

NFS Enumeration

NFS Enumeration

NFS stands for "Network File System" and allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files. It does this by mounting all, or a portion of a file system on a server. The portion of the file system that is mounted can be accessed by clients with whatever privileges are assigned to each file.

NFS runs on port 2049.

NFS Enumeration using superenum

To scan for NFS, use `./superenum` and provide .txt file with IP addresses to it.

NFS Enumeration using nmap

```
nmap -p 2049 [TARGET IP ADDRESS]
```

NFS Enumeration using rpc-scan

```
python3 rpc-scan.py 10.10.10.19 --rpc
```