Seguridad: Hackers

Por Paco Aldarias Raya

Impreso: 15 de diciembre de 2004

Email: pacolinux arroba inicia punto es
Web: `http://pagina.de/pacodebian`
Con Linux Debian. En Valencia (España)

Realizado con: LaTeX

Índice

1. Introducción **1**

2. La dirección ip **1**

2.1. Para saber la ip nuestra 2

2.2. Para saber las ips de la red 2

2.3. Para saber la ip de otra máquina con estos métodos 2

3. Como ver las conexiones de nuestra máquina con otras **2**

4. Como saber que es cada puerto **3**

5. Como entrar en una máquina **3**

6. Entrar a máquinas con windows **3**

7. Entrar a máquinas con el pueto 21 abierto **4**

8. Sacar contraseñas: snifers **4**

9. Bloquear el acceso al superservidor: inetd **4**

10.Los cortaguegos: iptables **5**

11.Cómo ver nuestras ips **6**

12.Cómo saber de donde es una ip: whois **6**

13.Programas para analisis de seguridad **6**

14.Páginas de hakers **8**

1. Introducción

La seguridad y hacker esta intimamente relaciónado.

Exiten dos elementos importantes:

1. La direccion ip
2. Los puertos

Conociendo la ip y los puertos abiertos podemos entrar en las máquinas.

La ip equivaldrá a la dirección de una persona. Y los puertos, las puertas de la vivienda, donde cada puerta nos da acceso a una habitación.

2. La dirección ip

Es la dirección en internet de una máquina

2.1. Para saber la ip nuestra

1. En windows: Incio-ejecutar-winipcfg
2. En linux: ifconfig

2.2. Para saber las ips de la red

1. En windows: !! de pago !! (ipscan)

2. En linux: nmap -sP 192.168.100.*
   Esto nos da las ip de la red 192.168.100

   En linux: nmap 192.168.100.*
   Esto nos da las ip de la red 192.168.100 y los puertos abiertos.

2.3. Para saber la ip de otra máquina con estos métodos

Métodos:

1. Viendo la cabecera del email
2. Viendo las conexiones con nuestra máquina, en netmeeting, ftp, etc.

3. Como ver las conexiones de nuestra máquina con otras

1. En windows:
   netstat -n
2. En linux:

   netstat -tupan ipnuestra
   Muesta nuestra conexiones

   netstat -tupan 127.0.0.1
   Muesta nuestras conexiones

   netstat -tupan 127.0.0.1 — grep ESTA
   Muesta nuestra conexiones establecidad

Las conexiones tienen varios estados:

1. Listen. Escuchando
2. Establised. Establecida.

Nota: Comprobar a q corresponde los puertos abiertos de tu máquina y la de otra que conozcais.

4. Como saber que es cada puerto

En windows:
No hay se sabe.

En linux:
cat /etc/services — grep 110
Nos dice a que servicio corresponde el puerto 110.

Nota: Comprobar a q corresponde los puertos abiertos de alguna máquina.

5. Como entrar en una máquina

Una máquina sin puertos abiertos no es posible entrar.

Según el puerto abierto usaremos una herramienta u otra.

Cada puerto corresponde a un servicio, deberemos usar herramientas para poder entrar a ese servicio.

6. Entrar a máquinas con windows

Windows usa el protocolo tcp/ip, ed decir, cuando conecta a internet, esta máquina tiene su ip por la cual podemos entrar. Si windows tiene activado compartir archivos e impresora. Podremos entrar por esta puerta abierta.

Las máquinas que tienen netbios (windows) abierto usan los puertos 139/tcp.

Haciendo nmap ip, podremos averiguar si esta abierto (open).

Forma de entrar:

1. Con windows:
   Inicio - Buscar pc - Poner su ip
   Apareceran las carpetas compartidas

2. Con linux:
   komba2

Nota: Comprobar una máquina con windows q comparte que puertos tiene abiertos e intentar acceder a sus archivos.

Es importante tener claro esto, pues cuando nos conectemos a internet, no debemos compartir archivos, ya que estos serán accesibles, desde el exterior. Si no tenemos una red en casa, no instaleis netbios. Si teneis una red, y quereris compartir archivos, ponerle siempre contraseña a las carpetas.

7. Entrar a máquinas con el pueto 21 abierto

El puerto 21 corresponde al servicio ftp

Para poder entrar debemos poner: ftp ip

Pero nos pide contraseña. !!! como sacarla !!!

8. Sacar contraseñas: snifers

Si estamos en una red publica, es peligros poner nuestra contraseña sin cifrar. Ya que circula por la red y cualquiera puede cogerla.

Vamos a ver como se consique y como evitar nos la cogan.

Para coger las contraseñas usaremos snifer (snifador). En linux:

1. En consola: tcpdump Ejemplo: tcpdump -X
2. Modo gráfico: ethereal
   `http://www.ethereal.com`

Para evitar que nos cogan las contraseñas debemos usar siempre protocolos cifrados. En lugar de telnet, debemos usar ssh. En lugar de ftp debemos usar sftp. En yahoo, debemos usar opcion de seguridad. Asi en todo.

Las páginas web cifradas son las https.

9. Bloquear el acceso al superservidor: inetd

Normalmente los servidores web, ftp, etc, en su configuración se puede indicar restricciones de acceso a máquinas.

El superdemonio xinetd, permite controla más de un servidor. Podemos indicar q al arrancar inetd, se arranque el servidor web, ftp, etc.

Inetd es como una programa q arranca q y controla otros programas o servidores.

El control de acceso a los servicios de inetd, se controla en el fichero:

Aqui están las maquinas q pueden entrar:
/etc/hosts.allow

Aqui estan las maquinas q no pueden entrar:
/etc/hosts.deny

En estos ficheros se indica el servicio:máquina

Suele denegarse a todos, y luego ir indicando q maquinas pueden usar los servicios. El uso de hosts.allow y hosts.deny se llama tcpwraper

Ejemplos: /etc/hosts.deny
ALL:ALL
Nota: Esto deniega todo a todas las maquinas.

/etc/hosts.allow
ftp.in:192.168.100.2
Nota: Esto permite acceso a ftp a la máquina 192.168.100.2

10. Los cortaguegos: iptables

Un cortafuetos es un sistema q permite aceptar o denegar el acceso a ciertas máquinas.

Permite no pueda entrar a la nuestra. Tb permite bloquear ciertos puertos.

Es necesario que el kernel tenga activado la opcion del iptables.

Existen varios cadenas de reglas que se aplican a lo q entra y a lo que sale:
INTUT: Entrada
OUTPUT: Salida
FORWARD: Reenvio

Instrucciones básicas:
Para ver las reglas: iptables -L -n -v
Para borrarlas todas: iptables -F
Para añadir una regla: iptables -a regla
Para borrar una regla: iptables -d regla

Ejemplo:

Bloquemos la entrarda desde cualquier IP
iptables -a INPUT -s 0.0.0.0/0 -j DROP

Esto equivale a quedarnos sin red, es decir:
ifconfig eth0 down

Ejemplo:

Bloquemos la entrada cuyo destino sea el puerto 21 desde cualquier IP .
Con ello bloqueriamos el servidor ftp.
iptables -a INPUT -s 0.0.0.0/0 -dport 21 -j DROP

Esto rechazaria:
iptables -a INPUT -s 0.0.0.0/0 -dport 21 -j REJECT

Esto aceptaria
iptables -a INPUT -s 0.0.0.0/0 -dport 21 -j ACCEPT

11. Cómo ver nuestras ips

Un maquina en una red local tiene una ip, por ejemplo, 192.168.0.1. Pero para salir a internet tenemos una ip válida en internet, por ejemplo, 217.128.45.23.

Eso se debe a q el router transforma nuestra ip para salir a internet.

Podemos ver la ip externa aqui:
http://www.whatismyip.com/

La ip interna o de la red local se puede ver con:
ifconfig

12. Cómo saber de donde es una ip: whois

Una vez tenemos la ip podemos saber de donde es esa maquina poniendo:
whois ip

También se puede consultar en la web:
http://www.ripe.net/db/whois/whois.html

13. Programas para analisis de seguridad

Satan/Saint: Aunque parezca que ya no tiene utilidad para mi sigue siendo útil para comprobar algunos fallos comunes de configuración del sistema.

Cops: Similar a Satan con algunas mejoras, también es un programa ya antiguo, pero sigue siendo útil.

Tiger: Muy similar a Cops pero más moderno y con más funcionalidad. Muy útil para los fallos de configuración y para la seguridad del sistema.

Tara: Una versión todavía más avanzada y modificada de Tiger/Cops.

Sara: Un derivado de Satan actualizado y modernizado, también muy recomendable.

Nessus: Una herramienta imprescindible. Es el sistema más avanzado para detectar fallos de seguridad tanto en Linux como en otros sistemas operativos. Tiene una librería inmensa de chequeos y se actualiza muy

frecuentemente con los últimos exploits que van apareciendo. Realiza una cantidad impresionante de chequeos sobre el sistema y genera informes donde se indican los errores y las posibles soluciones. Si tuvieras que elegir una única herramienta para chequear la seguridad de tus sistemas esta sería Nessus sin duda. Lo único que necesitarías es una herramienta como Satan/Cops/Tiger/Tara que te chequee permisos, bits suid y malas prácticas de configuración del sistema que no chequea Nessus.

Nmap: Otro imprescindible. Una herramienta de escaneado con prácticamente todas las opciones existentes en este campo. Muy bueno para chequear la seguridad de tu firewall.

Whisker/Nikto: Nikto usa Whisker como librería, así que podría decirse que la herramienta es Nikto. Chequea la seguridad de servidores web. Tiene una base de datos con montones de ataques y puede realizar diversas modificaciones sobre los ataques para intentar evadir detecciones con NIDSs como snort.

Fragrouter: Un toolkit que implementa técnicas de evasión sobre todo usando diversos tipos de fragmentación y de parámetros raros en el protocolo TCP. Muy bueno para probar la eficacia de firewalls e NIDSs.

Hydra: La herramienta más potente de bruteforce sobre servidores de login y similares. Permite usar diccionarios para forzar logins en servidores telnet/ssh/etc.

Hunt: Una herramienta para realizar ataques del tipo Hijacking y Man-in-the-middle. También realiza tormentas ARP.

Ettercap: Similar a Hunt. Realiza ARP poisoning y otros ataques sobre redes ethernet.

hping2: Una herramienta de generación de paquetes TCP/IP. Sabiendolo utilizar puede realizar todo tipo de ataques y pruebas sobre servidores. Especialmente útil para probar NIDS y firewalls. Imprescindible.

John the ripper: Una herramienta de crackeado de passwords que utiliza diccionarios. Imprescindible para probar la seguridad de los passwords de tus usuarios. Hay que complementarlo con una buena colección de diccionarios.

kismet/airsnort: Herramientas para estudio de redes WLAN.

chkrootkit: Imprescindible. Detecta la presencia de los rootkits y modulos LKM más comunes en sistemas Linux.

p0f: Herramienta pasiva de detección de sistemas operativos. Útil para comprobar si tus servidores y clientes están propagando por la red información sobre sus sistemas operativos.

Ethereal: El rey indiscutible de los sniffers. Muy útil para capturar el tráfico de tu red y conocer lo que están mandando tus máquinas.

Nbtscan: Para escanear redes Netbios/Samba.

Metasploit: Un framework para probar exploits. Un poco raro de usar y no tiene demasiados exploits.

14. Páginas de hakers

El FAQ de es.comp.hackers que está en estas páginas:

`http://www.geocities.com/crino1p/index.html`
`http://www.navegalia.com/hosting/00084/isocrono`
`http://www.hello.to/nbk`
`http://members.es.tripod.de/omg`
`http://fly.to/tomacheli`

Con ello se tendrían los conicimientos básicos.