
# Identify and Mount NFS

## Requirements

- NMAP

## Information

- OS: Kali Linux[Debian]
- RHOST: Target or victim computer
- LHOST: Local computer or attacking computer

**Author:** Scott Anderson AKA CyberMunky

**Date:** 8.31.2020

**LinkedIn:** www.linkedin.com/in/scottanderson1989

**YouTube: Exploit Security**

## LHOST - Attacking Computer

During port scanning you may notice an open port on 111 for rpcbind. *The rpcbind utility is a server that converts RPC program numbers into universal addresses**. You can run the NMAP NSE 'rpcinfo' which *connects to portmapper and fetches a list of all registered programs. It then prints out a table including (for each program) the RPC program number, supported version numbers, port number and protocol, and program name**. Out of best practice, especially first starting out, it is a good idea to save the

output. This can home in handy when writing reports or just working an especially tough target. Run the following code:

```
LHOST@exploit-security:~$ sudo nmap -sV -p 111 --script=rpcinfo -oA RPCInfo {RHOST}
```

```
cybermunky@exploit-security:~/Labs/HTB/Remote/NMAP$ sudo nmap -sV -p 111 --script=rpcinfo -oA RPCInfo 10.10.10.180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 12:13 EDT
Nmap scan report for 10.10.10.180
Host is up (0.029s latency).

PORT    STATE SERVICE VERSION
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/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
```

You can also run all NMAP NSE NFS scripts by running nfs with a wildcard:

```
LHOST@exploit-security:~$ sudo nmap -p 111 --script=nfs* -oA NFS {RHOST}
```

```
cybermunky@exploit-security:~/Labs/HTB/Remote/NMAP$ sudo nmap -p 111 --script=nfs* -oA NFS 10.10.10.180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 12:14 EDT
Nmap scan report for 10.10.10.180
Host is up (0.029s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /site_backups
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID         GID         SIZE   TIME                 FILENAME
| rwx------   4294967294  4294967294  4096   2020-02-23T18:35:48  .
| ??????????  ?           ?           ?      ?                    ..
| rwx------   4294967294  4294967294  64     2020-02-20T17:16:39  App_Browsers
| rwx------   4294967294  4294967294  4096   2020-02-20T17:17:19  App_Data
| rwx------   4294967294  4294967294  4096   2020-02-20T17:16:40  App_Plugins
| rwx------   4294967294  4294967294  8192   2020-02-20T17:16:42  Config
| rwx------   4294967294  4294967294  64     2020-02-20T17:16:40  aspnet_client
| rwx------   4294967294  4294967294  49152  2020-02-20T17:16:42  bin
| rwx------   4294967294  4294967294  64     2020-02-20T17:16:42  css
| rwx------   4294967294  4294967294  152    2018-11-01T17:06:44  default.aspx
|_
| nfs-showmount:
|_  /site_backups
| nfs-statfs:
|   Filesystem     1K-blocks   Used        Available   Use%  Maxfilesize  Maxlink
|_  /site_backups  31119356.0  12163100.0  18956256.0  40%   16.0T        1023

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

Next you will create a directory. It is recommended that you give it the same name as the identified directory during your NFS scan. You will follow up by mounting the directory.

```
LHOST@exploit-security:~$ mkdir {DIRECTORY}
ex: mkdir site_backups

LHOST@exploit-security:~$ sudo mount -o nolock {RHOST}:{DIRECTORY} {PATH TO CREATED DIRECTORY}
ex: sudo mount -o nolock 10.10.10.180:/site_backups ~/Labs/HTB/Remote/site_backups
```

## References

- https://linux.die.net/man/8/rpcbind
- https://nmap.org/nsedoc/scripts/rpcinfo.html