TryHackMe Advent of Cyber 2025

Day 7 Challenge Report

Network Discovery with Nmap

1. Executive Summary

This report documents the completion of Day 7 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on network service discovery using Nmap and various network tools. Through systematic port scanning, service enumeration, and protocol analysis, successfully recovered three key fragments from FTP, a custom service, and DNS, gaining administrative access to the compromised QA server and locating the final flag in a MySQL database.

2. Challenge Overview

Objective: Recover access to the tbfc-devqa01 server (YOUR_VM_IP) compromised by HopSec attackers by discovering network services, collecting key fragments, and accessing the admin console.

Tools Used: Nmap, FTP client, Netcat, dig, MySQL client

3. Engagement Planning

Target Intelligence:

- **Target Server:** tbfc-devqa01
- **IP Address:** {YOUR_VM_IP}
- **Status:** Compromised by HopSec

Attack Strategy:

1. Scan for open ports (common: SSH 22, HTTP 80)
2. Enumerate services on discovered ports
3. Exploit exposed services to gather intelligence
4. Recover admin access and secure server

4. Initial Reconnaissance

4.1 Basic Port Scan

Executed basic Nmap scan targeting the top 1000 most common ports:

```
nmap 10.65.172.249
```

Results:

- **Port 22/tcp:** SSH (Secure Shell) - Open
- **Port 80/tcp:** HTTP (Web Server) - Open

Web Application Reconnaissance:

Accessed http://10.65.172.249 revealing defaced website:

Defacement Message:
"EAST-mas TAKEOVER - Your QA server answers to HopSec now. Its console is sealed with a lock only TBFC can pick. I scattered three fragments of the passphrase across your own chaos. Find them. Stitch the words together. Speak them to the gate and take your box back, if you can. - King Malhare 🐰🥚 "

Site Header: "Pwned by HopSec"

5. Comprehensive Port Scanning

5.1 Full TCP Port Range Scan

Expanded scan to all 65,535 ports with banner grabbing:

```
nmap -p- --script=banner 10.65.172.249
```

Complete Results:

Port 22/tcp - SSH:

```
Banner: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14
```

Port 80/tcp - HTTP:

Defaced website with locked admin panel

Port 21212/tcp - FTP (Non-Standard):

```
Banner: 220 (vsFTPd 3.0.5)
```

Service: FTP running on non-standard port (typically port 21)

Port 25251/tcp - Custom Application:

```
Banner: TBFC maintd v0.2 - Type HELP for commands
```

6. Service Exploitation & Key Fragment Recovery

6.1 FTP Service Enumeration (Port 21212)

Connected to FTP service using anonymous authentication:

```
ftp 10.65.172.249 21212
ls
```

Discovered Files:

Located file containing key fragment hint

```
get {filename}
```

KEY FRAGMENT 1: 3aster_

6.2 Custom TBFC Service (Port 25251)

Connected to custom maintenance service using Netcat:

```
nc -v 10.65.172.249 25251
```

Service Commands:

```
HELP
```

Revealed available commands for the maintenance daemon

```
GET KEY
```

KEY FRAGMENT 2: 15_th3_

6.3 UDP Port Scanning & DNS Enumeration

Expanded reconnaissance to UDP protocols (65,535 additional ports):

```
nmap -sU 10.65.172.249
```

UDP Port Discovered:

Port 53/udp - DNS: Domain Name System service

DNS Query for Key Fragment:

Queried DNS server for TXT record containing third key:

```
dig @10.65.172.249 TXT key3.tbfc.local +short
```

KEY FRAGMENT 3: n3w_xm45

7. Administrative Access Recovery

7.1 Passphrase Assembly

Combined three key fragments in order:

Complete Passphrase: 3aster_15_th3_n3w__xm45

7.2 Admin Console Access

Submitted passphrase to locked admin console on port 80, successfully gaining administrative shell access.

8. Internal Service Discovery

8.1 Listing Listening Ports

From admin console, enumerated all listening services:

```
ss -tunlp
```

Internal Services Discovered:

- Services on 0.0.0.0 (externally accessible)
- Services on 127.0.0.1 (localhost only)

Port 3306 - MySQL Database:

Identified default MySQL port listening on localhost, typically allowing unauthenticated local connections while requiring credentials for remote access.

8.2 Database Enumeration

Accessed MySQL database from localhost context:

Table Discovery:

```
mysql -D tbfcqa01 -e "show tables;"
```

Flag Extraction:

```
mysql -D tbfcqa01 -e "select * from flags;"
```

Final Flag: THM{4ll_s3rvice5_d1sc0vered}

9. Key Skills Developed

- Comprehensive port scanning (TCP and UDP)
- Service enumeration with banner grabbing
- FTP anonymous access exploitation
- Custom protocol interaction with Netcat
- DNS TXT record enumeration
- Internal service discovery from compromised host
- Database enumeration and SQL querying

10. Conclusion

Day 7 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in network service discovery and enumeration. Through systematic use of Nmap and complementary tools, successfully identified services across TCP and UDP protocols, exploited multiple services to recover key fragments, and gained administrative access to the compromised server.

The challenge demonstrated the importance of thorough reconnaissance, including non-standard ports and UDP protocols, in penetration testing engagements. The multi-stage approach of external scanning followed by internal enumeration showcased realistic attack progression and the value of comprehensive service discovery.

Challenge Status: **COMPLETED ✓**