Cyber Security
Major Project Report

Project: Cyber Security June Major Project
Submitted By: SHASHANK KUMAR

1. Introduction

Cybersecurity plays a crucial role in safeguarding digital systems from unauthorized access, attacks, and misuse. This project involves two important activities: network and port scanning using Nmap, and password strength testing using Ophcrack. Both activities are carried out in a safe virtual lab environment using Windows 11 (attacker machine), Windows 7 (victim machine), and Kali Linux (victim machine).**(NOTE:** Used windows 11 instead of 10 as windows 10 has no supported virtual machine) **.**

2. Tools Used

1. Nmap - Open-source tool for network discovery and security auditing.
2. Ophcrack - Password cracking tool based on rainbow tables.
3. VMware/VirtualBox - Virtualization software to simulate lab environment.
4. Operating Systems - Windows 11, Windows 7, Kali Linux.

3. Task 1: Network and Port Scanning using Nmap

The objective of this task is to identify open and closed ports and detect services running on the victim machines.

Nmap was used to perform scanning from the Windows 11 attacker machine.

Steps:

1. Install Nmap on the attacker machine.
2. Find the IP addresses of victim machines.
3. Run scans such as:

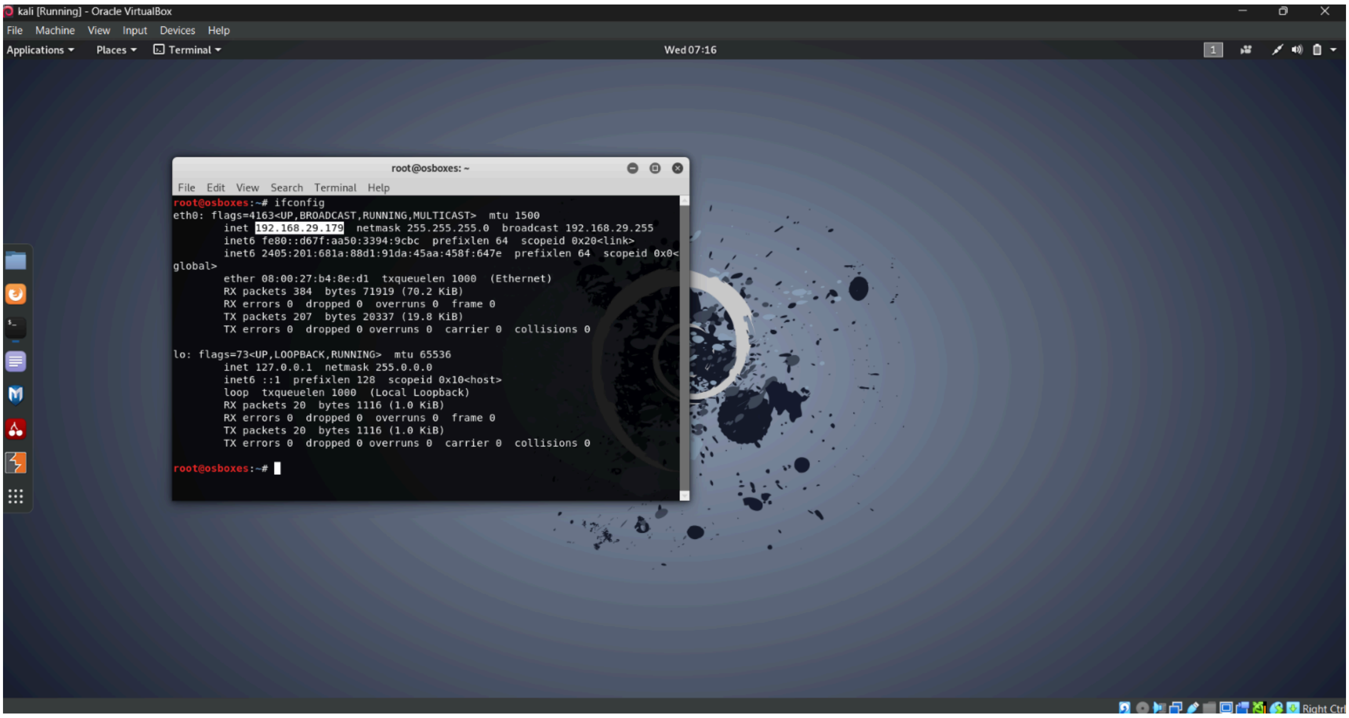
- nmap 192.168.29.21
- nmap -sV 192.168.29.21
- nmap -A 192.168.29.21

4. Analyze the results to check for open ports and active services.

Results:

Sample results include:

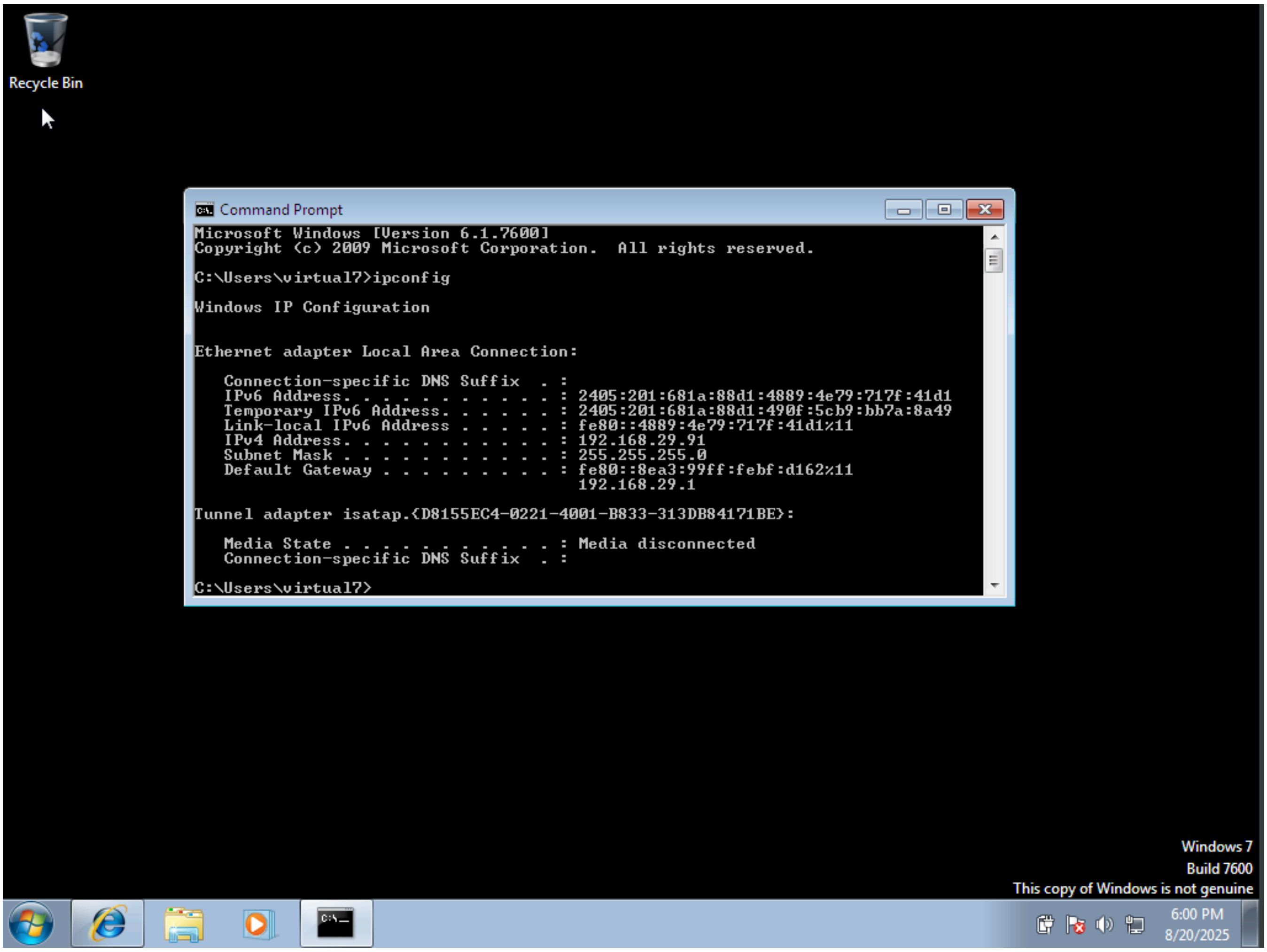
- Kali Linux: Port 111(TCP) open.
- Wind ows 7: Port 135 (RPC), Port 445 (SMB) open.



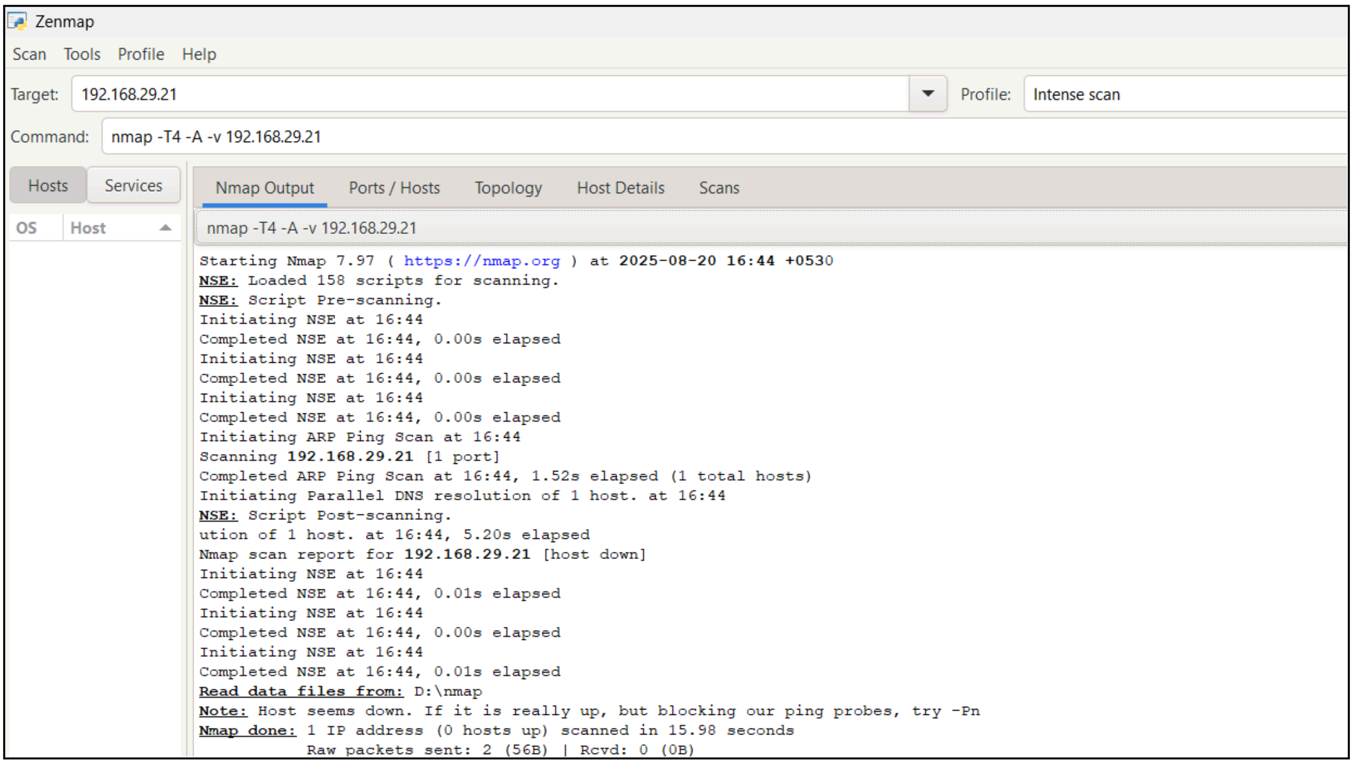
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Wed 07:16
root@osboxes: ~
File Edit View Search Terminal Help
Right Ctrl

```
root@osboxes:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.179  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::d67f:aa50:3394:9cbc  prefixlen 64  scopeid 0x20<link>
        inet6 2405:201:681a:88d1:91da:45aa:458f:647e  prefixlen 64  scopeid 0x0<
global>
        ether 08:00:27:b4:8e:d1  txqueuelen 1000  (Ethernet)
        RX packets 384  bytes 71919 (70.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 207  bytes 20337 (19.8 KiB)
        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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@osboxes:~# 
```

-



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\virtual7>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:201:681a:88d1:4889:4e79:717f:41d1
   Temporary IPv6 Address. . . . . . : 2405:201:681a:88d1:490f:5cb9:bb7a:8a49
   Link-local IPv6 Address . . . . . : fe80::4889:4e79:717f:41d1%11
   IPv4 Address. . . . . . . . . . . : 192.168.29.91
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8ea3:99ff:febf:d162%11
                                       192.168.29.1

Tunnel adapter isatap.{D8155EC4-0221-4001-B833-313DB84171BE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\virtual7>
```



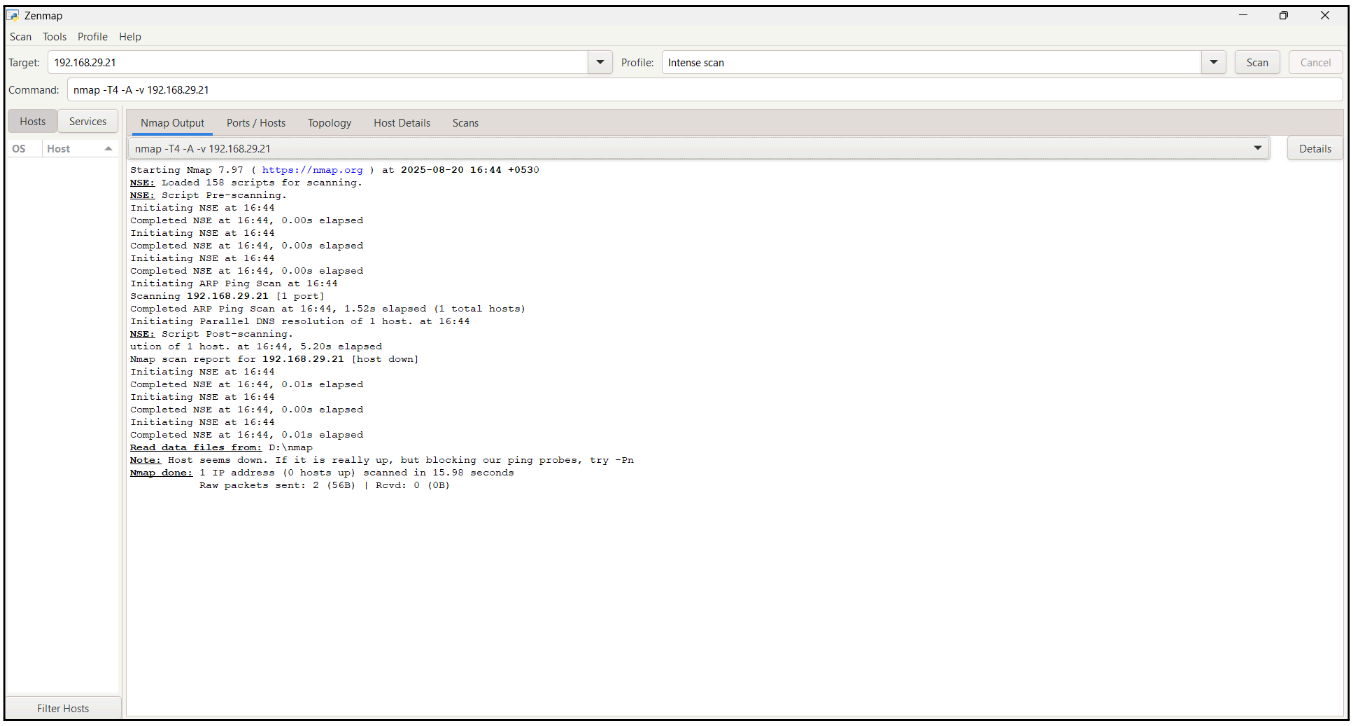
Target: 192.168.29.21

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.29.21

nmap -T4 -A -v 192.168.29.21

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-20 16:44 +0530
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating ARP Ping Scan at 16:44
Scanning 192.168.29.21 [1 port]
Completed ARP Ping Scan at 16:44, 1.52s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
NSE: Script Post-scanning.
ution of 1 host. at 16:44, 5.20s elapsed
Nmap scan report for 192.168.29.21 [host down]
Initiating NSE at 16:44
Completed NSE at 16:44, 0.01s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.01s elapsed
Read data files from: D:\nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 15.98 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```



Target: 192.168.29.21

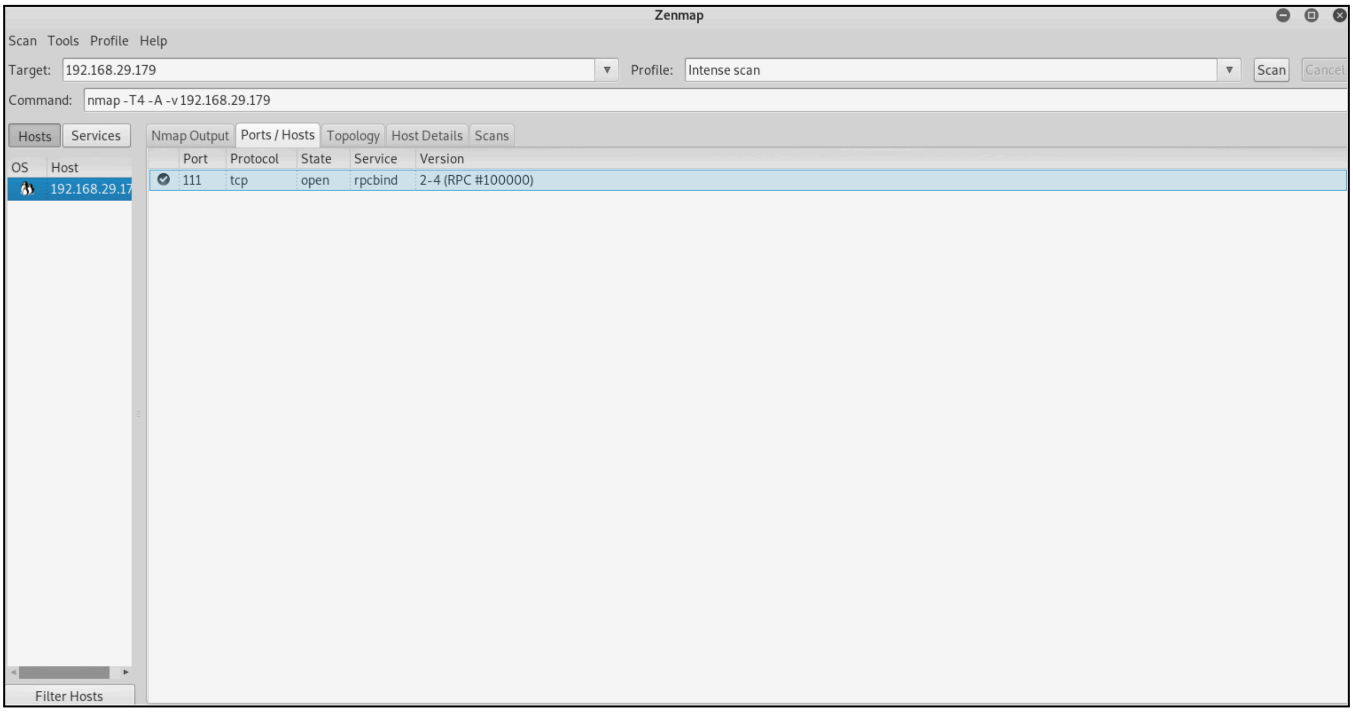
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.29.21

nmap -T4 -A -v 192.168.29.21

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-20 16:44 +0530
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating ARP Ping Scan at 16:44
Scanning 192.168.29.21 [1 port]
Completed ARP Ping Scan at 16:44, 1.52s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
NSE: Script Post-scanning.
ution of 1 host. at 16:44, 5.20s elapsed
Nmap scan report for 192.168.29.21 [host down]
Initiating NSE at 16:44
Completed NSE at 16:44, 0.01s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.00s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 0.01s elapsed
Read data files from: D:\nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 15.98 seconds
           Raw packets sent: 2 (56B) | Rcvd: 0 (0B)
```

-

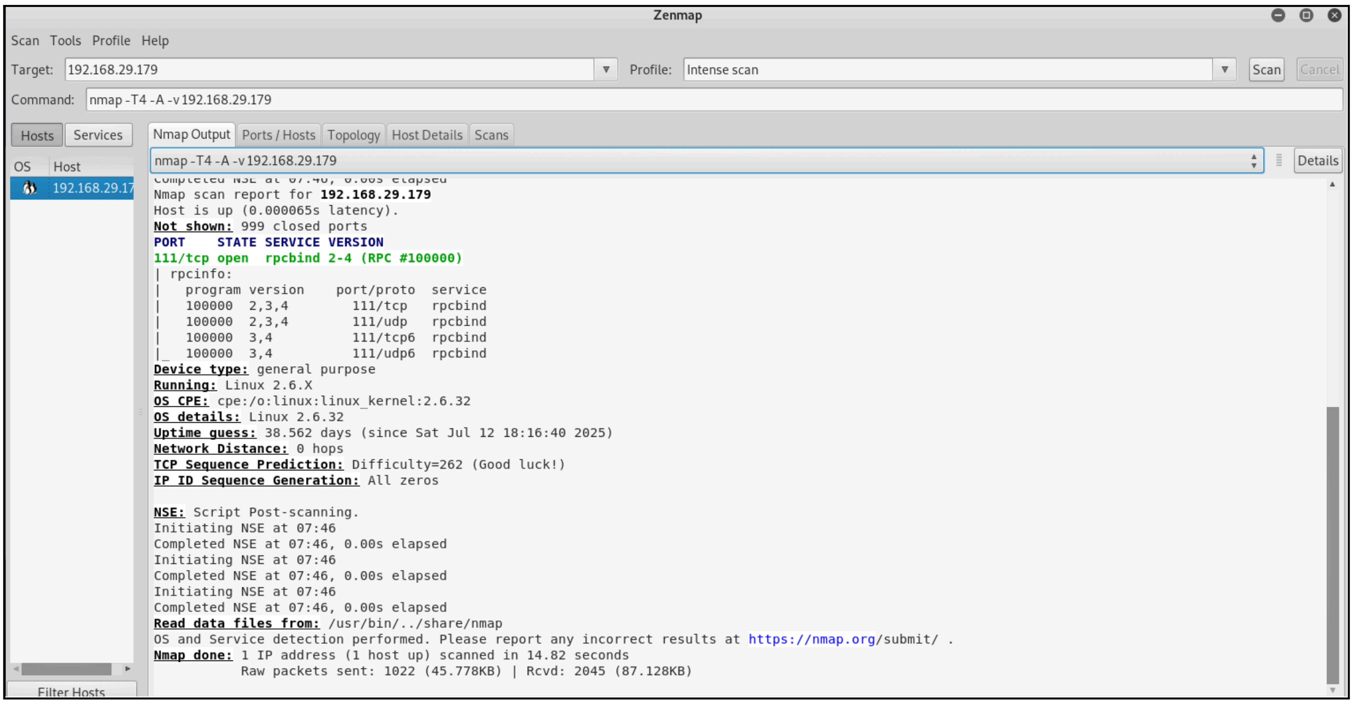


Target: 192.168.29.179

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.29.179

Port	Protocol	State	Service	Version
111	tcp	open	rpcbind	2-4 (RPC #100000)



Target: 192.168.29.179

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.29.179

```
nmap -T4 -A -v 192.168.29.179
```

```
Completed NSE at 07:46, 0.00s elapsed
Nmap scan report for 192.168.29.179
Host is up (0.000065s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 38.562 days (since Sat Jul 12 18:16:40 2025)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Initiating NSE at 07:46
Completed NSE at 07:46, 0.00s elapsed
Initiating NSE at 07:46
Completed NSE at 07:46, 0.00s elapsed
Initiating NSE at 07:46
Completed NSE at 07:46, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
           Raw packets sent: 1022 (45.778KB) | Rcvd: 2045 (87.128KB)
```

-

Countermeasures:

1. Disable unnecessary ports and services.
2. Use firewalls to restrict access.
3. Regularly monitor and audit network traffic.
4. Deploy intrusion detection/prevention systems (IDS/IPS).

4. Task 2: Password Strength Testing using Ophcrack

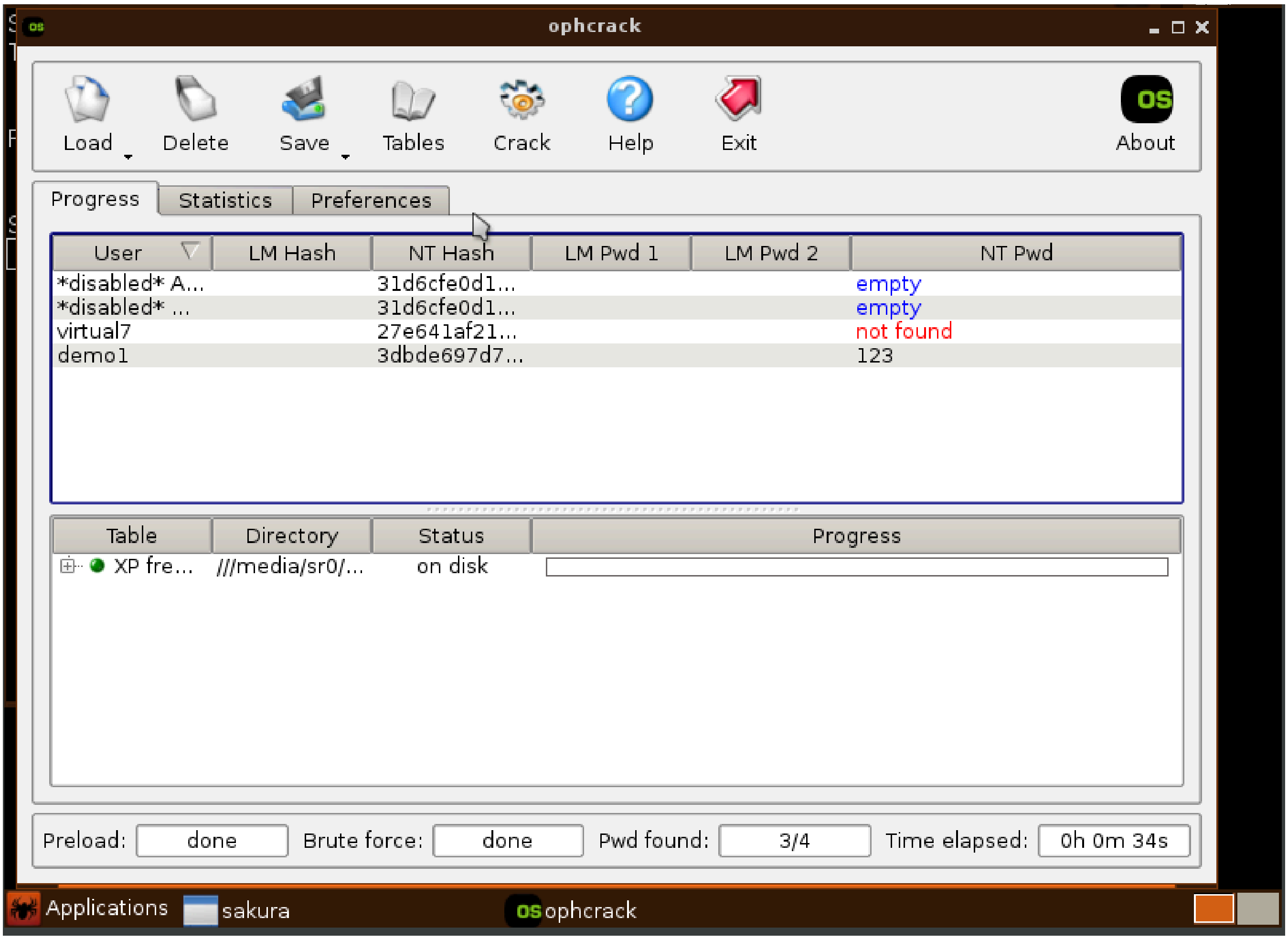
The objective of this task is to check the strength of Windows 7 passwords by attempting to crack them using Ophcrack. Weak passwords can be cracked easily, showing the importance of using strong credentials.

Steps:

1. Install Ophcrack in the virtual environment.
2. Locate the SAM file in Windows 7 at: **C:\Windows\System32\config\SAM**
3. Load the SAM file into Ophcrack.
4. Use rainbow tables to attempt cracking the password.

Results:

Ophcrack was able to crack simple passwords within minutes. Strong, complex passwords resisted cracking.



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
disabled A...		31d6cfe0d1...			empty
disabled ...		31d6cfe0d1...			empty
virtual7		27e641af21...			not found
demo1		3dbde697d7...			123

Table	Directory	Status	Progress
⊞ ● XP fre...	///media/sr0/...	on disk	

Preload: done Brute force: done Pwd found: 3/4 Time elapsed: 0h 0m 34s

Here i used two id's virtual7 and demo1 and ophcrack managed to crack password of demo1 but not vishw7.

Explanation of SAM File:

The Security Account Manager (SAM) file stores password hashes in Windows. Attackers can extract this file to attempt cracking the stored passwords. Protecting it is essential for system security.

Countermeasures:

1. Use strong and unique passwords.
2. Change passwords regularly.
3. Enable account lockout policies.
4. Enable multi-factor authentication (MFA).
5. Encrypt sensitive system files including SAM.

5. Conclusion

This project highlights two critical security areas: network vulnerabilities and password security. The experiments demonstrated how open ports and weak passwords can be exploited by attackers. By applying preventive measures such as firewalls, IDS/IPS, strong passwords, and MFA, organizations can significantly enhance their cybersecurity posture.