Exploring nmap Script and Nessus Exploration

Karthikeyan G
Roll No: CB.SC.P2.CYS24008

January 24, 2025

1 Nmap Script

```
#!/bin/bash

read -p "Enter target IP address: " target

echo "Running all scans on the target: $target"

echo "1. Checking if target is active (ping scan)..."
nmap -sn $target
echo "Ping scan completed."

echo "2. Scanning specific ports (SSH, HTTP, HTTPS)..."
nmap -p 22,80,443 $target
echo "Specific port scan completed."

echo "3. Performing full TCP connection scan..."
nmap -sT $target
echo "Full TCP connection scan completed."

echo "4. Performing stealth scan..."
nmap -sS $target
echo "Stealth scan completed."

echo "5. Identifying service versions..."
nmap -sV $target
echo "Service version scan completed."

echo "6. Detecting operating system..."
nmap -O $target
echo "OS detection completed."

echo "7. Performing a comprehensive scan..."
nmap -A $target
echo "Comprehensive scan completed."

read -p "Enter an IP range to scan (e.g., 192.168.1.1-254): " range
echo "8. Scanning the given range: $range"
nmap $range
echo "IP range scan completed."

echo "9. Scanning the subnet..."
nmap -sn $target
echo "Subnet scan completed."

echo "10. Scanning common ports (1-1024)..."
nmap -p 1-1024 $target
echo "Common port scan completed."

echo "All scans are completed."
```

```
┌──(karthikeyan㉿kali)-[~/Documents]
└─$ sudo ./nmap_script.sh
Enter target IP address: 192.168.133.132
Running all scans on the target: 192.168.133.132
1. Checking if target is active (ping scan)...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:52 IST
Nmap scan report for 192.168.133.132
Host is up (0.00058s latency).
MAC Address: 00:0C:29:E5:0F:F9 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
Ping scan completed.
2. Scanning specific ports (SSH, HTTP, HTTPS)...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:52 IST
Nmap scan report for 192.168.133.132
Host is up (0.00065s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:E5:0F:F9 (VMware)
```

```
3. Performing full TCP connection scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:52 IST
Nmap scan report for 192.168.133.132
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:E5:0F:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
Full TCP connection scan completed.
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
Full TCP connection scan completed.
4. Performing stealth scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:52 IST
Nmap scan report for 192.168.133.132
Host is up (0.00093s 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:E5:0F:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
Stealth scan completed.
```

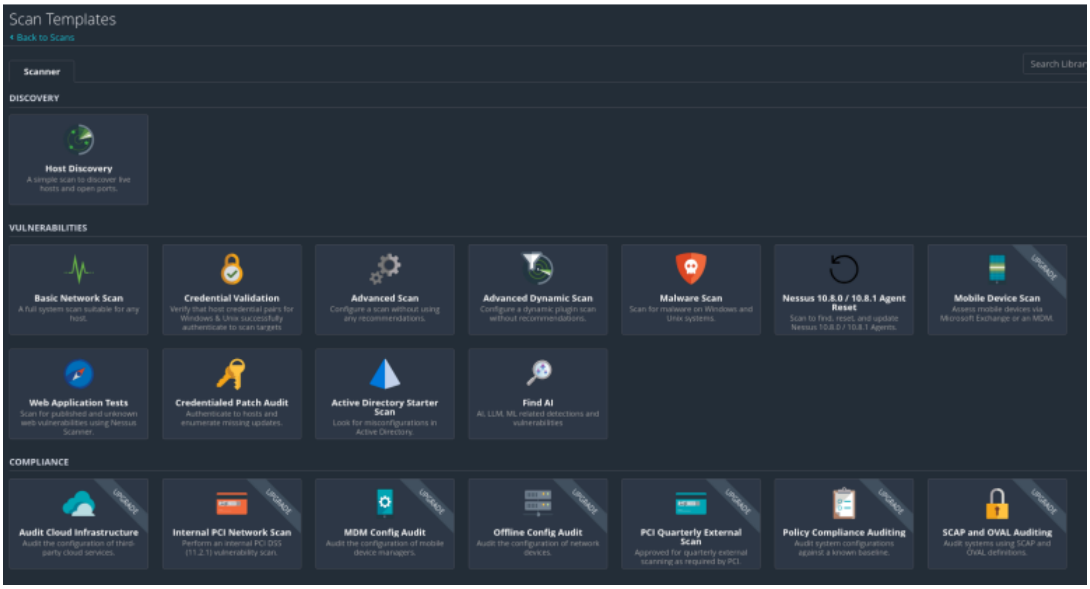
```
5. Identifying service versions...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:52 IST
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 22:54 (0:00:00 remaining)
Nmap scan report for 192.168.133.132
Host is up (0.00082s latency).
Not shown: 977 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
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
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
8009/tcp open  ajp13?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:E5:0F:F9 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_My_scan: ERROR: Script execution failed (use -d to debug)
```

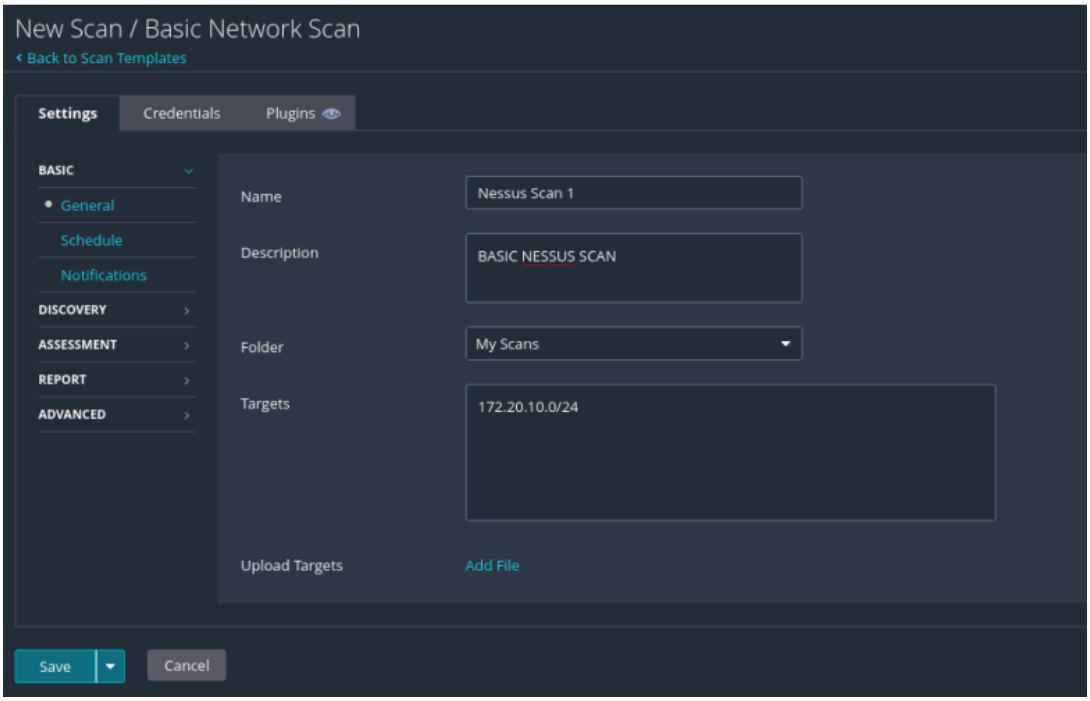
```
6. Detecting operating system...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:54 IST
Nmap scan report for 192.168.133.132
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
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 filtered ajp13
8180/tcp open     unknown
MAC Address: 00:0C:29:E5:0F:F9 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
OS detection completed.
```

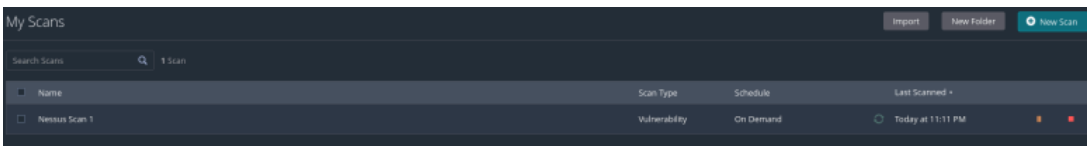
```
7. Performing a comprehensive scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 22:54 IST
Nmap scan report for 192.168.133.132
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.133.130
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
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      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
|_ssl-date: 2025-01-24T16:53:07+00:00; -33m16s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

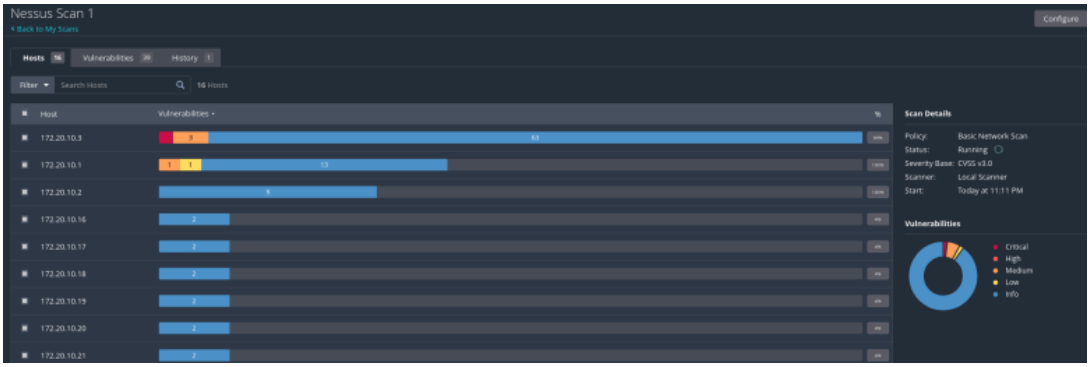
```
MAC Address: 00:0C:29:E5:0F:F9 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_My_scan: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-24T11:51:53-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 41m43s, deviation: 2h30m00s, median: -33m16s

TRACEROUTE
HOP RTT     ADDRESS
1   2.08 ms 192.168.133.132
```

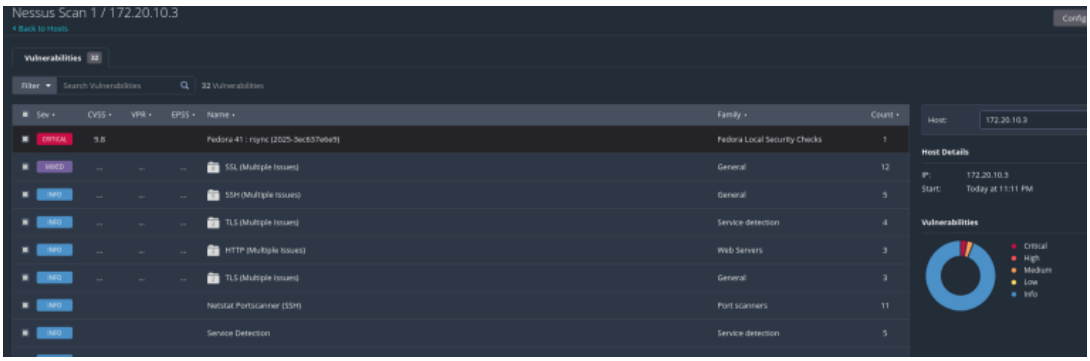
2 Nessus Basic Scan


Scan Templates
Back to Scans
Scanner
DISCOVERY
Host Discovery
VULNERABILITIES
Basic Network Scan
Credential Validation
Advanced Scan
Advanced Dynamic Scan
Malware Scan
Nessus 10.8.0 / 10.8.1 Agent Reset
Mobile Device Scan
Web Application Tests
Credentialed Patch Audit
Active Directory Starter Scan
Find AI
COMPLIANCE
Audit Cloud Infrastructure
Internal PCI Network Scan
MDM Config Audit
Offline Config Audit
PCI Quarterly External Scan
Policy Compliance Auditing
SCAP and OVAL Auditing


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Nessus Scan 1
Description
BASIC NESSUS SCAN
Folder
My Scans
Targets
172.20.10.0/24
Upload Targets
Add File
Save
Cancel


My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Nessus Scan 1
Vulnerability
On Demand
Today at 11:11 PM


Nessus Scan 1
Configure
Hosts
Vulnerabilities
History
Scan Details
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus Scan 1 / 172.20.10.3
Vulnerabilities
Host Details
Vulnerabilities