

Executive Post Graduate Certification in Cyber Security and Ethical Hacking

Project

Nmap Network Reconnaissance:

To identify open ports, active services, and OS details, we performed an **Nmap scan** with the following command: `nmap -sS -sV -O -p- <target-IP>` and our target IP is 192.168.27.131.

```
(root@kali)~/home/kali
# nmap -sS -sV -O -p- 192.168.27.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-14 10:46 EDT
Nmap scan report for 192.168.27.131
Host is up (0.0017s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
33897/tcp open  nlockmgr     1-4 (RPC #100021)
35696/tcp open  status       1 (RPC #100024)
38948/tcp open  mountd       1-3 (RPC #100005)
60075/tcp open  java-rmi     GNU Classpath grmiregistry
MAC Address: 00:10:C2:9:B3:21:17 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 136.87 seconds
```

Command executed:

`nmap -sS -sV -O -p- 192.168.27.131`

Nmap Scan Results:

Target IP: 192.168.27.131

Host Status: Up (0.0017s latency):

Identified Open Ports and Services:

Port	State	Service	Version
21/tcp	open	FTP	vsftpd 2.3.4
22/tcp	open	SSH	OpenSSH 4.7p1 Debian 8ubuntu1
23/tcp	open	Telnet	Linux telnetd
25/tcp	open	SMTP	Postfix smtpd
53/tcp	open	DNS	ISC BIND 9.4.2
80/tcp	open	HTTP	Apache 2.2.8
139/tcp	open	NetBIOS-SSN	Samba smbd 3.X - 4.X
445/tcp	open	SMB	Samba smbd 3.X - 4.X
2049/tcp	open	NFS	2-4 (RPC #100003)
3306/tcp	open	MySQL	MySQL 5.0.51a-3ubuntu5
5900/tcp	open	VNC	VNC (protocol 3.3)
6667/tcp	open	IRC	UnrealIRCd
8009/tcp	open	AJP13	Apache JServ (Protocol v1.3)
8180/tcp	open	HTTP	Apache Tomcat/Coyote JSP engine 1.1

Operating System: Linux 2.6.X

Device Type: General-purpose

Service Info: Unix, Linux, metasploitable.localdomain

SMB Enumeration:

Enumerating SMB Shares with smbclient

Command : smbclient -L \\192.168.27.131 --no-pass

```
(root@kali)-[/home/kali]
# smbclient -L \\192.168.27.131 --no-pass
Anonymous login successful

      Sharename      Type      Comment
      -----      -
      print$         Disk      Printer Drivers
      tmp            Disk      oh noes!
      opt            Disk
      IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
      ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

      Server          Comment
      -----
      Workgroup       Master
      -----
      WORKGROUP       METASPLOITABLE

(root@kali)-[/home/kali]
```

Command executed:

Findings:

Anonymous login successful.

Shared resources identified on the target system.

Possible misconfigured permissions.

<u>Sharename</u>	Type	Comment
print\$	Disk	Printer Drivers
<u>tmp</u>	Disk	oh noes!
opt	Disk	
IPC\$	IPC	IPC Service (<u>metasploitable</u> server (Samba 3.0.20-Debian))
ADMIN\$	IPC	IPC Service (<u>metasploitable</u> server (Samba 3.0.20-Debian))

Workgroup & Server Details:

Workgroup	Master
WORKGROUP	METASPLOITABLE

Enumerate SMB with enum4linux

enum4linux -a 192.168.27.131 | tee smb_enum_results.txt

```
(root@kali)-[/home/kali]
# enum4linux -a 192.168.27.131 | tee smb_enum_results.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 14 11:31:49 2025

===== ( Target Information ) =====
Target ..... 192.168.27.131
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.27.131 ) =====
[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 192.168.27.131 ) =====
Looking up status of 192.168.27.131
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

===== ( Session Check on 192.168.27.131 ) =====
[+] Server 192.168.27.131 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.27.131 ) =====
```

rpcclient -U "" 192.168.27.131

```
(root@kali)-[/home/kali]
# rpcclient -U "" 192.168.27.131
Password for [WORKGROUP\]:
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
rpcclient $>
```

This project involved various reconnaissance and enumeration techniques to identify vulnerabilities in a target system (192.168.27.131). Using Nmap, we identified open ports, active services, and OS details, revealing that the system is running Linux 2.6.X with multiple exposed services.

Further, SMB enumeration using smbclient and enum4linux indicated potential misconfigurations, including anonymous login access and shared resources, which could be exploited by attackers. These findings highlight the importance of securing network services, implementing proper access controls, and regularly monitoring for misconfigurations to prevent unauthorized access.

The project demonstrates the effectiveness of ethical hacking methodologies in identifying security gaps, reinforcing the need for proactive security measures in an organizational environment.