eJPT Lab Series 01 : Network Discovery with Nmap, ARP-Scan and Netdiscover

Paris Smith

7/1/25

Objective **2**
Tools **2**
Environment/Setup **2**
Methodology/Steps **3**
Planning & Scope / PreEngagement Interactions 3
Networking Issue on boot with KaliBox in Proxmox environment 3
Vulnerable Config Steps 5
Creating the user 5
Unexpected Network Issue on Debian Desktop 9
SSH enabled for attack simulation on Debian Desktop 10
Reconnaissance/Intelligence Gathering (Pre Access) 12
Locate endpoints on a network 12
Scanning/Vulnerability Analysis(Pre Access) 12
Identify open ports and services on a target 12
Identify operating system of target 13
Exploitation 14
Post Exploitation 14
Enumeration(Post Access) 14
Enumerate network information from files on target 14
Enumerate system information on target 15
Gather user account information on target 16
Data Exfiltration 16
Compile information from files on target & Transfer files to and from target 16
Setting up Secure Copy over SSH - Secure FIle Transfer to Host 17
Lessons Learned/Reflection 18
Appendix **19**
Raw Output arp.txt 19
Raw Output scan2.txt 20
Raw Output scan.txt 22
Raw Output netdiscover.txt 24
References **27**

Objective

The goal of this lab is to demonstrate the ability to locate active endpoints on a local network using tools such as *arp-scan. netdiscover, and nmap.* This is aligned with eJPT's *Assessment Methodologies domain*: 'Locate endpoints on a network' and *Host and Networking Auditing:* 'Transfer files to and from target' & 'Compile information from files on target'

Domains Demonstrated

Assessment Methodologies - Locate endpoints on a network
Assessment Methodologies - Identify open ports and services on a target
Assessment Methodologies - Identify operating system of a target
Host and Networking Auditing - Compile information from files on target
Host and Networking Auditing - Enumerate network information from files on target
Host and Networking Auditing - Enumerate system information on target
Host and Networking Auditing - Gather user account information on target
Host and Networking Auditing - Transfer files to and from target
Host and Networking Auditing - Gather hash/password information from target

Tools

OS & Platforms

Win11 Desktop - Host
Proxmox Virtual Environment - via GUI @192.168.4.15
Kali Linux - Attacker VM @192.168.4.25

Network Discovery Tools

arp-scan
nmap
netdiscover

File Transfer / Remote Access

ssh
scp

Environment/Setup

The lab was executed in a Proxmox virtualized environment. The Kali Linux machine (192.168.4.25) acted as the attacker system. Multiple other devices—including routers, smart devices, and other endpoints—were present on the 192.168.4.0/24 subnet, simulating a real-world internal network.

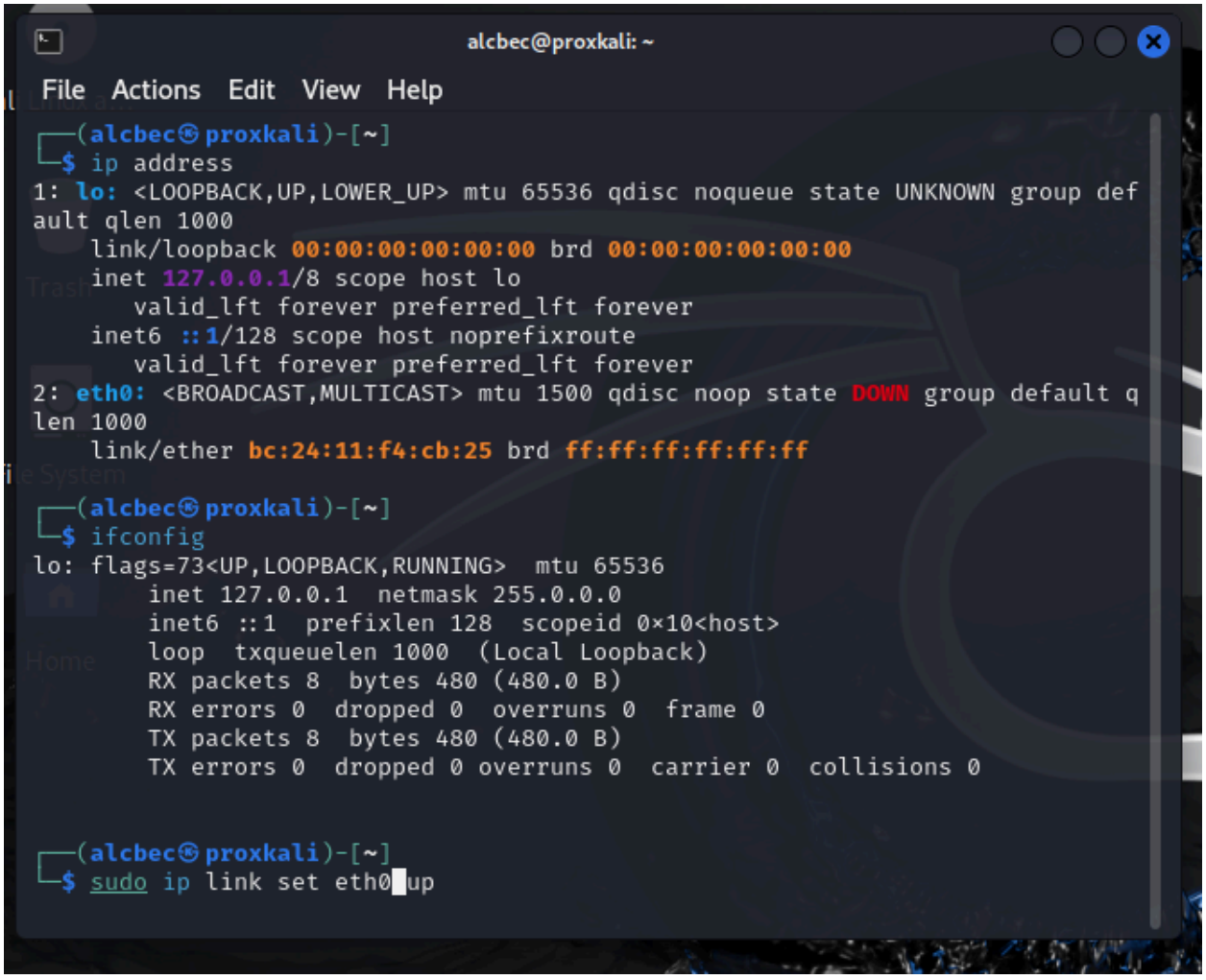
Methodology/Steps

Planning & Scope / PreEngagement Interactions

Define lab goal, set up environment

Networking Issue on boot with KaliBox in Proxmox environment

Firstly on 7/5 I ran into a networking issue, below are the remediations



^not receiving ipv4 on eth0

```
┌──(alcbec㉿proxkali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::be24:11ff:fef4:cb25  prefixlen 64  scopeid 0x20<link>
        ether bc:24:11:f4:cb:25  txqueuelen 1000  (Ethernet)
        RX packets 1101  bytes 159248 (155.5 KiB)
        RX errors 0  dropped 151  overruns 0  frame 0
        TX packets 6  bytes 516 (516.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The angle I took was then going to /etc/network/interfaces and I found that I was missing the auto lo within my network config (below is the corrected version)

```
  GNU nano 8.2                 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.4.25
        netmask 255.255.255.0
        gateway 192.168.4.1
        dns-nameservers 192.168.4.1
```

I then ran the following commands in a sudo terminal

```
┌──(root㉿proxkali)-[~]
└─# sudo systemctl restart networking

┌──(root㉿proxkali)-[~]
└─# ifdown eth0 && ifup eth0

┌──(root㉿proxkali)-[~]
└─# ip a show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
roup default qlen 1000
    link/ether bc:24:11:f4:cb:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.25/24 brd 192.168.4.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fef4:cb25/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(root㉿proxkali)-[~]
└─#
```

^Networking issue resolved, good to go with the lab

Vulnerable Config Steps

Creating the user

bring self to super user

```
paris@paris-VirtualBox:~$ sudo su
[sudo] password for paris:
root@paris-VirtualBox:/home/paris#
```

I then ran cat /etc/passwd but my eyes hurt and I thought “what am i looking for” which led to this

```
root@paris-VirtualBox:/home/paris# cat /etc/passwd | grep paris
paris:x:1000:1000:paris:/home/paris:/bin/bash
root@paris-VirtualBox:/home/paris#
```

So, i at least know that account is real and active…but need to figure out what the whole output means

I then ran into a small issue:
Ran the ‘adduser test’ but I interrupted with CTRL+Z which output to the CLI “Stopped” then I ran a CTRL+C to kill it entirely. I felt like I messed up the process. Thus, I had to investigate to confirm. Below is the screenshot of me investigating
****i changed some visual aspects of my CLI in this box****

```
paris@paris-VirtualBox:~$ sudo su
[sudo] password for paris:
root@paris-VirtualBox:/home/paris# adduser test
info: Adding user `test' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test' (1001) ...
info: Adding new user `test' (1001) with group `test (1001)' ...
info: Creating home directory `/home/test' ...
info: Copying files from `/etc/skel' ...
New password:
[1]+  Stopped                 adduser test
root@paris-VirtualBox:/home/paris#
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: ^C
```

^the CLI when I ran CTRL+C and CTRL+Z

Ran the following commands

```
root@paris-VirtualBox:/home/paris# cat /etc/passwd | grep paris
paris:x:1000:1000:paris:/home/paris:/bin/bash
root@paris-VirtualBox:/home/paris# cat /etc/passwd | grep test
test:x:1001:1001::/home/test:/bin/bash
```

cat /etc/passwd - super noisy
cat /etc/passwd | grep paris - confirmed my original was discoverable
cat /etc/passwd | grep test - confirmed my ‘test’ account was created

I ran into a constant error when attempting to confirm I can still add users

```
root@paris-VirtualBox:/home/paris# adduser test1
warn: Waiting for lock to become available...
warn: Waiting for lock to become available...
warn: Waiting for lock to become available...
warn: Waiting for lock to become available...
```

```
root@paris-VirtualBox:/home/paris# adduser test
warn: Waiting for lock to become available...
warn: Waiting for lock to become available...
^Cerr: Caught a SIG%s.
root@paris-VirtualBox:/home/paris# adduser ohno
warn: Waiting for lock to become available...
warn: Waiting for lock to become available...
```

I then did some research and came to the decision of killing any processes related to adduser that were active, assuming I broke it earlier. Remediation steps are below

```
root@paris-VirtualBox:/home/paris# ps aux | grep adduser
root        2988  0.0  0.2  19212 11632 pts/1    T    16:40   0:00 adduser
root        3050  0.0  0.2  18612 11060 pts/1    T    16:45   0:00 adduser
root        3061  0.0  0.0   9144  2248 pts/1    S+   16:47   0:00 grep --color=
auto adduser
```

```
root@paris-VirtualBox:/home/paris# sudo kill -9 3050
[2]+  Killed                  adduser ohno
root@paris-VirtualBox:/home/paris# sudo kill -9 2988

Password change has been aborted.
[1]+  Killed                  adduser test
root@paris-VirtualBox:/home/paris# passwd: Authentication token manipulation err
or
passwd: password unchanged
```

```
root@paris-VirtualBox:/home/paris# ps aux | grep adduser
root        3092  0.0  0.0   9144  2248 pts/1    S+   16:49   0:00 grep --color=
auto adduser
```

Following those remediations we can verify that no other ‘adduser’ processes are running that would interfere with our desired operations.

So! We've confirmed vulnerable users and configurations are complete, we can move onto attempting to exploit and satisfy the following exam objectives thoroughly.

```
root@paris-VirtualBox:/home/paris# adduser ohno
info: Adding user `ohno' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ohno' (1002) ...
info: Adding new user `ohno' (1002) with group `ohno (1002)' ...
info: Creating home directory `/home/ohno' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for ohno
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `ohno' to supplemental / extra groups `users' ...
info: Adding user `ohno' to group `users' ...
root@paris-VirtualBox:/home/paris# adduser testuser
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1003) ...
info: Adding new user `testuser' (1003) with group `testuser (1003)' ...
info: Creating home directory `/home/testuser' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Adding user `testuser' to group `users' ...
```

Unexpected Network Issue on Debian Desktop

However, after I changed my adapter from NAT to bridged on my Debian desktop, I had to make some networking changes as it was getting an IP in the wrong network and subnet. *turning on and off the firewall inside of proxmox was the necessary remediation after ensuring correct ip assigned

The /etc/network/interfaces was empty so I ran nmcli and remediated the networking issue via static addressing.

```
root@paris-VirtualBox:/home/paris# nmcli
enp0s3: connected to netplan-enp0s3
        "Intel 82540EM"
        ethernet (e1000), 08:00:27:B1:40:EA, hw, mtu 1500
        ip4 default
        inet4 192.168.7.134/22
        route4 192.168.4.0/22 metric 100
        route4 default via 192.168.4.1 metric 100
        inet6 fda8:28f5:e3a3:1:8223:8126:98d7:511a/64
        inet6 fda8:28f5:e3a3:1:a00:27ff:feb1:40ea/64
        inet6 2603:9000:c200:168:a00:27ff:feb1:40ea/64
        inet6 2603:9000:c200:168:8dc2:6682:ae18:4629/64
        inet6 fe80::a00:27ff:feb1:40ea/64
        route6 fe80::/64 metric 256
        route6 default via fe80::3257:8eff:fe5d:ff12 metric 1024
        route6 fda8:28f5:e3a3:1::/64 metric 256
        route6 2603:9000:c200:168::/64 metric 256

lo: connected (externally) to lo
        "lo"
        loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
        inet4 127.0.0.1/8
        inet6 ::1/128

DNS configuration:
        servers: 192.168.4.1
        interface: enp0s3
```

```
root@paris-VirtualBox:/home/paris# nmcli connection modify "ensp0s3"

Error: unknown connection 'ensp0s3'.
root@paris-VirtualBox:/home/paris# nmcli connection modify "enp0s3"

Error: unknown connection 'enp0s3'.
root@paris-VirtualBox:/home/paris# nmcli connection modify "netplan-enp0s3"

Error: <setting>.<property> argument is missing.
root@paris-VirtualBox:/home/paris# nmcli connection modify "netplan-enp0s3" \ ipv4.address 192.168.4.71/24 \ ipv4.gatewa
y 192.168.4.1 \ipv4.dns "8.8.8.8 1.1.1.1 192.168.4.1" \ ipv4.method manual
Error: invalid or not allowed setting ' ipv4': ' ipv4' not among [connection, 802-3-ethernet (ethernet), 802-1x, dcb, sr
iov, ethtool, match, ipv4, ipv6, hostname, link, tc, proxy].
root@paris-VirtualBox:/home/paris# nmcli connection modify "netplan-enp0s3" \ipv4.address 192.168.4.71/24 \ipv4.gateway
192.168.4.1 \ipv4.dns "8.8.8.8 1.1.1.1 192.168.4.1" \ipv4.method manual
```

```
root@paris-VirtualBox:/home/paris# nmcli connection up "netplan-enp0s3"

Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
root@paris-VirtualBox:/home/paris# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b1:40:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.71/24 brd 192.168.4.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 2603:9000:c200:168:305e:7b37:918c:4eb4/64 scope global temporary dynamic
       valid_lft 565261sec preferred_lft 86136sec
    inet6 2603:9000:c200:168:a00:27ff:feb1:40ea/64 scope global dynamic mngtmpaddr
       valid_lft 565261sec preferred_lft 565261sec
    inet6 fda8:28f5:e3a3:1:e34d:658b:f26c:d2c4/64 scope global temporary dynamic
       valid_lft 604798sec preferred_lft 86136sec
    inet6 fda8:28f5:e3a3:1:a00:27ff:feb1:40ea/64 scope global dynamic mngtmpaddr
       valid_lft 2591998sec preferred_lft 604798sec
    inet6 fe80::a00:27ff:feb1:40ea/64 scope link
       valid_lft forever preferred_lft forever
root@paris-VirtualBox:/home/paris#
```

From here we have a kalibox on 4.x/24 subnet and a vulnerable debiandesktop on the 4.x/24 subnet. They can communicate with one another.

SSH enabled for attack simulation on Debian Desktop

```
paris@paris-VirtualBox:~$ sudo systemctl start ssh
Failed to start ssh.service: Unit ssh.service not found.
paris@paris-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm17t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 211 not upgraded.
Need to get 1,737 kB of archives.
After this operation, 6,743 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
paris@paris-VirtualBox:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/system
d/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.s
ervice.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/l
ib/systemd/system/ssh.service.
paris@paris-VirtualBox:~$
```

```
paris@paris-VirtualBox:~$ sudo systemctl start ssh
paris@paris-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
     Active: active (running) since Sat 2025-07-05 19:19:30 EDT; 7s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 4871 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4872 (sshd)
      Tasks: 1 (limit: 4605)
     Memory: 1.2M (peak: 1.5M)
        CPU: 17ms
     CGroup: /system.slice/ssh.service
             └─4872 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 05 19:19:30 paris-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Sec>
Jul 05 19:19:30 paris-VirtualBox sshd[4872]: Server listening on :: port 22.
Jul 05 19:19:30 paris-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secu>
lines 1-17/17 (END)
```

Verified changes via nmap on attack machine

```
┌──(alcbec㉿proxkali)-[~]
└─$ nmap -Pn 192.168.4.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 19:20 EDT
Nmap scan report for 192.168.4.71
Host is up (0.00090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:B1:40:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

The meat and potatoes is upnext.

Reconnaissance/Intelligence Gathering (Pre Access)

Locate endpoints on a network

arp.txt - arp scan

```
┌──(root㉿proxkali)-[~alcbec/Documents]
└─# arp-scan --interface=eth0 --localnet > arp.txt
```

scan.txt & scan2.txt - nmap ping sweep

```
┌──(root㉿proxkali)-[~alcbec/Documents]
└─# nmap -sn 192.168.4.0/24 > scan2.txt
```

```
┌──(root㉿proxkali)-[~alcbec/Documents]
└─# nmap -sn 192.168.4.1/24 > scan.txt
```

netdiscover.txt - netdiscover passive listening

```
┌──(root㉿proxkali)-[~alcbec/Documents]
└─# netdiscover -r 192.168.4.0/24 > netdiscover.txt
```

Scanning/Vulnerability Analysis(Pre Access)

Identify open ports and services on a target

```
┌──(alcbec㉿proxkali)-[~]
└─$ nmap -sS -sV -T4 -Pn 192.168.4.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 19:10 EDT
Nmap scan report for 192.168.4.71
Host is up (0.00089s latency).
All 1000 scanned ports on 192.168.4.71 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:B1:40:EA (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds
```

^prior to ssh being setup

```
┌──(alcbec㉿proxkali)-[~]
└─$ nmap -sS -sV -T4 -Pn 192.168.4.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 19:22 EDT
Nmap scan report for 192.168.4.71
Host is up (0.0010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; proto
col 2.0)
MAC Address: 08:00:27:B1:40:EA (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.65 seconds
```

^following the [set up of ssh]

Identify operating system of target

```
┌──(alcbec㉿proxkali)-[~]
└─$ nmap -O 192.168.4.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 19:12 EDT
Nmap scan report for 192.168.4.71
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.4.71 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:B1:40:EA (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
```

```
┌──(alcbec㉿proxkali)-[~]
└─$ nmap -O --osscan-guess 192.168.4.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-05 19:32 EDT
Nmap scan report for 192.168.4.71
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:B1:40:EA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
```

Exploitation

Exploit poor credential management to gain SSH access
Create vulnerable user accounts with common passwords for brute forcing

Post Exploitation

Enumeration(Post Access)

Enumerate network information from files on target

Networking Files

```
testuser@paris-VirtualBox:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 paris-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
testuser@paris-VirtualBox:/etc/NetworkManager$ cat /etc/NetworkManager/Netwo
rkManager.conf
[main]
plugins=ifupdown,keyfile

[ifupdown]
managed=false

[device]
wifi.scan-rand-mac-address=no
```

```
testuser@paris-VirtualBox:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-reso
lved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but
only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in
a
# different way, replace this symlink by a static file or a different symli
nk.
#
# See man:systemd-resolved.service(8) for details about the supported modes
 of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search .
```

Enumerate system information on target

OS & Kernel version

```
testuser@paris-VirtualBox:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.1 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.1 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy
-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

```
testuser@paris-VirtualBox:~$ cat /etc/issue
Ubuntu 24.04.1 LTS \n \l
```

Gather user account information on target

```
testuser@paris-VirtualBox:~$ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
paris:x:1000:1000:paris:/home/paris:/bin/bash
test:x:1001:1001::/home/test:/bin/bash
ohno:x:1002:1002:,,,:/home/ohno:/bin/bash
testuser:x:1003:1003:,,,:/home/testuser:/bin/bash
```

Data Exfiltration

Extract password hashes or sensitive files for offline cracking

Compile information from files on target & **Transfer files to and from target**

Attacker was able to exploit poor credential management on the victim machine to establish an ssh connection.

```
┌──(alcbec㉿proxkali)-[~]
└─$ ssh testuser@192.168.4.71
testuser@192.168.4.71's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.0-29-generic x86_64)
```

Below is a comparison of "ls" output in the ssh conenction prior to first sign in. I want to later investigate what is inside of '/home/testuser/snap' on a new profile.

```
testuser@paris-VirtualBox:~$ pwd
/home/testuser
testuser@paris-VirtualBox:~$ ls
snap
testuser@paris-VirtualBox:~$ ls
Desktop    Downloads  Pictures  snap       Videos
Documents  Music      Public    Templates
testuser@paris-VirtualBox:~$
```

Compiling/Outputting a file in a stealthy location to simulate real world data exfiltration

```
testuser@paris-VirtualBox:/tmp$ cp /var/log/dpkg.log  /tmp/vulndebian_dpkg-o
utput.txt
testuser@paris-VirtualBox:/tmp$
```

Exfiltrating file to Kali via scp

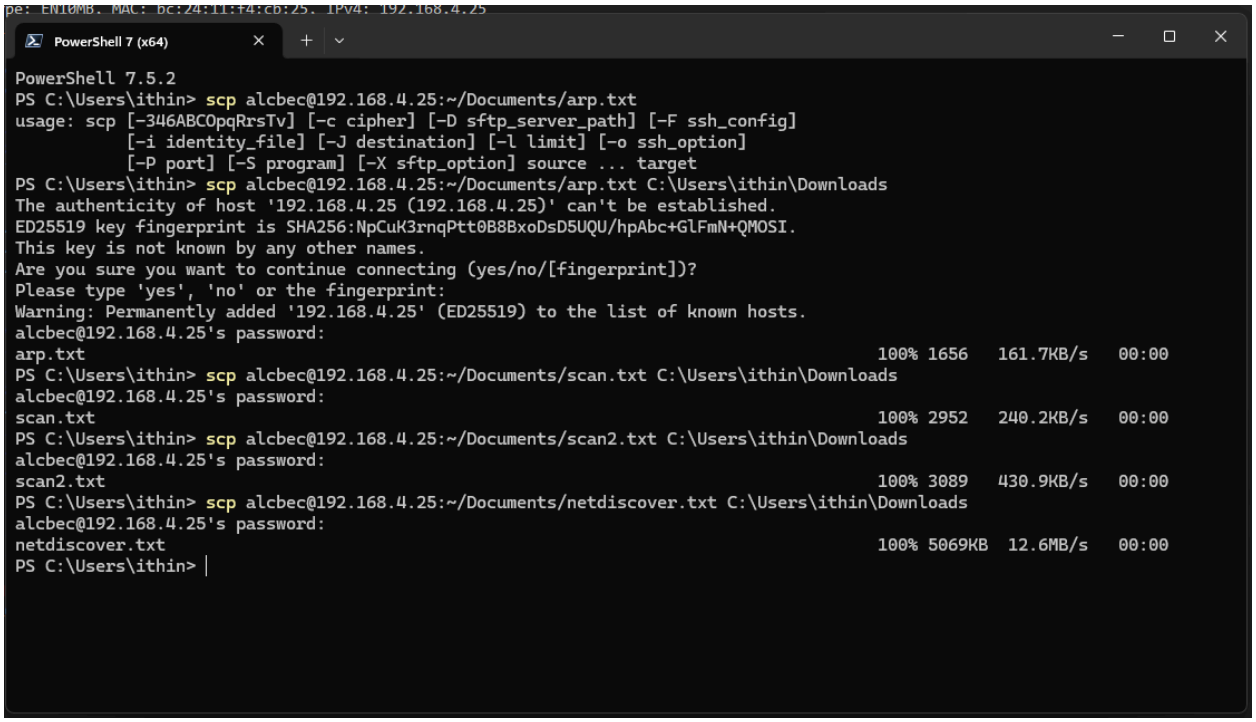
```
testuser@paris-VirtualBox:~$ scp testuser@192.168.4.71:/home/testuser/tmp/vu
lndebian_dpkg-output.txt ~/Desktop
The authenticity of host '192.168.4.71 (192.168.4.71)' can't be established.
ED25519 key fingerprint is SHA256:nwO5z+mcIrKTmDNKSJIcHO3fnCKuAWW+1uPx8vyC4O
U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.4.71' (ED25519) to the list of known hos
ts.
testuser@192.168.4.71's password:
scp: /home/testuser/tmp/vulndebian_dpkg-output.txt: No such file or director
y
```

```
testuser@paris-VirtualBox:/tmp$ scp testuser@192.168.4.71:/tmp/vulndebian_dp
kg-output.txt ~/Desktop
testuser@192.168.4.71's password:
vulndebian_dpkg-output.txt                    100% 1078KB 182.9MB/s   00:00
testuser@paris-VirtualBox:/tmp$
```

Setting up Secure Copy over SSH - Secure FIle Transfer to Host

Within Kali: sudo systemctl start ssh

Within requesting machine: scp alcbec@192.168.4.25:~/Documents/'targetfile'.txt C:\Users\yourprofile\Downloads\



Lessons Learned/Reflection

- Installing VMs takes forever (talking to you kali & parrotOS)
- Netdiscover proved effective to list/discover devices by listening for arp requests on the LAN passively. Enabled with ability to have insights in volume, mac address ip and vendor.
- Arp-scan can send actively requests and record their responses with ip/mac info to enumerate active devices for ip address, mac address and vendor
- Nmap -sn performed host discovery using an ARP request determining who has IPs within the subnet, logging up IPs and their MAC addresses & vendor
- More to be added ……..

Appendix

Raw Output arp.txt

Interface: eth0, type: EN10MB, MAC: bc:24:11:f4:cb:25, IPv4: 192.168.4.25
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.4.1 30:57:8e:5d:ff:12 eero inc.
192.168.4.15 04:d4:c4:6f:53:2d ASUSTek COMPUTER INC.
192.168.4.20 04:d4:c4:8f:4c:22 ASUSTek COMPUTER INC.
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate
192.168.4.40 40:a9:cf:d7:6c:d8 Amazon Technologies Inc.
192.168.4.66 ec:8a:c4:01:16:a4 Amazon Technologies Inc.
192.168.4.53 08:7c:39:02:e5:2e Amazon Technologies Inc.
192.168.4.52 c8:3a:6b:e5:62:f4 Roku, Inc
192.168.4.22 88:57:1d:7d:57:aa Seongji Industry Company
192.168.4.36 c8:47:8c:10:37:76 Beken Corporation
192.168.4.35 c8:47:8c:01:31:43 Beken Corporation
192.168.4.37 c8:47:8c:01:31:86 Beken Corporation
192.168.4.54 10:59:32:eb:1f:1b Roku, Inc
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate (DUP: 2)
192.168.4.41 cc:6a:10:28:2a:67 The Chamberlain Group, Inc
192.168.4.50 40:ca:63:c3:3b:7a Seongji Industry Company
192.168.4.51 40:ca:63:bf:f8:5e Seongji Industry Company
192.168.4.64 70:89:76:c7:c8:cb Tuya Smart Inc.
192.168.4.67 c8:47:8c:40:2b:2c Beken Corporation
192.168.4.84 6c:29:90:f9:b6:3c WiZ Connected Lighting Company Limited
192.168.4.91 2c:aa:8e:58:41:87 Wyze Labs Inc
192.168.4.73 2c:aa:8e:3c:c7:b9 Wyze Labs Inc
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate (DUP: 3)
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate (DUP: 4)
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate (DUP: 5)
192.168.4.57 c8:34:8e:53:ca:5d Intel Corporate (DUP: 6)

26 packets received by filter, 0 packets dropped by kernel

Ending arp-scan 1.10.0: 256 hosts scanned in 4.331 seconds (59.11 hosts/sec). 21 responded

Raw Output scan2.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2025-07-02 01:49 EDT
Nmap scan report for 192.168.4.1
Host is up (0.023s latency).
MAC Address: 30:57:8E:5D:FF:12 (eero)
Nmap scan report for 192.168.4.15
Host is up (0.00022s latency).
MAC Address: 04:D4:C4:6F:53:2D (ASUSTek Computer)
Nmap scan report for 192.168.4.20
Host is up (0.0022s latency).
MAC Address: 04:D4:C4:8F:4C:22 (ASUSTek Computer)
Nmap scan report for 192.168.4.22
Host is up (0.12s latency).
MAC Address: 88:57:1D:7D:57:AA (Seongji Industry Company)
Nmap scan report for 192.168.4.35
Host is up (0.023s latency).
MAC Address: C8:47:8C:01:31:43 (Beken)
Nmap scan report for 192.168.4.36
Host is up (0.066s latency).
MAC Address: C8:47:8C:10:37:76 (Beken)
Nmap scan report for 192.168.4.37
Host is up (0.090s latency).
MAC Address: C8:47:8C:01:31:86 (Beken)
Nmap scan report for 192.168.4.40
Host is up (1.4s latency).
MAC Address: 40:A9:CF:D7:6C:D8 (Amazon Technologies)
Nmap scan report for 192.168.4.41
Host is up (0.10s latency).
MAC Address: CC:6A:10:28:2A:67 (The Chamberlain Group)
Nmap scan report for 192.168.4.50
Host is up (0.11s latency).

MAC Address: 40:CA:63:C3:3B:7A (Seongji Industry Company)
Nmap scan report for 192.168.4.51
Host is up (0.098s latency).
MAC Address: 40:CA:63:BF:F8:5E (Seongji Industry Company)
Nmap scan report for 192.168.4.53
Host is up (0.14s latency).
MAC Address: 08:7C:39:02:E5:2E (Amazon Technologies)
Nmap scan report for 192.168.4.54
Host is up (0.047s latency).
MAC Address: 10:59:32:EB:1F:1B (Roku)
Nmap scan report for 192.168.4.57
Host is up.
MAC Address: C8:34:8E:53:CA:5D (Intel Corporate)
Nmap scan report for 192.168.4.64
Host is up (0.060s latency).
MAC Address: 70:89:76:C7:C8:CB (Tuya Smart)
Nmap scan report for 192.168.4.66
Host is up (0.0084s latency).
MAC Address: EC:8A:C4:01:16:A4 (Amazon Technologies)
Nmap scan report for 192.168.4.67
Host is up (0.056s latency).
MAC Address: C8:47:8C:40:2B:2C (Beken)
Nmap scan report for 192.168.4.73
Host is up (0.12s latency).
MAC Address: 2C:AA:8E:3C:C7:B9 (Wyze Labs)
Nmap scan report for 192.168.4.82
Host is up (0.035s latency).
MAC Address: D8:EB:46:B1:61:1E (Google)
Nmap scan report for 192.168.4.84
Host is up (0.19s latency).
MAC Address: 6C:29:90:F9:B6:3C (WiZ Connected Lighting Company Limited)
Nmap scan report for 192.168.4.85
Host is up (0.038s latency).
MAC Address: A8:BB:50:83:1B:11 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.86

Host is up (0.19s latency).
MAC Address: A8:BB:50:C3:D7:82 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.88
Host is up (0.097s latency).
MAC Address: A8:BB:50:C3:AC:49 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.89
Host is up (0.18s latency).
MAC Address: A8:BB:50:E5:D6:A8 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.90
Host is up (0.19s latency).
MAC Address: A8:BB:50:C3:AC:A6 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.91
Host is up (0.033s latency).
MAC Address: 2C:AA:8E:58:41:87 (Wyze Labs)
Nmap scan report for 192.168.4.25
Host is up.
Nmap done: 256 IP addresses (27 hosts up) scanned in 10.57 seconds

Raw Output scan.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2025-07-02 01:43 EDT
Nmap scan report for 192.168.4.1
Host is up (0.0052s latency).
MAC Address: 30:57:8E:5D:FF:12 (eero)
Nmap scan report for 192.168.4.15
Host is up (0.00028s latency).
MAC Address: 04:D4:C4:6F:53:2D (ASUSTek Computer)
Nmap scan report for 192.168.4.20
Host is up (0.0015s latency).
MAC Address: 04:D4:C4:8F:4C:22 (ASUSTek Computer)
Nmap scan report for 192.168.4.35
Host is up (0.078s latency).
MAC Address: C8:47:8C:01:31:43 (Beken)
Nmap scan report for 192.168.4.36
Host is up (0.098s latency).

MAC Address: C8:47:8C:10:37:76 (Beken)
Nmap scan report for 192.168.4.37
Host is up (0.084s latency).
MAC Address: C8:47:8C:01:31:86 (Beken)
Nmap scan report for 192.168.4.40
Host is up (0.0023s latency).
MAC Address: 40:A9:CF:D7:6C:D8 (Amazon Technologies)
Nmap scan report for 192.168.4.41
Host is up (0.099s latency).
MAC Address: CC:6A:10:28:2A:67 (The Chamberlain Group)
Nmap scan report for 192.168.4.50
Host is up (0.088s latency).
MAC Address: 40:CA:63:C3:3B:7A (Seongji Industry Company)
Nmap scan report for 192.168.4.51
Host is up (0.092s latency).
MAC Address: 40:CA:63:BF:F8:5E (Seongji Industry Company)
Nmap scan report for 192.168.4.52
Host is up (0.14s latency).
MAC Address: C8:3A:6B:E5:62:F4 (Roku)
Nmap scan report for 192.168.4.53
Host is up (0.14s latency).
MAC Address: 08:7C:39:02:E5:2E (Amazon Technologies)
Nmap scan report for 192.168.4.54
Host is up (0.19s latency).
MAC Address: 10:59:32:EB:1F:1B (Roku)
Nmap scan report for 192.168.4.57
Host is up.
MAC Address: C8:34:8E:53:CA:5D (Intel Corporate)
Nmap scan report for 192.168.4.64
Host is up (0.15s latency).
MAC Address: 70:89:76:C7:C8:CB (Tuya Smart)
Nmap scan report for 192.168.4.66
Host is up (0.0056s latency).
MAC Address: EC:8A:C4:01:16:A4 (Amazon Technologies)
Nmap scan report for 192.168.4.67

Host is up (0.099s latency).
MAC Address: C8:47:8C:40:2B:2C (Beken)
Nmap scan report for 192.168.4.73
Host is up (0.16s latency).
MAC Address: 2C:AA:8E:3C:C7:B9 (Wyze Labs)
Nmap scan report for 192.168.4.82
Host is up (0.056s latency).
MAC Address: D8:EB:46:B1:61:1E (Google)
Nmap scan report for 192.168.4.84
Host is up (0.19s latency).
MAC Address: 6C:29:90:F9:B6:3C (WiZ Connected Lighting Company Limited)
Nmap scan report for 192.168.4.85
Host is up (0.029s latency).
MAC Address: A8:BB:50:83:1B:11 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.86
Host is up (0.19s latency).
MAC Address: A8:BB:50:C3:D7:82 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.88
Host is up (0.071s latency).
MAC Address: A8:BB:50:C3:AC:49 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.90
Host is up (0.18s latency).
MAC Address: A8:BB:50:C3:AC:A6 (WiZ IoT Company Limited)
Nmap scan report for 192.168.4.91
Host is up (0.19s latency).
MAC Address: 2C:AA:8E:58:41:87 (Wyze Labs)
Nmap scan report for 192.168.4.25
Host is up.
Nmap done: 256 IP addresses (26 hosts up) scanned in 4.04 seconds

Raw Output netdiscover.txt

1245 Captured ARP Req/Rep packets, from 35 hosts. Total size: 90614

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.4.15	04:d4:c4:6f:53:2d	1	42	ASUSTek COMPUTER INC.
192.168.4.20	04:d4:c4:8f:4c:22	5	300	ASUSTek COMPUTER INC.
192.168.4.40	40:a9:cf:d7:6c:d8	23	1646	Amazon Technologies Inc.
192.168.4.66	ec:8a:c4:01:16:a4	17	1202	Amazon Technologies Inc.
192.168.4.41	cc:6a:10:28:2a:67	1	60	The Chamberlain Group, Inc
192.168.4.52	c8:3a:6b:e5:62:f4	1	60	Roku, Inc
192.168.4.53	08:7c:39:02:e5:2e	1	60	Amazon Technologies Inc.
192.168.4.82	d8:eb:46:b1:61:1e	1	60	Google, Inc.
192.168.4.51	40:ca:63:bf:f8:5e	1	60	Seongji Industry Company
192.168.4.50	40:ca:63:c3:3b:7a	2	120	Seongji Industry Company
192.168.4.22	88:57:1d:7d:57:aa	75	5536	Seongji Industry Company
192.168.4.36	c8:47:8c:10:37:76	3	208	Beken Corporation
192.168.4.35	c8:47:8c:01:31:43	12	874	Beken Corporation
192.168.4.37	c8:47:8c:01:31:86	8	578	Beken Corporation
192.168.4.54	10:59:32:eb:1f:1b	2	134	Roku, Inc
192.168.4.57	c8:34:8e:53:ca:5d	1	60	Intel Corporate
192.168.4.64	70:89:76:c7:c8:cb	4	282	Tuya Smart Inc.
192.168.4.67	c8:47:8c:40:2b:2c	7	504	Beken Corporation
192.168.4.73	2c:aa:8e:3c:c7:b9	1	60	Wyze Labs Inc
192.168.4.34	38:1f:8d:ab:0f:d6	12	888	Tuya Smart Inc.
192.168.6.147	c4:82:e1:4d:df:99	9	666	Unknown vendor
192.168.6.103	7c:78:b2:ca:04:a7	24	1776	Wyze Labs Inc
192.168.4.84	6c:29:90:f9:b6:3c	26	1924	WiZ Connected Lighting Company Limited
192.168.4.33	c8:47:8c:30:29:6c	13	962	Beken Corporation
192.168.4.68	c8:47:8c:40:2a:02	16	1184	Beken Corporation
192.168.6.70	fc:d7:49:2d:3f:6b	22	1586	Amazon Technologies Inc.

References

https://ine.com/security/certifications/ejpt-certification
https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/
https://phoenixnap.com/kb/how-to-list-users-linux
https://www.reddit.com/r/OracleVMVirtualBox/comments/11sfn62/how_to_exit_full_screen_on_virtualbox/
https://forums.virtualbox.org/viewtopic.php?t=18657
https://www.stationx.net/nmap-cheat-sheet/
Nmcli is NetworkManager
http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
https://owasp.org/www-project-web-security-testing-guide/v42/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
https://www.nist.gov/privacy-framework/nist-sp-800-115
https://www.stationx.net/penetration-testing-steps/
https://www.compassitc.com/blog/penetration-testing-phases-steps-in-the-process
https://www.stationx.net/penetration-testing-methodologies/