Discover Network Services

Overview

Room URL: https://tryhackme.com/room/networkservices-aoc2025-jnsoqbxgky

Difficulty: Easy

Category: Network Scanning

Date Completed: 12/7/2025

Objectives

- Learn the basics of network service discovery with Nmap
- Learn core network protocols and concepts along the way
- Apply your knowledge to find a way back into the server

Table of Contents

Introduction

After regaining knowledge of the **tbfc-devqa01** QA server's IP address, TBFC's security team launches a counterattack to reclaim the compromised system from HopSec's grasp. The server greets you with a defaced website proclaiming "Pwned by HopSec," but beneath this digital taunt lies a vulnerability: exposed services running on non-standard ports. Your mission is to systematically discover these hidden services through multi-layered port scanning, extract three critical keys scattered across different protocols (FTP, custom TCP, and DNS), and use them to

access a secret admin console. Once inside, you'll uncover additional internal services and retrieve the final flag from the MySQL database, exposing the full extent of the breach and paving the way for complete system recovery.

Key Information

- **Target Server**: `tbfc-devqa01` QA server (IP: `10.81.144.241`) - currently compromised and defaced with the message "Pwned by HopSec"
- **Multi-Protocol Attack Surface**: The server exposes five key services across different ports and protocols:
  - **Port 22/TCP**: SSH (OpenSSH 9.6p1 Ubuntu-3ubuntu13.14)
  - **Port 80/TCP**: HTTP web server (defaced landing page)
  - **Port 21212/TCP**: FTP server (vsFTPd 3.0.5) - contains `tbfc_qa_key1`
  - **Port 25251/TCP**: Custom TBFC maintd v0.2 application - contains `tbfc_qa_key2`
  - **Port 53/UDP & TCP**: DNS server - contains `tbfc_qa_key3` in TXT records
- **Three Critical Keys Required**: All keys follow the format `KEYNAME:KEY` and are distributed across:
  1. FTP anonymous login on port 21212
  2. Netcat connection to custom TBFC app on port 25251 (requires `GET KEY` command)
  3. DNS TXT record query via `dig @10.81.144.241 TXT key3.tbfc.local`
- **Internal Services Discovered Post-Access**: After gaining admin console access using the combined keys (`e3ster_15_th3_n3w_xm45`), additional localhost-only services are revealed:
  - **Port 3306/TCP (127.0.0.1)**: MySQL database (`tbfcqa01`) containing the final flag in the `flags` table
  - **Port 8000/TCP (127.0.0.1)**: Internal application service
  - **Port 7681/TCP (127.0.0.1)**: Additional internal service
- **Reconnaissance Tools**:
  - `nmap` for TCP/UDP port scanning with banner detection (`-p-` for all ports, `--script=banner` for service identification, `-sU` for UDP scanning)
  - `ftp` client for anonymous FTP access
  - `nc` (Netcat) for custom protocol interaction
  - `dig` for DNS queries
  - `ss -tunlp` or `netstat` for listing active listening ports post-exploitation

---

Walk Through

1. Start the target machine and connect to the VPN
2. What evil message do you see on top of the website?
    1. IP `10.81.144.241`
        1. In web-browser go to `http://10.81.144.241`
    2. Top Banner says ~~TBF QA~~ Pwned by HopSec
3. What is the first key part found on the FTP server?
    1. Run a simple scan on `10.81.144.241` using `nmap`
    2. `nmap 10.81.144.241`
        1. Results show `22/tcp open` and `80/tcp open`
        2. Pasted image 20251207142408.png
    3. `nmap -p- --script=banner 10.81.144.241`
        1. `-p-` scans all ports
        2. `--script=banner` shows what is likely behind the ports
        3. This san revealed two extra ports
            1. `21212/tcp open` `(vsFTPd 3.0.5)`
            2. `25251/tcp open` `(TBFC maintd v0.2x0A`
            3. Pasted image 20251207143126.png
    4. Opened `FTP` connection in using `ftp 10.81.144.241 21212`
        1. username `anonymous`
        2. `ls` to list files
        3. `get tbfc qa_key1` to download file
        4. `exit`
        5. `cat tbfc_qa_key1` to view key
        6. Pasted image 20251207144408.png
4. What is the second key part found in the TBFC app?
    1. Use `netcat` to get more information from port `25251`
    2. `nc -v 10.81.144.241 25251`
        1. Pasted image 20251207144836.png
    3. Use `HELP` to view commands
        1. Pasted image 20251207144916.png
    4. Use `GET KEY` to view key
        1. Pasted image 20251207144948.png

5. What is the third key part found in the DNS records? 1. Use `nmap` to scan `UDP` ports instead of `TCP` 2. `nmap -sU 10.81.144.241` 1. Pasted image 20251207150711.png 3. Use `dig` to see records on DNS server 1. `dig @10.81.144.241 TXT key3.tbfc.local` 1. Pasted image 20251207151127.png
6. Which port was the MySQL database running on?
    1. Log into the admin portal at `http://10.81.144.241`
    2. use `e3ster_15_th3_n3w_xm45` to access portal
        1. Pasted image 20251207151548.png
    3. Can use `histroy` to see the terminal history
        1. That reveals ports `56123` and `3306` used in `mysql` commands
    4. Can also use `ss -tulnp` to see open listening connections
        1. This reveals port `3306` is active and listening on the localhost
            1. Pasted image 20251207151953.png
    5. Finally, what's the flag you found in the database?
        1. The history reveals a database of `tbfcqa01`
            1. Pasted image 20251207152151.png
        2. `mysql -D tbfcqa01 -e "show tables;"` to view tables
        3. `mysql -D tbfcqa01 -e "select * from flags;"`
            1. Screenshot 2025-12-07 at 3.26.20 PM.png

Lessons Learned

- **Multi-Protocol Reconnaissance**: Mastered comprehensive port scanning techniques using Nmap (TCP full range, UDP scanning, and banner detection) to identify hidden services beyond the default 1000 ports, discovering that attackers often hide malicious services on non-standard ports like 21212 (FTP) and 25251 (custom TBFC application).
- **Service Enumeration and Exploitation**: Learned to interact with discovered services using protocol-specific tools (FTP client, Netcat for custom protocols, dig for DNS queries) and post-exploitation techniques (ss/netstat for internal service discovery, MySQL querying) to progressively escalate access and extract sensitive information from both external and internal-only services.

Resources

TryHackMe

Dig CheatSheet

MySql CheatSheet

Nmap CheatSheet

NetCat CheatSheet

Revision #2

Created 2025-12-07 20:34:39 UTC by David Rizzo

Updated 2025-12-07 21:00:26 UTC by David Rizzo