Python Automation Scripting with Nmap

Objective

The objective of this task was to automate network scanning using Python and the python-nmap library. Automation reduces manual effort, ensures consistency, and generates structured reports that are easy to analyze.

Tools and Libraries Used

- **Python 3.13**
- **python-nmap library**
- **Nmap (Network Mapper)**

Process Followed

1. **Environment Setup**
   - Created and activated a Python virtual environment.
   - Installed the python-nmap package inside the environment.
2. **Script Development**
   - Developed a Python script (nmap_automation.py) to:
     - Accept a target IP address as input.
     - Perform three types of scans:
       - **SYN Scan** (-sS)
       - **TCP Connect Scan** (-sT)
       - **UDP Scan (Top 100 ports)** (-sU --top-ports 100)
     - Extract host information, open ports, and running services.
3. **Report Generation**
   - Generated a **scan_report.txt** file summarizing results:
     - Scan timestamp
     - Target IP address
     - Consolidated table of open ports, services, and versions
   - Created a **CSV file (open_ports.csv)** for structured results.
   - Saved raw Nmap scan outputs (.nmap, .xml, .gnmap) for reference.

Sample Output (Extract from scan_report.txt)

Target: 192.168.0.206

Scan Timestamp: 2025-09-30 03:20:21

Port	Protocol	State	Service	Version/Info
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	—
913	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (VNC, SOAP)
1521	tcp	open	oracle-tns	Oracle TNS Listener 10.2.0.1.0 (Windows)
903	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (VNC, SOAP)

(Full details are in the attached scan_report.txt and open_ports.csv files.)

Outcomes Achieved

- Automated three different types of Nmap scans.
- Generated both human-readable and structured reports.
- Preserved raw scan outputs for verification and further analysis.

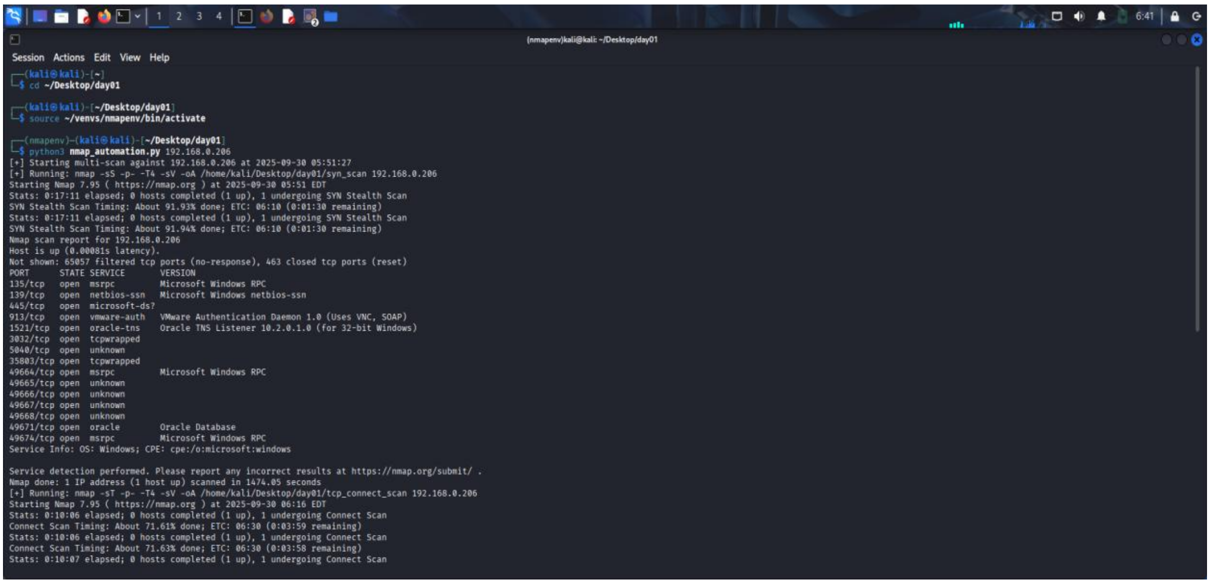
Key Learnings

- Learned how to use Python to automate Nmap scanning.
- Understood differences between **SYN, TCP Connect, and UDP scans**.
- Gained experience in exporting results to multiple formats (TXT, CSV, XML).
- Realized the value of automation for efficient and repeatable security assessments.

Deliverables in Folder:

- nmap_automation.py (Python script)
- scan_report.txt (Text report)
- open_ports.csv (Structured CSV report)
- python_automation.pdf(Explanation about what I did and what I have learned)

Terminals O/P:

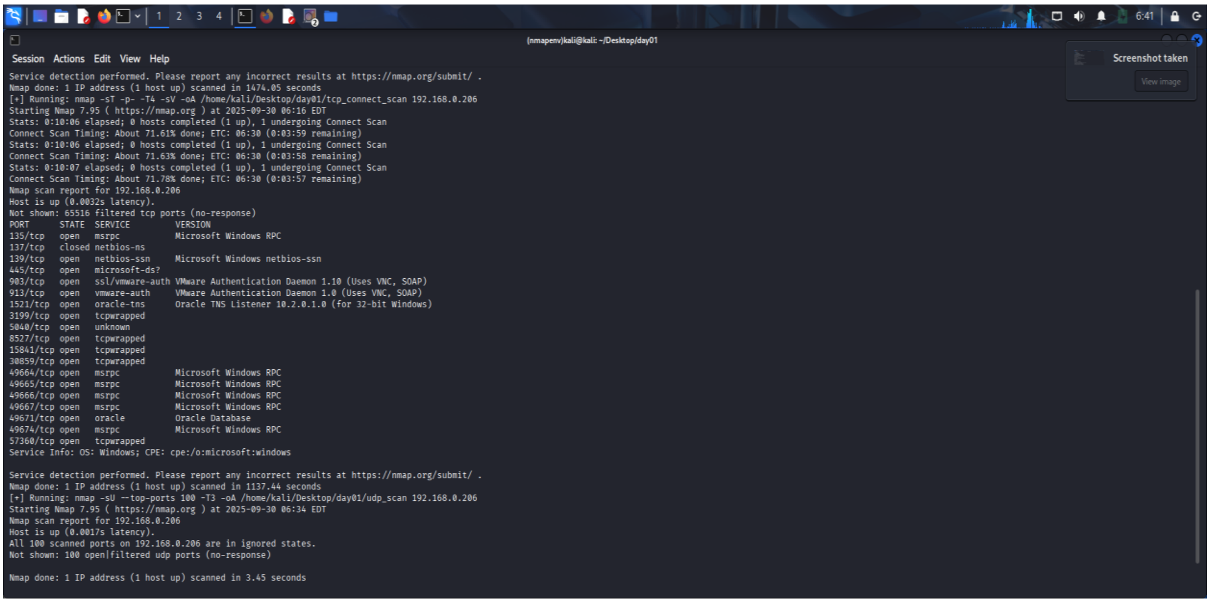


```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop/day01

┌──(kali㉿kali)-[~/Desktop/day01]
└─$ source ~/venvs/nmapenv/bin/activate

┌──(nmapenv)─(kali㉿kali)-[~/Desktop/day01]
└─$ python3 nmap_automation.py 192.168.0.206
[+] Starting multi-scan against 192.168.0.206 at 2025-09-30 05:51:27
[+] Running: nmap -sS -p- -T4 -sV -oA /home/kali/Desktop/day01/syn_scan 192.168.0.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 05:51 EDT
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.93% done; ETC: 06:10 (0:01:30 remaining)
Stats: 0:17:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.94% done; ETC: 06:10 (0:01:30 remaining)
Nmap scan report for 192.168.0.206
Host is up (0.00081s latency).
Not shown: 65057 filtered tcp ports (no-response), 463 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
913/tcp   open  vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1521/tcp  open  oracle-tns    Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
3032/tcp  open  tcpwrapped
5040/tcp  open  unknown
35803/tcp open  tcpwrapped
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49671/tcp open  oracle        Oracle Database
49674/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1474.05 seconds
[+] Running: nmap -sT -p- -T4 -sV -oA /home/kali/Desktop/day01/tcp_connect_scan 192.168.0.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 06:16 EDT
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.61% done; ETC: 06:30 (0:03:59 remaining)
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.63% done; ETC: 06:30 (0:03:58 remaining)
Stats: 0:10:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
```



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1474.05 seconds
[+] Running: nmap -sT -p- -T4 -sV -oA /home/kali/Desktop/day01/tcp_connect_scan 192.168.0.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 06:16 EDT
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.61% done; ETC: 06:30 (0:03:59 remaining)
Stats: 0:10:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.63% done; ETC: 06:30 (0:03:58 remaining)
Stats: 0:10:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 71.78% done; ETC: 06:30 (0:03:57 remaining)
Nmap scan report for 192.168.0.206
Host is up (0.0032s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE  SERVICE         VERSION
135/tcp   open   msrpc           Microsoft Windows RPC
137/tcp   closed netbios-ns
139/tcp   open   netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open   microsoft-ds?
903/tcp   open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
913/tcp   open   vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1521/tcp  open   oracle-tns      Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
3199/tcp  open   tcpwrapped
5040/tcp  open   unknown
8527/tcp  open   tcpwrapped
15841/tcp open   tcpwrapped
30859/tcp open   tcpwrapped
49664/tcp open   msrpc           Microsoft Windows RPC
49665/tcp open   msrpc           Microsoft Windows RPC
49666/tcp open   msrpc           Microsoft Windows RPC
49667/tcp open   msrpc           Microsoft Windows RPC
49671/tcp open   oracle          Oracle Database
49674/tcp open   msrpc           Microsoft Windows RPC
57360/tcp open   tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1137.44 seconds
[+] Running: nmap -sU --top-ports 100 -T3 -oA /home/kali/Desktop/day01/udp_scan 192.168.0.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 06:34 EDT
Nmap scan report for 192.168.0.206
Host is up (0.0017s latency).
All 100 scanned ports on 192.168.0.206 are in ignored states.
Not shown: 100 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
```