Advanced Executive Program in Cybersecurity

Virtual Internship Project Problem Statement

Submitted By :

DEEPAK SHARMA

Penetration Tester

Problem statement:

You are working as a Penetration Tester for El Banco Bank. You are running a gray-box penetration test to probe for vulnerabilities that hackers with nefarious intent might be able to exploit to gather secure data and intelligence.

As a first step, you must gather more information about the target's environment and network-related information using the tools at your disposal.

Background of the problem statement:

El Banco Bank is one of the fastest growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber-attacks and data breaches has become a significant issue for every organization.

Expected deliverables:

TASK 1:

Perform a half-open scan against the target network to quickly identify all open ports in the network.

✅ Task 1 Report – Half-Open SYN Scan

📌 **Project: Capstone Project 1 – Penetration Tester**

🎯 **Task: Identify all open ports using half-open scan (`SYN scan`)**

👨 **Tester: DEEPAK SHARMA**

🖥️ **Lab Environment: AWS Virtual Lab (Kali, Ubuntu, Windows 10, WebGoat)**

🔍 Objective:

To perform a **half-open TCP SYN scan** (`-sS` in Nmap) on target systems to identify all open TCP ports without establishing full connections. This method is fast and stealthy and often evades basic firewall detection.

🛠️ Tools & Commands Used:

Tool: Nmap
Command Template:

```
nmap -sS -T4 -Pn -oN [output_file.txt] [Target IP]
```

- `-sS`: TCP SYN scan (half-open)
- `-T4`: Faster scan speed
- `-Pn`: Skip host discovery (assume host is up)
- `-oN`: Save output in human-readable format

🖥️ Target Systems and Results:

🔹 1. Ubuntu (172.31.6.190)

Port	State	Service
22	open	SSH
8443	open	HTTPS-alt

2. WebGoat (172.31.14.129)

Port	State	Service
22	open	SSH
80	open	HTTP
8443	open	HTTPS-alt

---

3. Windows 10 (172.31.12.236)

Port	State	Service
3389	open	ms-wbt-server (RDP)
5357	open	wsdapi
8443	open	HTTPS-alt

✅ Conclusion:

The half-open scan successfully identified open ports and available services on all three target systems. This information provides the initial attack surface and will be used for further enumeration and vulnerability assessment in subsequent tasks.

TASK 2:

Perform an aggressive mode that enables OS detection, version detection, script scanning, and traceroute in the network.

✅ Task 2 Report – Aggressive Scan

📌 Project: Capstone Project 1 – Penetration Tester

🎯 Task: Perform an aggressive scan to detect OS, service versions, scripts, and traceroute

👱 Tester: [Your Name]

🖥️ Lab Environment: AWS Virtual Lab (Kali, Ubuntu, Windows 10, WebGoat)

🔍 Objective:

To perform an **aggressive Nmap scan** (`-A`) to gather detailed information about each host, including:

- Open ports and services
- Operating system (OS) detection
- Script-based service enumeration
- SSL and HTTP certificate details
- Traceroute information

🛠️ Tools & Commands Used:

Tool: Nmap
Command Template:

```
bash
CopyEdit
nmap -A -T4 -Pn -oN [output_file.txt] [Target IP]
```

🖥️ Target Systems and Findings:

1. WebGoat (172.31.14.129)

Attribute	Details
OS Detected	Linux (No exact match)
Traceroute	1 hop
Open Ports	`22/tcp`, `80/tcp`, `8443/tcp`
Services	SSH (OpenSSH 8.2p1), HTTP (nginx 1.18.0), DCV on 8443
Cert Info (8443)	CN: ip-172-31-62-151, Expired: 2022-04-02
Notes	Port 8443 is running NICE DCV; SSL randomness issues

---

2. Windows 10 (172.31.12.236)

Attribute	Details
OS Detected	Likely Microsoft Windows (uncertain due to filtered ports)
Traceroute	1 hop
Open Ports	`3389/tcp`, `5357/tcp`, `8443/tcp`
Services	RDP (Terminal Services), Microsoft HTTPAPI 2.0, DCV
Cert Info (8443)	CN: DESKTOP-61SVOEB, Valid: 2025-06-14 to 2025-12-14
RDP Details	NetBIOS & DNS name: DESKTOP-61SVOEB, Version: 10.0.19041

---

3. Ubuntu (172.31.6.190)

Attribute	Details
OS Detected	Linux (No exact match)
Traceroute	1 hop
Open Ports	22/tcp, 8443/tcp
Services	SSH (OpenSSH 8.2p1), DCV on 8443
Cert Info (8443)	CN: ip-172-31-62-151, **Expired:** 2022-04-02
Notes	Port 8443 is running NICE DCV; expired certificate; TLS randomness issues

☑ Conclusion:

The aggressive scans provided deep insights into service configurations and OS fingerprints:

- **WebGoat** appears to run a Linux-based nginx web server with a DCV desktop session on 8443.
- **Windows 10** exposes critical remote access services like RDP and an HTTPAPI interface, useful for vulnerability assessment.
- **Ubuntu** exposes exposes SSH (OpenSSH 8.2p1) and NICE DCV (remote desktop) on port 8443 with an **expired SSL certificate**, revealing system and service details that could aid attackers.

TASK 3:

While examining web server logs, you notice some HyperText Transfer Protocol (HTTP) GET requests that look suspicious. You need to carefully examine the logs, identify the attacks, and determine the appropriate mitigation control.

Log #1:

```
"18.66.78.71 - - [22/Dec/2021:16:18:20 +0300] "GET /media/system/js/caption.js HTTP/1.1" 200 751
"http://18.66.78.71/?wvstest=javascript:domxssExecutionSink(1,%22'%5C%22%3E%3Cxsstag%3E()locxss%22)" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21""
```

Log #2

```
"18.66.78.71 - - [22/Dec/2021:15:20:03 +0300] "GET /DVWA/vulnerabilities/fi/?page=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.1" 200 2190 "http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36""
```

Log #3

```
"18.66.78.71 - - [22/Dec/2021:15:19:59 +0300] "GET /DVWA/vulnerabilities/fi/?page=%27AND%201%3dcast(0x5f21403264696c656d6d61%20as%20varchar(8000))%20or%20%271%27%3d%27 HTTP/1.1" 200 1433
"http://18.66.78.71/DVWA/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.16 Safari/537.36""
```

✅ TASK 3 Table:

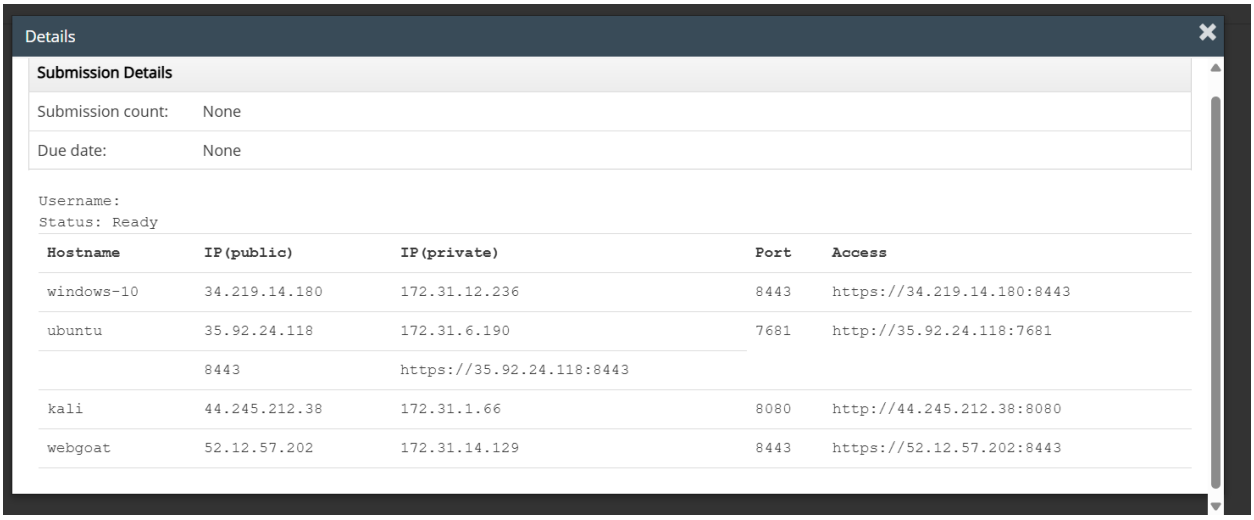
Log #	Attack Type	Description	Mitigation Measures
1	DOM-Based XSS	JavaScript reads untrusted data from URL	Input sanitization, CSP, avoid unsafe DOM sinks
2	Directory Traversal	Accessing system files via path manipulation	Input validation, whitelist files, disable directory listing
3	SQL Injection (SQLi)	Injected SQL logic in user parameter	Use prepared statements, validate input, WAF

Using Encoder/Decoder Tool

🛡️ Summary Table

Log #	Decoded Payload	Attack Type
1	`javascript:domxssExecutionSink(...)`	**DOM-Based XSS**
2	`/../../../../etc/passwd`	**Directory Traversal**
3	`'AND 1=cast(...) or '1'='`	**SQL Injection**

ScreenShots :-



Details

Submission Details

Submission count:	None
Due date:	None

Username:
Status: Ready

Hostname	IP (public)	IP (private)	Port	Access
windows-10	34.219.14.180	172.31.12.236	8443	https://34.219.14.180:8443
ubuntu	35.92.24.118	172.31.6.190	7681	http://35.92.24.118:7681
	8443	https://35.92.24.118:8443		
kali	44.245.212.38	172.31.1.66	8080	http://44.245.212.38:8080
webgoat	52.12.57.202	172.31.14.129	8443	https://52.12.57.202:8443

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T4 -Pn 172.31.12.236 -oN  windows10_scan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-06-22 14:48 UTC
Nmap scan report for ip-172-31-12-236.us-west-2.compute.internal (172.31.12.236)
Host is up (0.00013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8443/tcp open  https-alt
MAC Address: 0A:9F:1F:71:97:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T4 -Pn 172.31.6.190 -oN  ubuntu__scan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-06-22 14:49 UTC
Nmap scan report for ip-172-31-6-190.us-west-2.compute.internal (172.31.6.190)
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8443/tcp open  https-alt
MAC Address: 0A:17:52:87:91:35 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T4 -Pn 172.31.14.129 -oN  webgoat__scan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-06-22 14:50 UTC
Nmap scan report for ip-172-31-14-129.us-west-2.compute.internal (172.31.14.129)
Host is up (0.00024s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8443/tcp open  https-alt
MAC Address: 0A:34:10:BD:67:91 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Logs	Attacker	Mitigation
Log1	DOM Based XSS	1. HTML encoding, and then 2. JavaScript encoding all untrusted input, as shown in these examples
Log2	TRIXBOX MULTIPLE PATH TRAVERSAL VULNERABILITIES	**avoid passing user-supplied input to filesystem APIs altogether**
Log3	SQL Injection	• **Option 1: Use of Prepared Statements (with Parameterized Queries)** • **Option 2: Use of Properly Constructed Stored Procedures** • **Option 3: Allow-list Input Validation** • **Option 4: Escaping All User Supplied Input**