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/EqZqVgNdnFNLp1QRnYk4dWkByB7GR8eBeZRTISIpg6WPNw?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.**

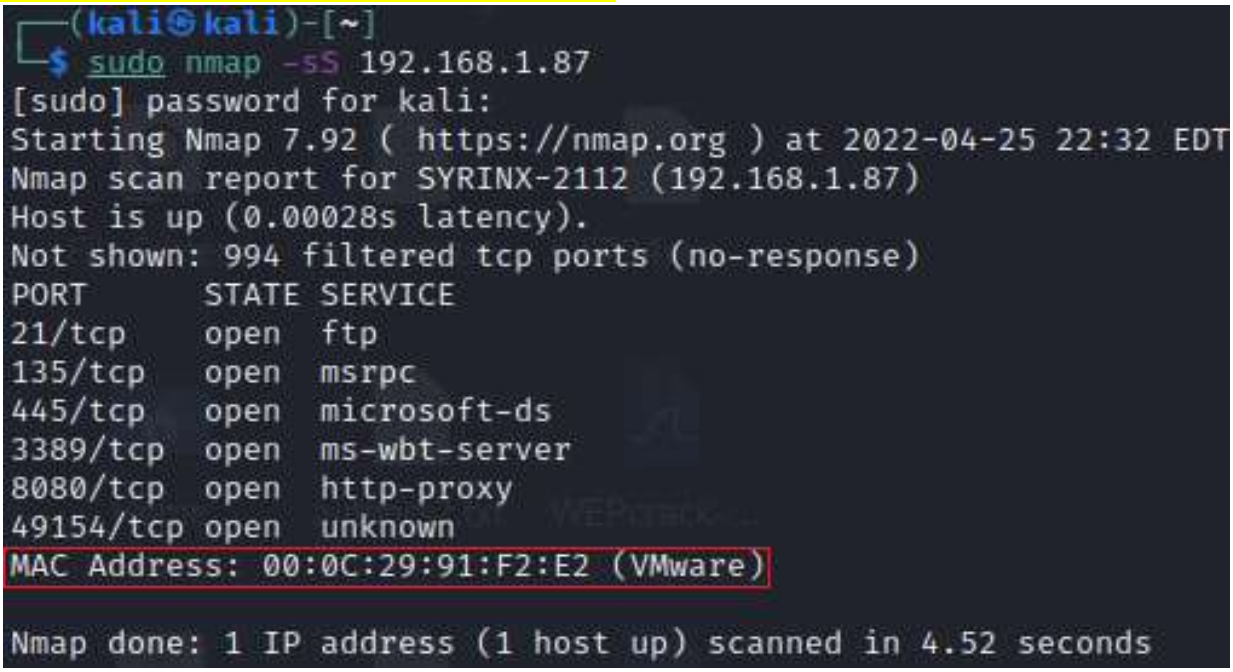
Part 1 Enumeration

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

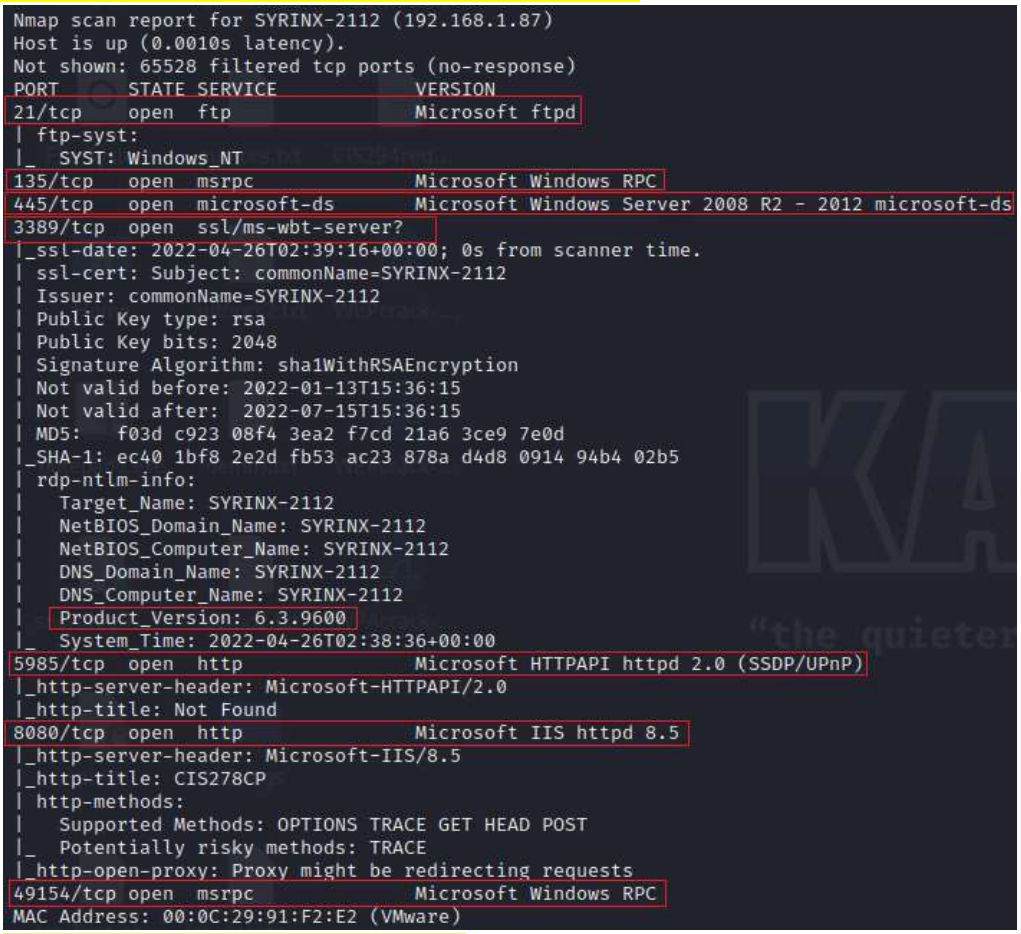
2. Insert a screenshot for the above results



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 microsft-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

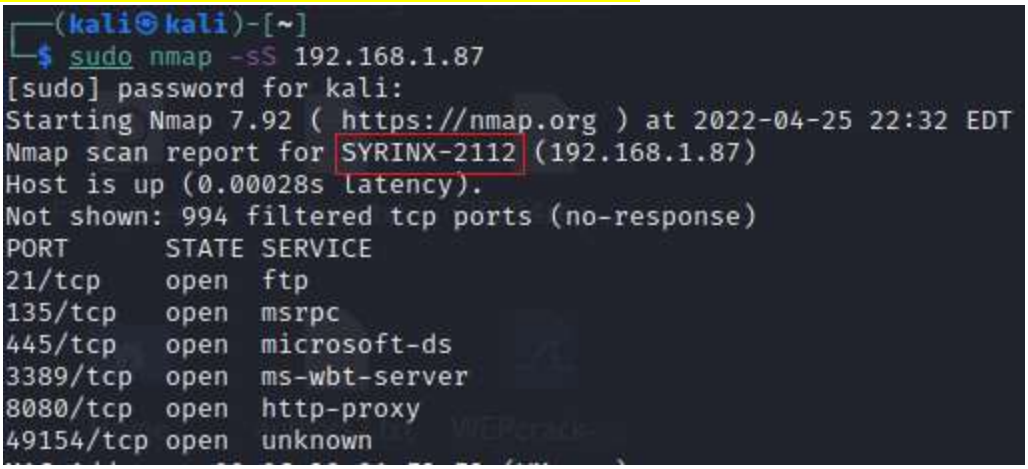
4. Insert a screenshot for the above result.



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

SYRINX-2112

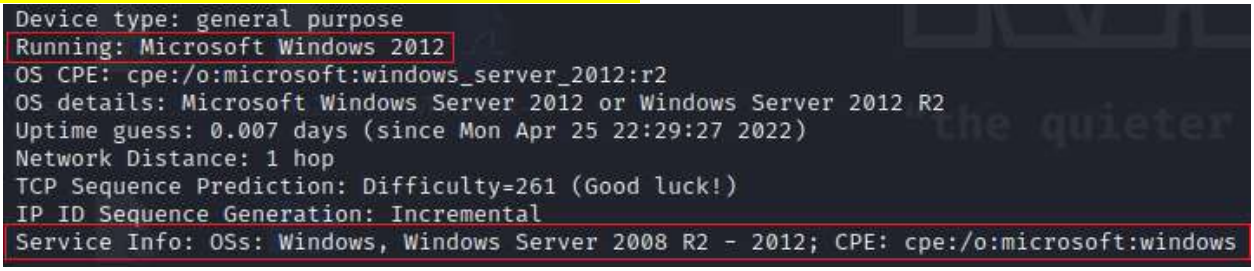
6. Insert a screenshot for the above result.



7. What is the operating system and version?

Microsoft Windows Server 2012 R2

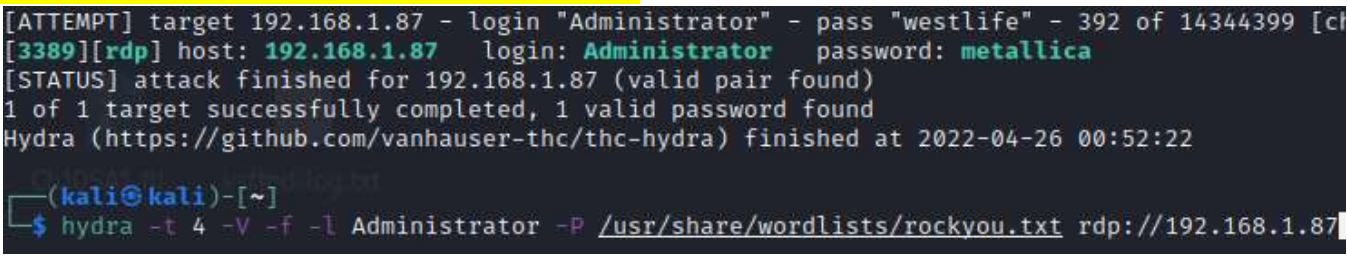
8. Insert a screenshot for the above result.



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

Username: "Administrator" Password: "metallica"

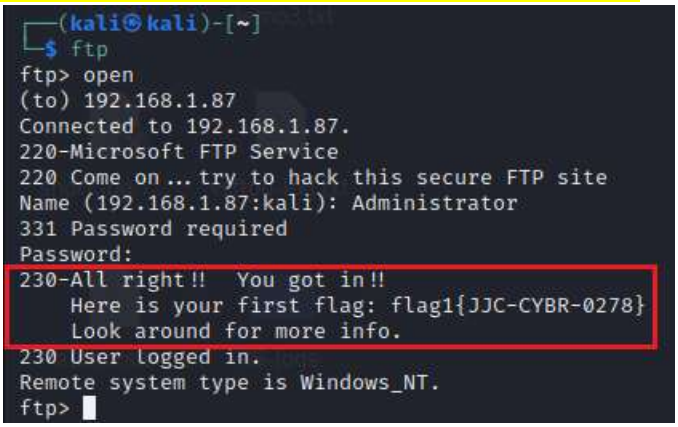
10. Insert a screenshot for the above result.



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."**

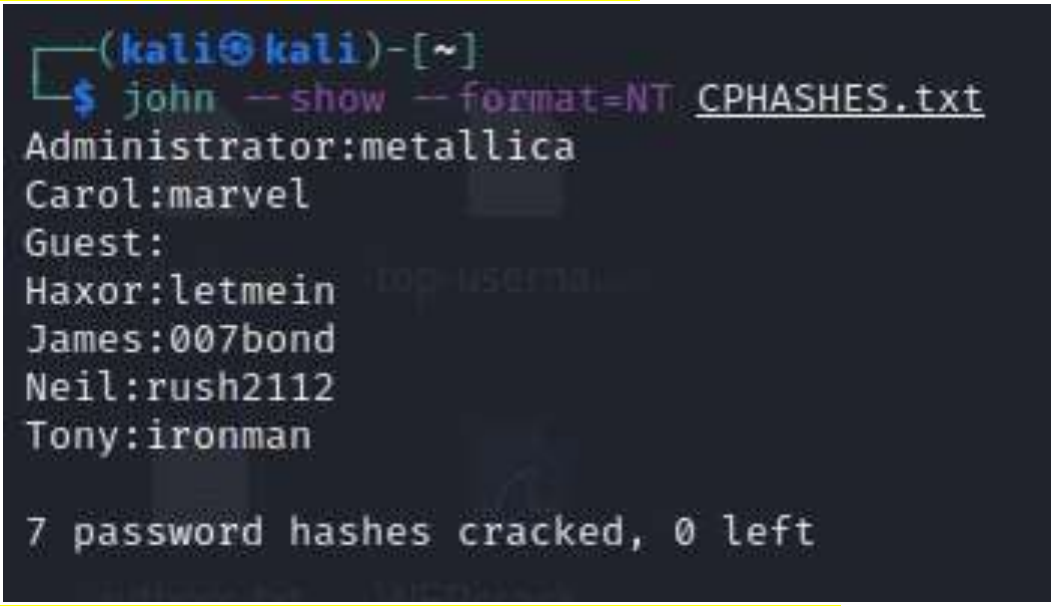
12. Insert a screenshot for the above result.



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.



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.

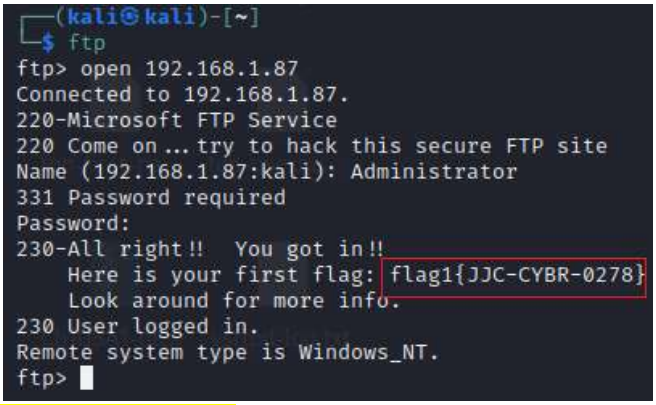
Part 2 Capture the Flags

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}

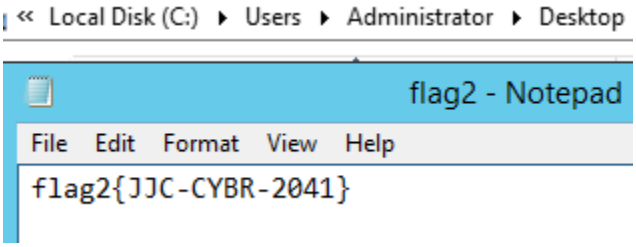
2. Insert a screenshot for the above result.



3. What is flag 2?

Flag2{JJC-CYBR-2041}

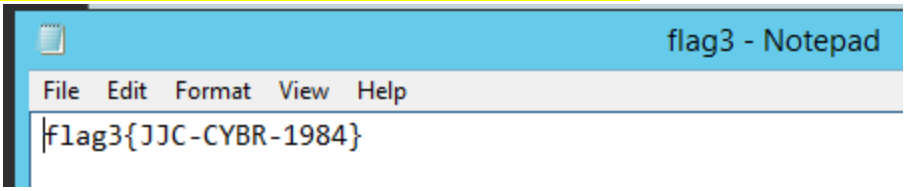
4. Insert a screenshot for the above result.



5. What is flag 3?

Flag3{JJC-CYBR-1984}

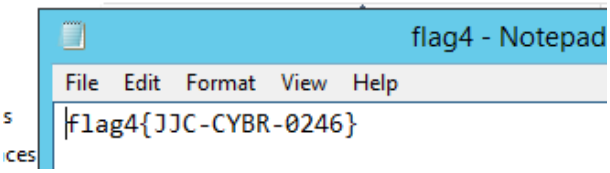
6. Insert a screenshot for the above result.



7. What is flag 4?

Flag4{JJC-CYBR-0246}

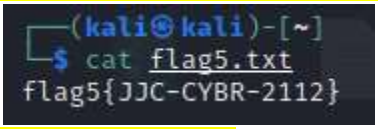
8. Insert a screenshot for the above result.



9. What is flag 5?

Flag5{JJC-CYBR-2112}

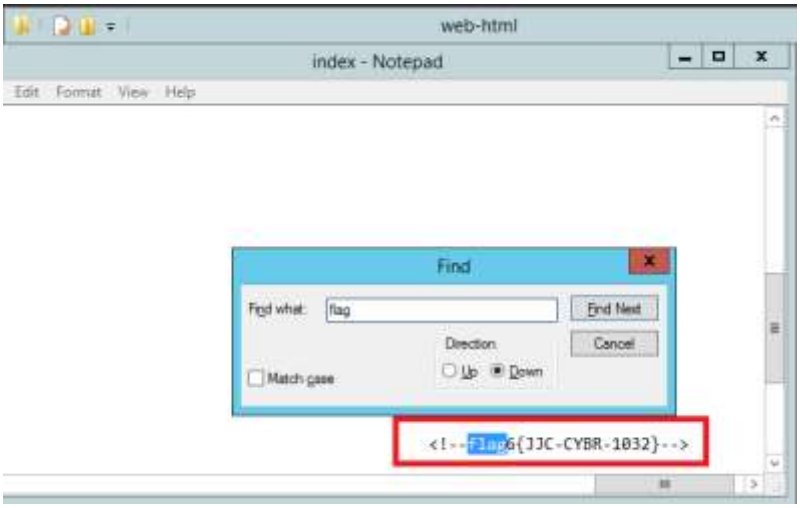
10.Insert a screenshot for the above result.



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.