NFS Enumeration

Network File System (NFS) is a distributed file system protocol that allows clients to access and manipulate files on remote servers as if they were local. While NFS provides a convenient way to share files across a network, improper configuration can leave systems vulnerable to unauthorized access and exploitation.

Enumeration with Nmap

Lets start NFS enumeration with nmap.

```
sudo nmap -sS -sV -p 111,2049 --script nfs* 192.168.29.141
```

Check if NFS is running

We can also use rpcinfo command line tool to check if NFS is running or not.

```
rpcinfo -p <TARGET IP>
```

View available mounts

- Next the most important thing, to check the available mounts that we can connect to. We will use the showmount command.

```
showmount -e <TARGET IP>
showmount -a <TARGET IP>
```

Mount a NFS Share

In order to perform the mount. We will first create a test folder in our temp or any working directory. Then we will use the mount command to connect the root filesystem of the target to our our test folder.

```
sudo mount -t nfs 192.168.29.141:/ /tmp/test
```

Now that we are into the target file system, lets understand how can we exploit it.

One technique is to create a SSH backdoor access. Like we discussed in FTP section, i guess so if we have write permissions to the root user directory via our mounted share, then we will upload our SSH keys to it and accessed the server as root from our machine.

Unmount a NFS share

We can also unmount our mounted NFS share using the umount command.

Lets see how

```
sudo umount -f -l /tmp/test
```

View available mounts with Metasploit

We have already seen how we can enumerate available mounts using showmount command. This can be also be done with metasploit, so lets cover this also.

```
use auxiliary/scanner/nfs/nfsmount
set RHOSTS <TARGET>
run
```

Enumeration with RPCScan

At last, we have one more tool by which we can perform NFS enumeration and that is RPCscan.

The idea of exposing you to multiple tools and techniques is that, if in case, one tool becomes irrelevant suddenly then you should have a backup in your arsenal for that.

Now coming back to RPCscan.

The first thing we can do with it is that we can confirm the RPC and NFS server is running or not

```
python3 rpc-scan.py 192.168.29.141 --rpc
```

Next we can view the available mounts using the --mounts flag in the end.

```
python3 rpc-scan.py 192.168.29.141 --mounts
```
