- Filename: eccouncil-ceh31250-v12-4-6-1-nfs-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: NFS Enumeration
  ==

NFS Enumeration

Objectives:

- Define NFS and explain potential vulnerabilities
- Search for and access sensitive data using NFS tools

- What is NFS?
    - Share local filesystem over network
        - Remote users can mount filesystem, locally
            - Centralization of data
    - Uses TCP/UDP port 2049
- !!! Using Metasploitable2 as target !!!
- How do we check for NFS?
    - `nmap -A -T5 -n -Pn -p 2049 target_IP`
    - `rpcinfo -p target_IP`
    - `showmount -e target_IP`
    - `rpc-scan.py`
        - https://github.com/hegusung/RPCScan
- How do we access the NFS share?
    1. `mkdir /tmp/NFS`
    2. `sudo mount.nfs target_IP:/path/to/share /tmp/NFS`
    3. `ls /tmp/NFS`