostrar información que podría conducir a una escalada de privilegios.

Figura 8: Seatbelt ejecutándose en un endpoint de Windows



La mayoría de estas herramientas y scripts buscan las siguientes debilidades o errores de configuración de Windows:

Credenciales almacenadas o en caché

Para verificar si hay créditos almacenados en caché o guardados que podrían permitirte ejecutar ejecutables con permisos elevados, ejecuta lo siguiente:

- Cmdkey /list = credenciales almacenadas actualmente
- winPEAS.exe cmd quite windowscreds
- findstr /si password *.txt

Servicios sin comillas

Los servicios mal configurados o los servicios con credenciales débiles o predeterminadas son el principal objetivo de la escalada de privilegios. Se puede abusar de los servicios que no están reforzados, como el acceso de escritura. La ruta de servicio sin comillas puede permitir a un atacante irrumpir y ejecutar malware malintencionado, permisos de registro no restringidos, etc.

Comprueba si hay configuraciones erróneas o controles de acceso débiles.

- tasklist /svc = enumera todos los procesos y servicios
- sc query [nombre] = servicio de consulta del administrador de control de servicios
- net start/stop [nombre] = detener e iniciar servicios
- sc config [nombre] = cambiar la configuración del servicio
- winPEAS.exe quiet applicationsinfo
- accesschk.exe /accepteula -uvqc
- estado de consulta sc= all I findtr “NOMBRE_SERVICIO:” >> NombresServicio.txt

Aplicaciones o sistema operativo sin parches

Un atacante buscará aplicaciones y sistemas operativos Windows sin parches.

- Systeminfo y luego compararlo con WES-NG
- lista de tareas /v

Recientemente, los exploits Potato aprovechan los ataques NTLM Relay para elevar los privilegios. Los ataques comunes incluyen Hot Potato, Juicy Potato y Rogue Potato.

Enumeración local

Los atacantes enumeran privilegios locales y de grupo normalmente utilizando los siguientes comandos.

- Privilegios de usuario
  - whoami
  - whoami /priv
  - usuarios de la red
- Enumeración de grupos
  - grupo local neto
  - grupo local neto/dominio

Perfiles Wi-Fi

Los atacantes pueden intentar conectarse directamente a tu Wi-Fi empresarial. Si no utilizas claves y utilizas una frase de contraseña WPA2, con privilegios locales, los atacantes pueden mostrar la contraseña en texto sin cifrar y luego conectar sus propios dispositivos a su red Wi-Fi.

- netsh wlan show profile
- netsh wlan show profile [nombre] key=clear

Ejecutar, copiar y revertir shells

Los atacantes utilizarán herramientas de seguridad populares o integradas para obtener más acceso y elevar los privilegios. Estos son sólo algunos de ellos:

- Certutil: Certutil.exe es un programa de línea de comandos que se instala como parte de los Servicios de Certificate Server.
- Mshta.exe: Mshta.exe ejecuta Microsoft HTML Application Host, la utilidad del sistema operativo Windows responsable de ejecutar archivos HTA (aplicación HTML).

- Powershell : PowerShell es un marco de administración de configuración y automatización de tareas de Microsoft.
- Misexec: proporciona los medios para instalar, modificar y realizar operaciones en Windows Installer desde la línea de comandos.

Otros ejecutables notables a los que hay que prestar atención y que podrían resultar sospechosos, especialmente si no están asociados con una solicitud de cambio autorizada o un ticket de servicio:

- PsExec: se usa comúnmente para administración remota; sin embargo, los atacantes malintencionados lo utilizan habitualmente para realizar cambios de configuración o ejecutar comandos remotos en los sistemas. Asegúrate de tener un proceso autorizado y controlado para usar PsExec que pueda identificar claramente una posible actividad maliciosa.
- RegEdit: otra herramienta común de Windows para leer o editar el registro de Windows y que puede usarse para ayudar a los administradores a realizar cambios autorizados en muchos sistemas. Nuevamente, al igual que con PsExec, asegúrate de monitorizar el uso no autorizado de RegEdit dentro de tu entorno y de tener un proceso controlado definido para su uso.
- Batch Scripts (también conocido como archivo .bat): asegúrate de monitorizar y auditar archivos con extensiones .bat en tu entorno y cuándo se ejecutan. Si bien pueden usarse para la actividad normal del administrador, los atacantes también los usan comúnmente para automatizar y ejecutar un conjunto de comandos. Pueden usarlo para robar credenciales, modificar la configuración de seguridad de los sistemas, asignar recursos compartidos de red o inicializar ransomware. Es importante tener visibilidad de estos archivos cuando se ejecutan en tu entorno. Por lo general, esto puede generar una advertencia temprana de que un atacante está a punto de hacer algo dañino para tu entorno.

Cada una de estas herramientas se utiliza con fines legítimos para la administración y configuración de sistemas, pero también suelen objeto de abuso por parte de actores malintencionados. Los atacantes pueden utilizar estas herramientas para descargar scripts, crear shells inversos, así como ejecutar comandos y aplicaciones.

Persistencia

Los atacantes necesitan perseverancia. Por supuesto, también necesitan dormir, por lo que abusan de estas configuraciones para mantener un acceso persistente a los sistemas. Cuando se despiertan, pueden recuperar el control del endpoint de Windows de la víctima.

Para que esto sea posible, utilizan:

- Servicios
- Ejecuciones automáticas
- Creación de usuarios
- Tareas programadas
  - schtasks /query /fo LIST /v = lista de tareas programadas

Otros métodos comunes para la escalada de privilegios son:

- Navegador
- Ejecuciones automáticas
- SNMP
- AlwaysInstallElevated
- Archivos de configuración
- Registro
- RDP
- Inyección de DLL
- Pass the Hash (Pasar el hash)
- Suplantar tokens de acceso
- Aplicaciones de inicio

Cómo protegerse contra la escalada de privilegios

- **Usa el control de aplicaciones.** Controla qué aplicaciones se pueden ejecutar, qué aplicaciones maliciosas conocidas se rechazan y cuáles requieren auditoría adicional. El control de aplicaciones también puede ayudar a evitar que se ejecuten scripts de enumeración.
- **Aplica parches y actualizaciones.** No es una solución absoluta, pero ralentiza a los atacantes.
- **Utiliza una solución de seguridad de acceso privilegiado.** Asegúrate de que todos los servicios tengan una cuenta aprovisionada con los controles de seguridad correctos, como contraseñas complejas o rotadas con frecuencia. Descarta las claves universales y los privilegios permanentes y pasa a privilegios según demanda y just-in-time (justo a tiempo).
- **Restringe el uso de la cuenta de administrador del dominio.** Rota las contraseñas de las cuentas después de cada uso.
- **Registra y audita tanta actividad de privilegios como sea posible.** Supervisa el uso abusivo y establece alertas para actividades anómalas.

Reforzar los endpoints de Windows es solo una parte de la reducción del riesgo

La seguridad absoluta no existe. Ninguna herramienta por sí sola puede proteger contra los ciberataques. Cuanto mejor comprendas cómo actúan los atacantes, más difícil se lo pondrás.

Los atacantes agotarán todos los métodos anteriores en su intento de infiltrarse en tu organización y acceder a información confidencial. Como protector, debes descubrir estos métodos y reforzar los endpoints de Windows lo mejor que puedas para defenderte de ellos.

Próximos pasos

Adherirse a una política de privilegios mínimos es especialmente importante para los trabajadores remotos que se conectan desde diversas estaciones de trabajo. Si los usuarios tienen derechos de administrador local y descargan involuntariamente software malintencionado, invitan a los ciberdelincuentes a toda tu red.

Un análisis rápido de tu entorno indica qué cuentas pueden tener privilegios excesivos y, por lo tanto, ser vulnerables a amenazas internas y ataques de malware.

Descarga la Herramienta de descubrimiento de privilegios mínimos de Delinea para ver cuáles de tus sistemas de TI y usuarios tienen mayores privilegios de los necesarios.

Acerca de Joseph Carson

- Científico jefe de Seguridad en Delinea
- Más de 25 años de experiencia en seguridad empresarial
- Autor de *Gestión de acceso privilegiado para principiantes* y *Ciberseguridad para principiantes*
- Asesor de ciberseguridad para varios gobiernos, infraestructura crítica, industrias financieras y de transporte.
- Ponente en conferencias a nivel mundial

Acerca de Delinea

Delinea es un proveedor líder de soluciones de gestión de accesos privilegiados (PAM) que proporciona una seguridad sin fisuras para la empresa híbrida moderna. La plataforma Delinea amplía la capacidad y el rendimiento de las soluciones PAM proporcionando autorización para todas las identidades, controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles. Su objetivo es ayudar a reducir el riesgo, garantizar el cumplimiento normativo y simplificar la seguridad. Delinea pone fin a la complejidad y define los límites de los accesos para miles de clientes en todo el mundo. Nuestros clientes comprenden desde pequeñas empresas hasta las mayores instituciones financieras del mundo, agencias de inteligencia y empresas de infraestructuras críticas. **delinea.com/es/**

Delinea

Defining the boundaries of access

Delinea es un proveedor líder de soluciones de gestión de accesos privilegiados (PAM) que proporciona seguridad sin fisuras a la empresa híbrida moderna. Delinea Platform amplía la capacidad y el rendimiento de las soluciones PAM proporcionando autorización para todas las identidades, controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles. Su objetivo es ayudar a reducir el riesgo, garantizar el cumplimiento normativo y simplificar la seguridad. Delinea reduce la complejidad y controla los límites en los accesos para miles de clientes en todo el mundo. Nuestros clientes comprenden desde pequeñas empresas hasta las mayores instituciones financieras del mundo, agencias de inteligencia y empresas de infraestructuras críticas. **delinea.com/es/**

 ENDP-WP-0124-ES