Network Scanning Report for Metasploitable-Linux-2.0.0

-By

Felicia.R.P

2nd yr BE Computer Science

Abstract:

This report presents a comprehensive overview of the network scanning conducted on the Metasploitable-Linux-2.0.0 system. The primary objective was to assess the security posture of the target by identifying its IP range, scanning for open ports, evaluating running services, extracting version information, and determining the underlying operating system. Additionally, the report explores techniques for bypassing security devices and emphasizes the importance of selecting the right type of scan.

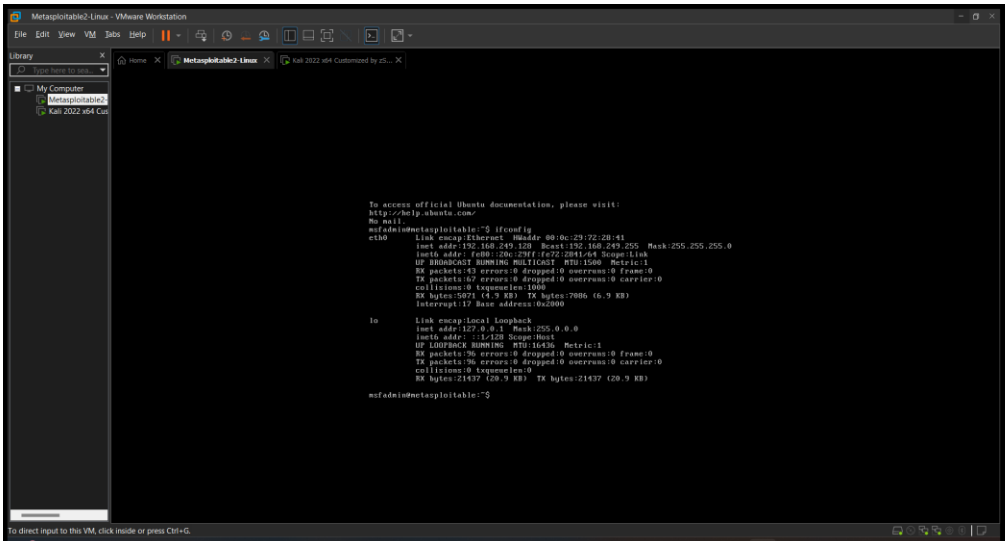
1. Introduction:

Network scanning is a critical phase in cybersecurity assessments aimed at identifying potential vulnerabilities within a system. The target for this analysis is Metasploitable-Linux-2.0.0, a purposely vulnerable virtual machine designed for penetration testing.

2. Methodology:

2.1 Aim Your Target:

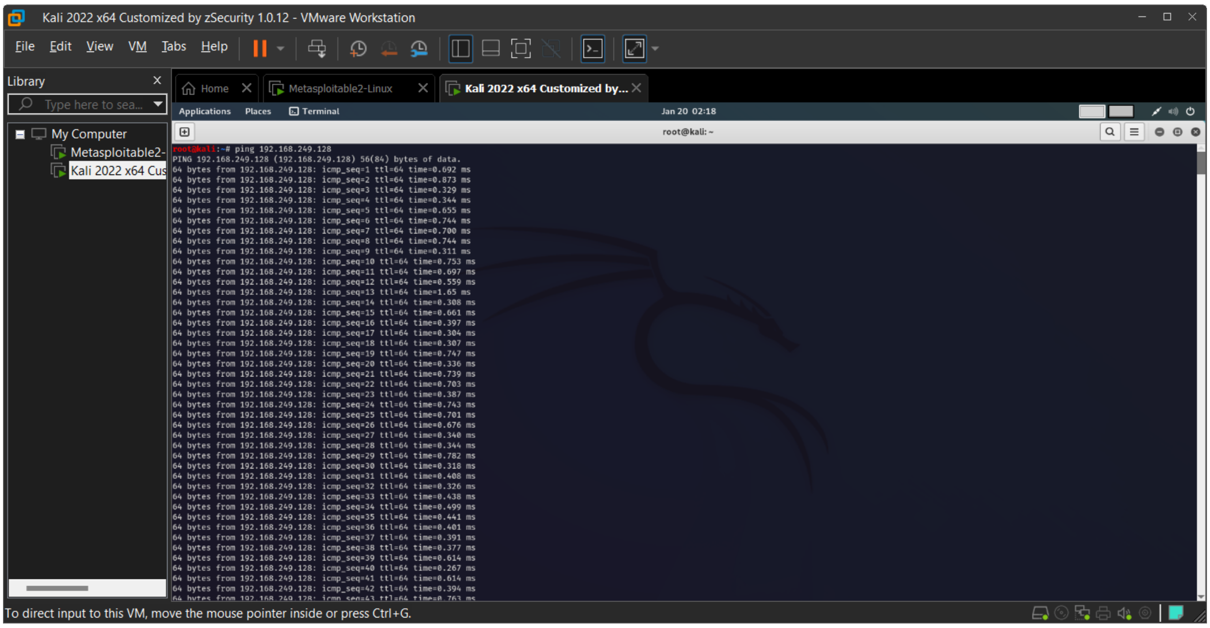
Define the scope of the scan and identify the specific goals. In this case, the objective is to assess the security of Metasploitable-Linux-2.0.0, focusing on IP range, open ports, services, and the operating system**.**


Metasploitable2-Linux - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to sea...
My Computer
Metasploitable2-
Kali 2022 x64 Cus
Home
Metasploitable2-Linux
Kali 2022 x64 Customized by zS...
To direct input to this VM, click inside or press Ctrl+G.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:72:28:41
          inet addr:192.168.249.128  Bcast:192.168.249.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe72:2841/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5071 (4.9 KB)  TX bytes:7086 (6.9 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$
```

2.2 Scan for IP Range:

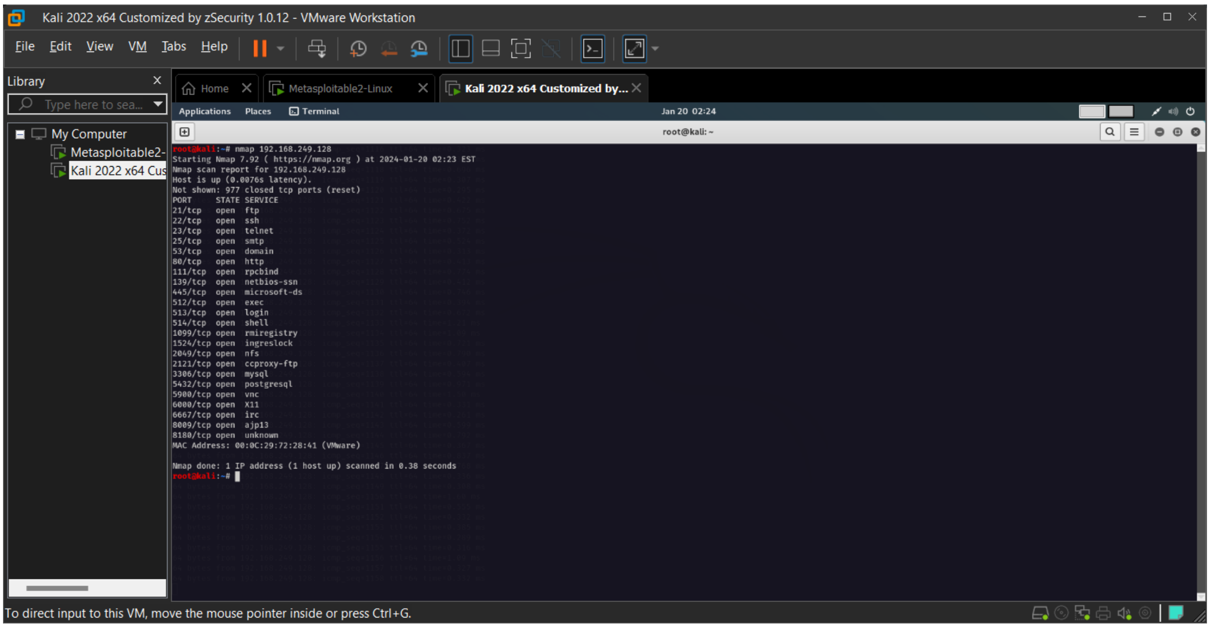
Utilize network discovery tools such as Nmap to identify the IP addresses within the target's range. This step helps in mapping the network infrastructure.


Kali 2022 x64 Customized by zSecurity 1.0.12 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2-
Kali 2022 x64 Cus
Home
Metasploitable2-Linux
Kali 2022 x64 Customized by...
Applications Places Terminal
Jan 20 02:18
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
root@kali:~# ping 192.168.249.128
PING 192.168.249.128 (192.168.249.128) 56(84) bytes of data.
64 bytes from 192.168.249.128: icmp_seq=1 ttl=64 time=0.692 ms
64 bytes from 192.168.249.128: icmp_seq=2 ttl=64 time=0.873 ms
64 bytes from 192.168.249.128: icmp_seq=3 ttl=64 time=0.329 ms
64 bytes from 192.168.249.128: icmp_seq=4 ttl=64 time=0.344 ms
64 bytes from 192.168.249.128: icmp_seq=5 ttl=64 time=0.655 ms
64 bytes from 192.168.249.128: icmp_seq=6 ttl=64 time=0.744 ms
64 bytes from 192.168.249.128: icmp_seq=7 ttl=64 time=0.700 ms
64 bytes from 192.168.249.128: icmp_seq=8 ttl=64 time=0.744 ms
64 bytes from 192.168.249.128: icmp_seq=9 ttl=64 time=0.311 ms
64 bytes from 192.168.249.128: icmp_seq=10 ttl=64 time=0.753 ms
64 bytes from 192.168.249.128: icmp_seq=11 ttl=64 time=0.697 ms
64 bytes from 192.168.249.128: icmp_seq=12 ttl=64 time=0.559 ms
64 bytes from 192.168.249.128: icmp_seq=13 ttl=64 time=1.65 ms
64 bytes from 192.168.249.128: icmp_seq=14 ttl=64 time=0.308 ms
64 bytes from 192.168.249.128: icmp_seq=15 ttl=64 time=0.661 ms
64 bytes from 192.168.249.128: icmp_seq=16 ttl=64 time=0.397 ms
64 bytes from 192.168.249.128: icmp_seq=17 ttl=64 time=0.304 ms
64 bytes from 192.168.249.128: icmp_seq=18 ttl=64 time=0.307 ms
64 bytes from 192.168.249.128: icmp_seq=19 ttl=64 time=0.747 ms
64 bytes from 192.168.249.128: icmp_seq=20 ttl=64 time=0.336 ms
64 bytes from 192.168.249.128: icmp_seq=21 ttl=64 time=0.739 ms
64 bytes from 192.168.249.128: icmp_seq=22 ttl=64 time=0.703 ms
64 bytes from 192.168.249.128: icmp_seq=23 ttl=64 time=0.387 ms
64 bytes from 192.168.249.128: icmp_seq=24 ttl=64 time=0.743 ms
64 bytes from 192.168.249.128: icmp_seq=25 ttl=64 time=0.701 ms
64 bytes from 192.168.249.128: icmp_seq=26 ttl=64 time=0.676 ms
64 bytes from 192.168.249.128: icmp_seq=27 ttl=64 time=0.340 ms
64 bytes from 192.168.249.128: icmp_seq=28 ttl=64 time=0.344 ms
64 bytes from 192.168.249.128: icmp_seq=29 ttl=64 time=0.782 ms
64 bytes from 192.168.249.128: icmp_seq=30 ttl=64 time=0.318 ms
64 bytes from 192.168.249.128: icmp_seq=31 ttl=64 time=0.408 ms
64 bytes from 192.168.249.128: icmp_seq=32 ttl=64 time=0.326 ms
64 bytes from 192.168.249.128: icmp_seq=33 ttl=64 time=0.438 ms
64 bytes from 192.168.249.128: icmp_seq=34 ttl=64 time=0.499 ms
64 bytes from 192.168.249.128: icmp_seq=35 ttl=64 time=0.441 ms
64 bytes from 192.168.249.128: icmp_seq=36 ttl=64 time=0.401 ms
64 bytes from 192.168.249.128: icmp_seq=37 ttl=64 time=0.391 ms
64 bytes from 192.168.249.128: icmp_seq=38 ttl=64 time=0.377 ms
64 bytes from 192.168.249.128: icmp_seq=39 ttl=64 time=0.614 ms
64 bytes from 192.168.249.128: icmp_seq=40 ttl=64 time=0.267 ms
64 bytes from 192.168.249.128: icmp_seq=41 ttl=64 time=0.614 ms
64 bytes from 192.168.249.128: icmp_seq=42 ttl=64 time=0.394 ms
64 bytes from 192.168.249.128: icmp_seq=43 ttl=64 time=0.763 ms
```

2.3 Scan for Open Ports:

Conduct a port scan using Nmap to identify open ports on the target. Open ports may indicate services or applications running on the system.


Kali 2022 x64 Customized by zSecurity 1.0.12 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2-
Kali 2022 x64 Cus
Home
Metasploitable2-Linux
Kali 2022 x64 Customized by...
Applications Places Terminal
Jan 20 02:24
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

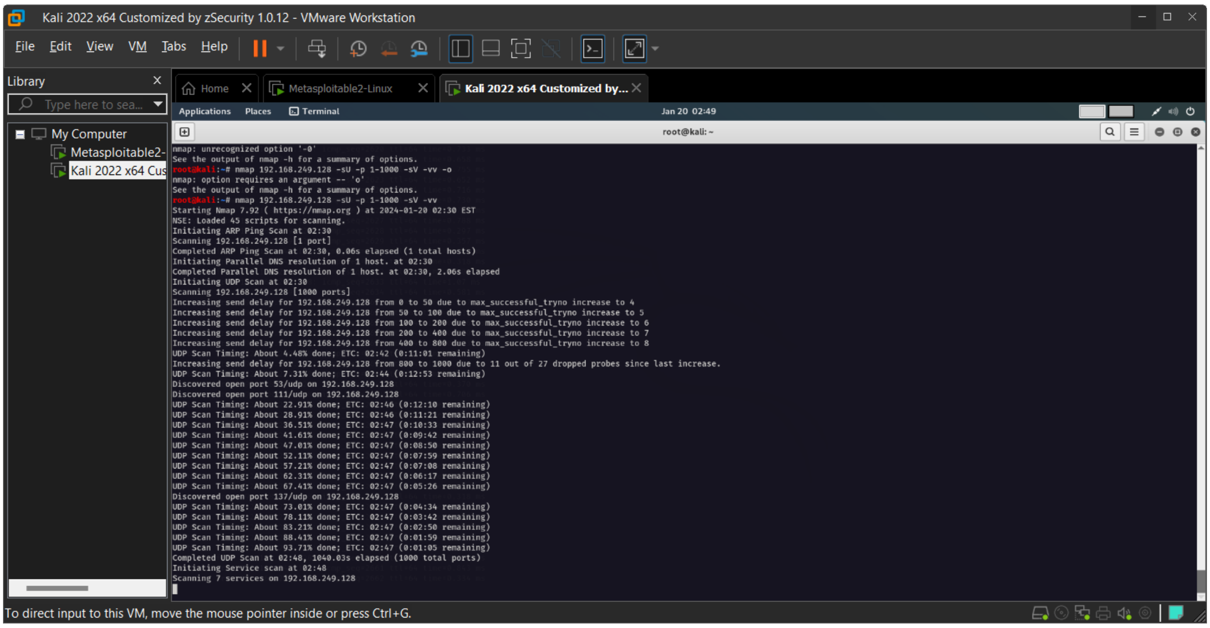
```
root@kali:~# nmap 192.168.249.128
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-20 02:23 EST
Nmap scan report for 192.168.249.128
Host is up (0.0076s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:72:28:41 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~# 
```

2.4 Check for Open Services:

Once open ports are identified, further inspect the services running on these ports. This involves querying services to determine their nature and purpose.

2.5 Grab the Version Running on the Service:

Extract version information from the identified services to assess the potential presence of known vulnerabilities associated with specific software versions.


Kali 2022 x64 Customized by zSecurity 1.0.12 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2-
Kali 2022 x64 Cus
Home
Metasploitable2-Linux
Kali 2022 x64 Customized by...
Applications
Places
Terminal
Jan 20 02:49
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.
root@kali:~# nmap 192.168.249.128 -sU -p 1-1000 -sV -vv -o
nmap: option requires an argument -- 'o'
See the output of nmap -h for a summary of options.
root@kali:~# nmap 192.168.249.128 -sU -p 1-1000 -sV -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-20 02:30 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 02:30
Scanning 192.168.249.128 [1 port]
Completed ARP Ping Scan at 02:30, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:30
Completed Parallel DNS resolution of 1 host. at 02:30, 2.06s elapsed
Initiating UDP Scan at 02:30
Scanning 192.168.249.128 [1000 ports]
Increasing send delay for 192.168.249.128 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.249.128 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.249.128 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.249.128 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.249.128 from 400 to 800 due to max_successful_tryno increase to 8
UDP Scan Timing: About 4.48% done; ETC: 02:42 (0:11:01 remaining)
Increasing send delay for 192.168.249.128 from 800 to 1000 due to 11 out of 27 dropped probes since last increase.
UDP Scan Timing: About 7.31% done; ETC: 02:44 (0:12:53 remaining)
Discovered open port 53/udp on 192.168.249.128
Discovered open port 111/udp on 192.168.249.128
UDP Scan Timing: About 22.91% done; ETC: 02:46 (0:12:10 remaining)
UDP Scan Timing: About 28.91% done; ETC: 02:46 (0:11:21 remaining)
UDP Scan Timing: About 36.51% done; ETC: 02:47 (0:10:33 remaining)
UDP Scan Timing: About 41.61% done; ETC: 02:47 (0:09:42 remaining)
UDP Scan Timing: About 47.01% done; ETC: 02:47 (0:08:50 remaining)
UDP Scan Timing: About 52.11% done; ETC: 02:47 (0:07:59 remaining)
UDP Scan Timing: About 57.21% done; ETC: 02:47 (0:07:08 remaining)
UDP Scan Timing: About 62.31% done; ETC: 02:47 (0:06:17 remaining)
UDP Scan Timing: About 67.41% done; ETC: 02:47 (0:05:26 remaining)
Discovered open port 137/udp on 192.168.249.128
UDP Scan Timing: About 73.01% done; ETC: 02:47 (0:04:34 remaining)
UDP Scan Timing: About 78.11% done; ETC: 02:47 (0:03:42 remaining)
UDP Scan Timing: About 83.21% done; ETC: 02:47 (0:02:50 remaining)
UDP Scan Timing: About 88.41% done; ETC: 02:47 (0:01:59 remaining)
UDP Scan Timing: About 93.71% done; ETC: 02:47 (0:01:05 remaining)
Completed UDP Scan at 02:48, 1040.03s elapsed (1000 total ports)
Initiating Service scan at 02:48
Scanning 7 services on 192.168.249.128
```

2.6 Grab OS:

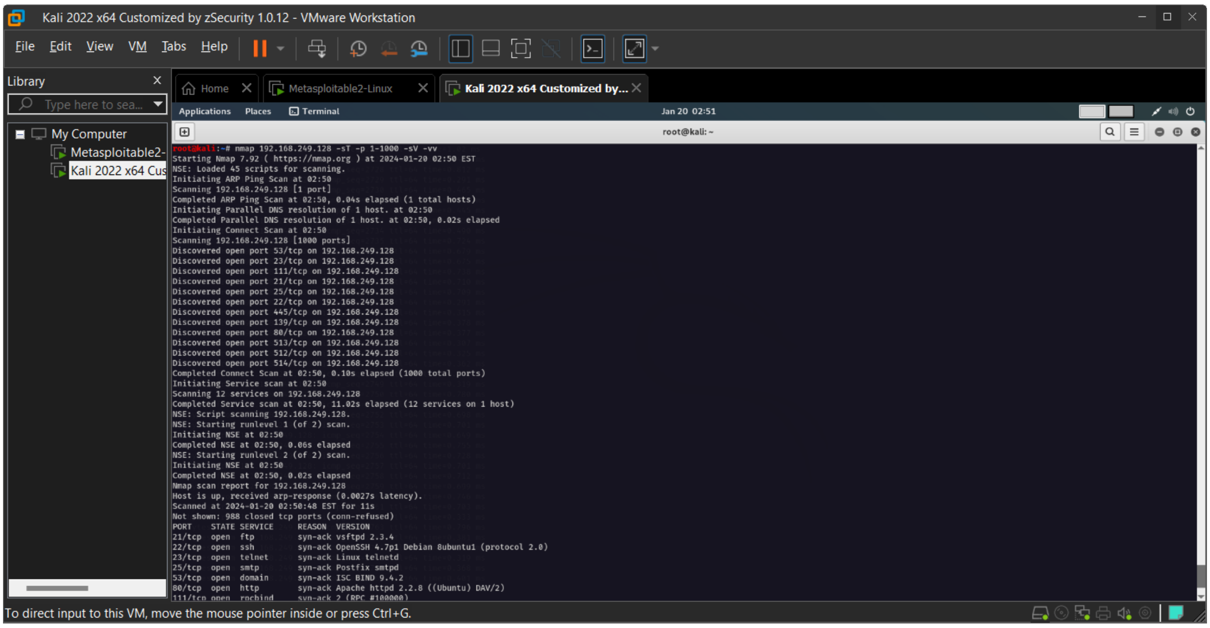
Leverage operating system detection tools to identify the underlying operating system on the target machine. This information is crucial for tailoring subsequent exploitation attempts.

2.7 Bypass Security Devices:

Explore techniques for evading common security devices like firewalls and intrusion detection systems. This step is crucial for simulating real-world scenarios where attackers attempt to bypass security measures.

2.8 Know the Right Type of Scan:

Select the appropriate scanning technique based on the desired level of stealth and thoroughness. Options include TCP scans, UDP scans, and comprehensive scans like SYN scans.


Kali 2022 x64 Customized by zSecurity 1.0.12 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Metasploitable2-
Kali 2022 x64 Cus
Home
Metasploitable2-Linux
Kali 2022 x64 Customized by...
Applications Places Terminal
Jan 20 02:51
root@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
root@kali:~# nmap 192.168.249.128 -sT -p 1-1000 -sV -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-20 02:50 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 02:50
Scanning 192.168.249.128 [1 port]
Completed ARP Ping Scan at 02:50, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:50
Completed Parallel DNS resolution of 1 host. at 02:50, 0.02s elapsed
Initiating Connect Scan at 02:50
Scanning 192.168.249.128 [1000 ports]
Discovered open port 53/tcp on 192.168.249.128
Discovered open port 23/tcp on 192.168.249.128
Discovered open port 111/tcp on 192.168.249.128
Discovered open port 21/tcp on 192.168.249.128
Discovered open port 25/tcp on 192.168.249.128
Discovered open port 22/tcp on 192.168.249.128
Discovered open port 445/tcp on 192.168.249.128
Discovered open port 139/tcp on 192.168.249.128
Discovered open port 80/tcp on 192.168.249.128
Discovered open port 513/tcp on 192.168.249.128
Discovered open port 512/tcp on 192.168.249.128
Discovered open port 514/tcp on 192.168.249.128
Completed Connect Scan at 02:50, 0.10s elapsed (1000 total ports)
Initiating Service scan at 02:50
Scanning 12 services on 192.168.249.128
Completed Service scan at 02:50, 11.02s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.249.128.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 02:50
Completed NSE at 02:50, 0.06s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 02:50
Completed NSE at 02:50, 0.02s elapsed
Nmap scan report for 192.168.249.128
Host is up, received arp-response (0.0027s latency).
Scanned at 2024-01-20 02:50:48 EST for 11s
Not shown: 988 closed tcp ports (conn-refused)
PORT    STATE SERVICE     REASON  VERSION
21/tcp  open  ftp         syn-ack vsftpd 2.3.4
22/tcp  open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      syn-ack Linux telnetd
25/tcp  open  smtp        syn-ack Postfix smtpd
53/tcp  open  domain      syn-ack ISC BIND 9.4.2
80/tcp  open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     syn-ack 2 (RPC #100000)
```

3. Results:

3.1 IP Range:

The scan revealed the IP range of Metasploitable-Linux-2.0.0, providing a foundation for subsequent analysis.

3.2 Open Ports:

Nmap identified open ports, indicating potential entry points for further investigation.

3.3 Open Services:

Analysis of open services revealed information about the applications and protocols in use.

3.4 Version Information:

Extracted version details provided insights into the software running on the target, aiding in vulnerability assessment.

3.5 Operating System:

The operating system detection tool successfully identified the underlying OS of Metasploitable-Linux-2.0.0.

3.6 Bypassing Security Devices:

Various techniques were explored to bypass or circumvent security devices, emphasizing the importance of adapting to the target environment.

3.7 Choosing the Right Scan:

The scan type was selected based on the desired balance between thoroughness and stealth, taking into consideration the potential impact on the target system.

4. Conclusion:

This report outlined the methodology and results of the network scanning conducted on Metasploitable-Linux-2.0.0. The findings provide valuable insights into the target's security posture, enabling further steps in the penetration testing process. It is crucial to continuously update and adapt methodologies to stay ahead of emerging threats and security technologies.

5. Recommendations:

Based on the results, it is recommended to prioritize patching and updating vulnerable software identified during the scanning process. Additionally, ongoing monitoring and regular security assessments are advised to ensure the continued resilience of the network.

6. Future Work:

Future assessments should focus on exploiting identified vulnerabilities to evaluate the system's resilience and determine the effectiveness of existing security measures.

7. Acknowledgments:

This report acknowledges the importance of ethical hacking practices and responsible disclosure. It emphasizes the necessity of obtaining proper authorization before conducting any security assessments.

In conclusion, this network scanning report provides a foundation for further penetration testing activities, ensuring a systematic approach to identifying and mitigating potential security risks within the Metasploitable-Linux-2.0.0 environment.