Lab 01 Report

Name: Madene Meriem Group : 01

October 15, 2025

Objective

Lab Title: Exploring Kali linux and Metasploit vms
Main Goal: Understanding basics about exploring machines with nmap

Environment Setup

Virtual Machines:

VM Name	IP Address
Kali Linux	192.168.153.128
Metasploitable2	192.168.153.129

Tools Used:

- `ip a` and `ifconfig` for network configurations
- `ping`
- `nmap`

Task 1: Startup and Network Checks

Description:
Network check in both machines (checking the network configurations and ip addresses)
Commands Executed:

```
$ ip a
$ ifconfig
```

Delivrables:

```
msfadmin@metasploitable: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:3e:23:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.153.129/24 brd 192.168.153.255 scope global eth0
    inet6 fe80::20c:29ff:fe3e:23ce/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:3e:23:d8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.8/24 brd 192.168.20.255 scope global eth1
    inet6 fe80::20c:29ff:fe3e:23d8/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

```
root@kali:~# ip q
Object "q" is unknown, try "ip help".
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1
    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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:0c:29:f0:f5:53 brd ff:ff:ff:ff:ff:ff
    inet 192.168.153.128/24 brd 192.168.153.255 scope global dynamic eth0
       valid_lft 1526sec preferred_lft 1526sec
    inet6 fe80::20c:29ff:fef0:f553/64 scope link
       valid_lft forever preferred_lft forever
root@kali:~#
```

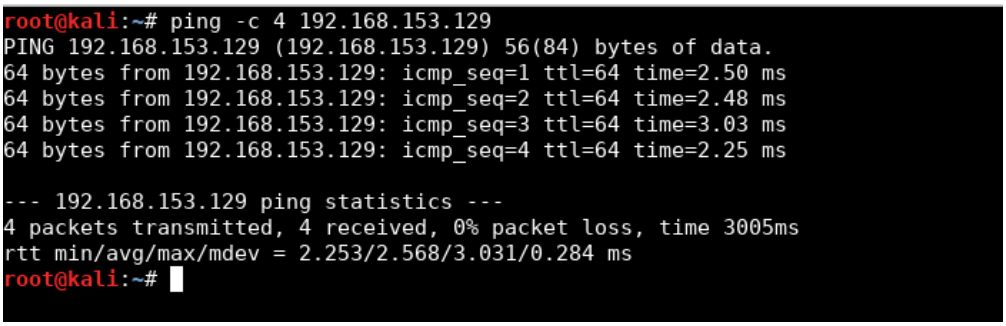
Key Findings:
Ip address of the metasploit machine : 192.168.153.129 Ip address of the kali machine : 192.168.153.128 **Analysis:**
Based on the results of the previous commands , we can notice that the two machines are in the same network (192.168.153.0/24) which means there might be a connectivity between them

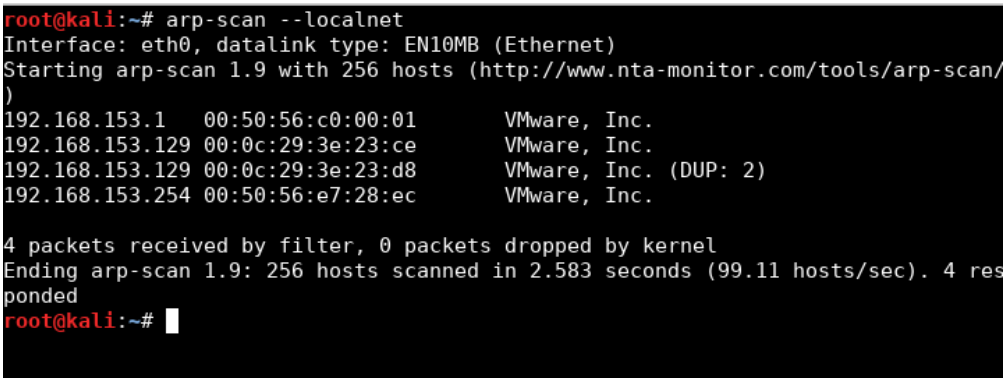
Task 2: Discovery and Quick scan

Description:
Testing the connectivity between the two machines and checking if there is any open ports in the metasploit machine **Commands Executed:**

```
$ ping -c 4 192.168.153.129
$ arp-scan --localhost
$ nmap -sC -sV -p 1-1000 192.168.153.128
```

Delivrables:






```
root@kali:~# nmap -sC -sV -p 1-1000 192.168.153.129 -oN nmap_result.txt

Starting Nmap 7.50 ( https://nmap.org ) at 2025-10-14 13:31 EDT
Nmap scan report for 192.168.153.129
Host is up (0.0055s latency).
Not shown: 988 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet?
25/tcp  open  smtp?
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
|_ssl-date: 2025-10-14T16:59:18+00:00; -35m42s from scanner time.
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

```
|   program version    port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      50088/udp  mountd
|   100005  1,2,3      50497/tcp  mountd
|   100021  1,3,4      41415/tcp  nlockmgr
|   100021  1,3,4      47214/udp  nlockmgr
|   100024  1          38253/tcp  status
|_  100024  1          41836/udp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec?
513/tcp open  login?
514/tcp open  shell?
MAC Address: 00:0C:29:3E:23:CE (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -35m42s, deviation: 0s, median: -35m42s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-10-14T12:59:04-04:00

Service detection performed. Please report any incorrect results at https://n
```

Key Findings:

- Successful ping from kali to metasploit
- The arp discovery shows that the kali has the MAC address of the metasploit machine
- Open ports in the result of nmap + use of old services

Analysis:
We notice that there is a successful connectivity between the two machine, and the kali machine has the MAC address of the metasploit machine as shown in the ARP table. Nmap shows many open ports that can be exploited like rsh, rlogin, etc. The machine also uses old services that can be vulnerable for many exploits. FTP protocol is anonymous which means we can download and upload files without entering any credentials and this could lead to severe problems.

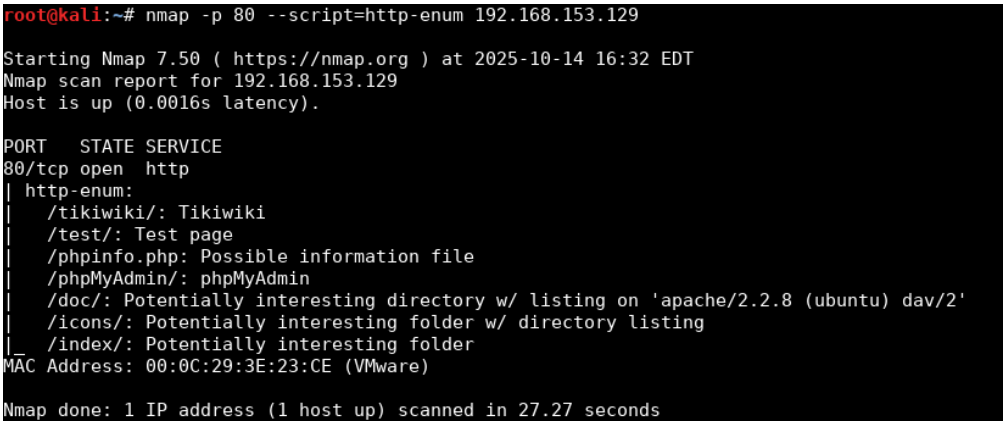
Task 3: Targeted scanning & non-destructive interactions

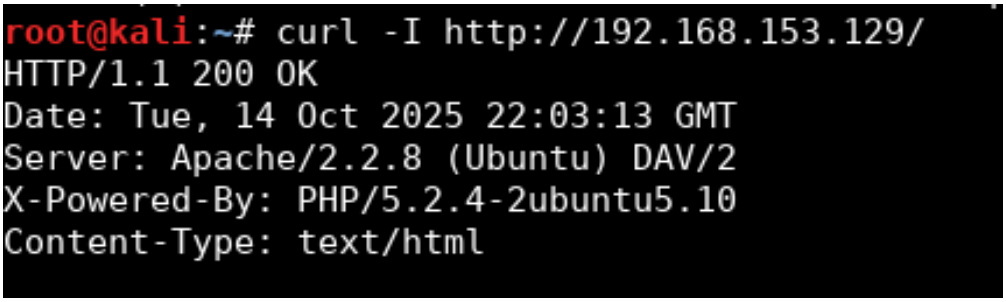
Description:
Scanning open ports and services in the target machine to check vulnerabilites and privacy breachs that can be used in malicious behaviors.

Commands Executed:

```
$ nmap -p 80 --script=http-enum 192.168.153.129
$ ftp 192.168.153.129
$ curl -I http://192.168.153.129
$ curl -I http://192.168.153.129/ > index.html
```

Delivrables:





Key Findings:

- Nmap scan finds many exposed endpoints
- Successful login in ftp, no files shown in the ls result
- Successful Get request
- Saved the result of the request in an html file

Analysis:
Open ports and old services which are vulnerable to exploit, for example port 80 for http. No permission to check the files with ls command in ftp. FTP accepted login with anonymous, meaning there is a privacy breach. Successful http request replied with the request header from Apache server powered by an old PHP version that is known to be vulnerable as it is outdated.

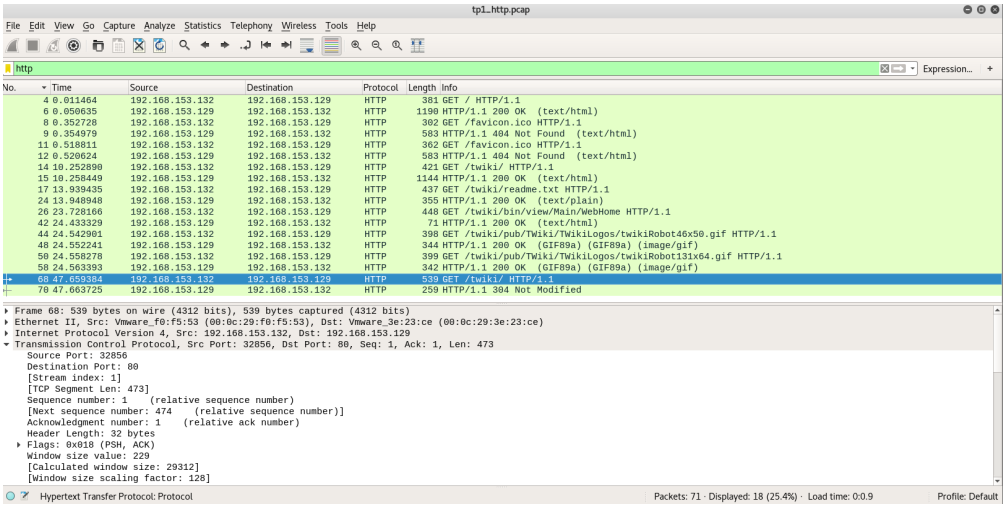
Task 4: Quick capture & analysis (tcpdump / Wireshark)

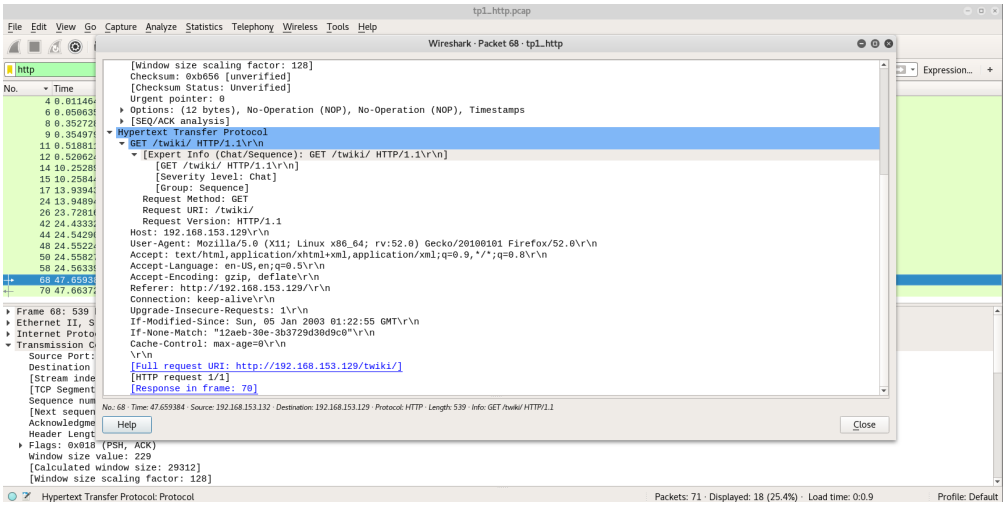
Description:
Capturing packets while visiting the url http://192.168.153.129/ and observing and filtering them with wireshark to see the packets behavior.

Commands Executed:

```
$ tcpdump -i eth0 port 80 -w tp1_http.pcap
```

Delivrables:





Key Findings:

- Capturing 71 packets while visiting the previous url
- Filtering the packets in wireshark and observing headers and payloads

Analysis:
Answers to the analytical questions:

- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
- No cookies were shown in the requests
- The GET request made was for /twiki/: GET /twiki/ HTTP/1.1

Conclusion

Summary:
The objective of this lab was to check connectivity between two machines and find out any possible ways to get information from the target machine. We find out many popular ports open (like http, tcp, ftp, etc.) as well as the use of outdated and old services (ftp, ssh, etc.). These privacy breaches could lead to exploitations and threats. The capture was made over HTTP traffic. Unlike HTTPS, this protocol is unencrypted so we can see all the requests and the responses in clear (html files, file types, etc.) which is not secure.

Security Implications:

- Unencrypted http traffic can make anyone in the network see the request and its content
- The use of outdated server lead to many vulnerabilities
- FTP accepting the anonymous login is very risky and vulnerable

Lessons Learned:

- Always use updated services
- Limit the open ports and services to avoid attacks
- Use HTTPS the encrypted protocol