JOHN WICK CTF

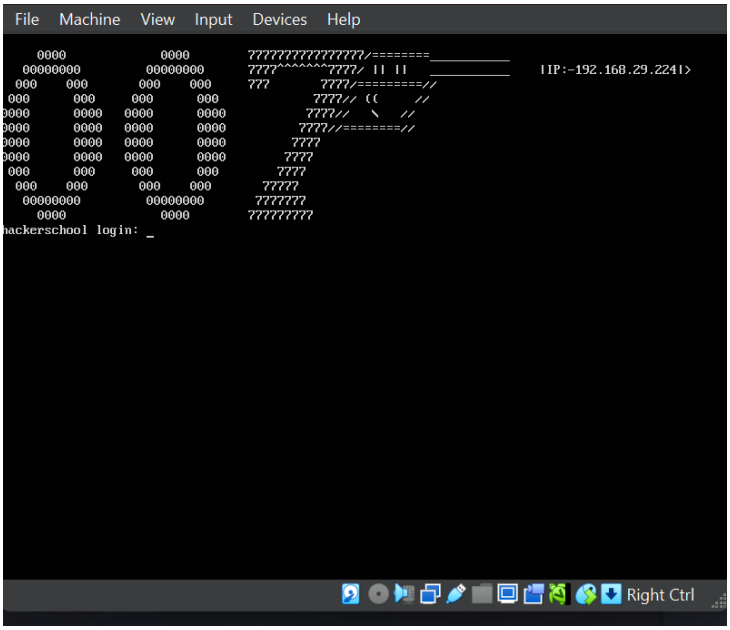
Introduction

This report provides a detailed walkthrough of how the *JohnWick* CTF was analyzed and solved. It includes an overview of the challenge environment, the methodologies used for enumeration and exploitation, and the key findings that led to successfully capturing the flag. The objective of this report is not only to document the solution but also to highlight the learning outcomes and techniques that can be applied in real-world penetration testing scenarios.

Tools used

- Nmap(network scanning)
- Hydra(password cracking)
- Exiftool(meta data inspecting)

Procedure



Fig(1) interface of the ctf

Step -1

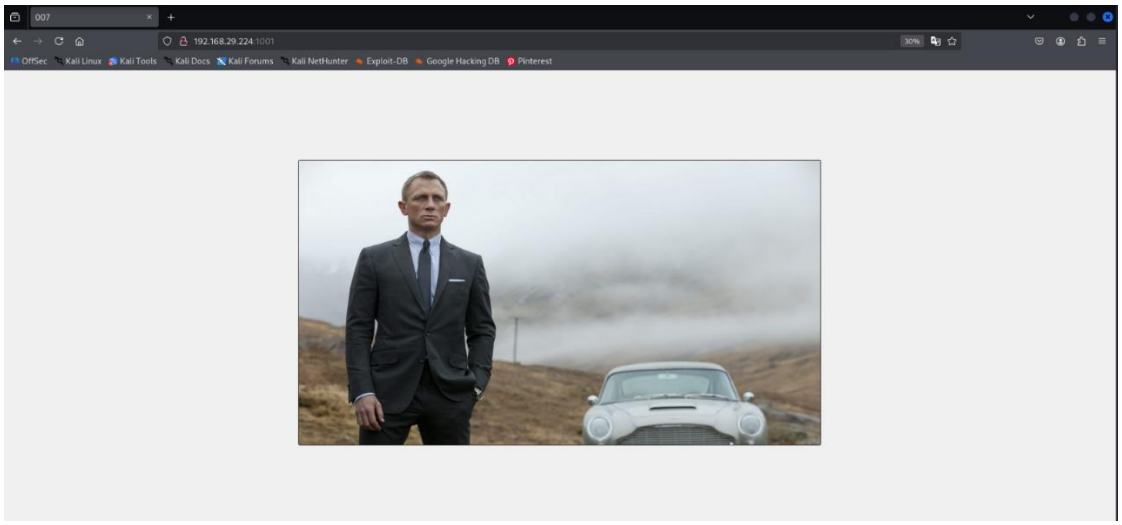
Initiating the nmap aggressive scan on the target ip…

.

we got http abnd ssh services running on port no 1001 & 1111

Step-2

accessing the webpage hosted on port no 1001

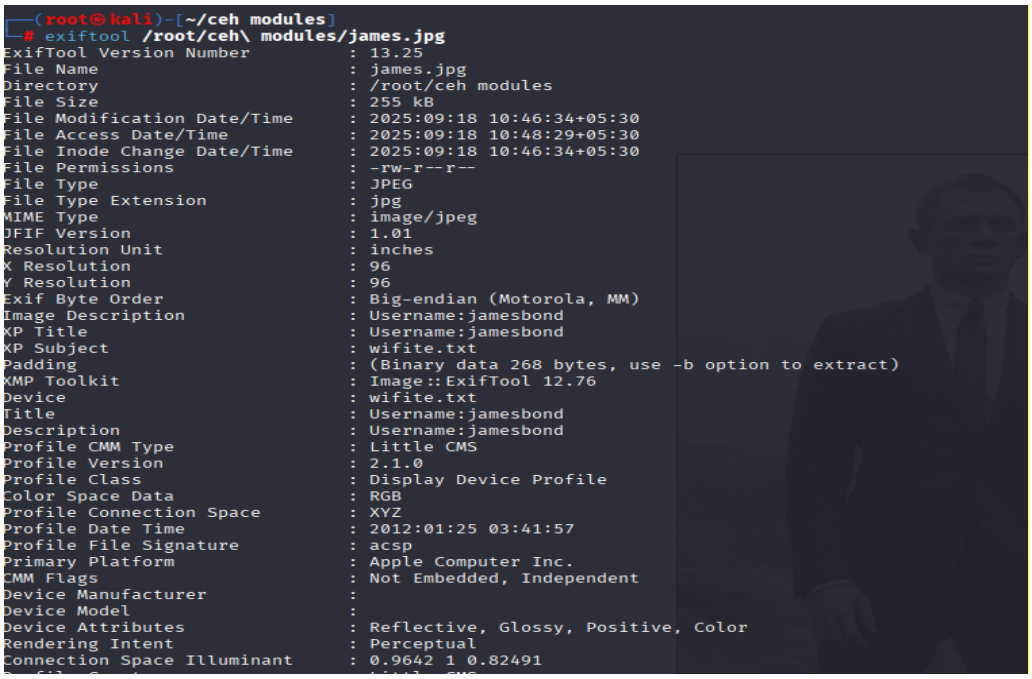


Got this interface and got nothing apart from this. Proceeding to download the image for further analysis

Step-3

Analyzing the metadata of the image using exiftool by migrating to the image path

Now migrating to the image path



As, we can see the title as username:jamesbond let's mark it as the 1st clue

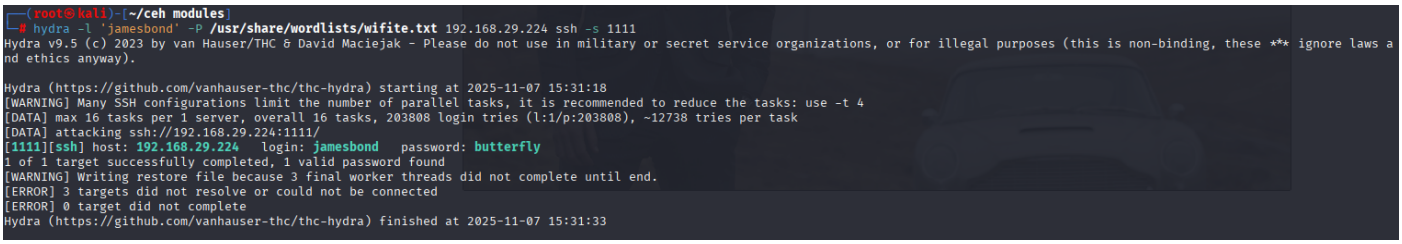
Step-4

As we know there is ssh service running on the target on port 1111 lets try to brute force our way in through hydra

As we can see on the xp-subject section there is a value like ‘wifite.txt’ which matches one is the wordlists in our local system in /usr/share/wordlists/wifite.txt

We are going to use it as the wordlist of the password section then the command goes like

“Hydra -l ‘jamesbond’ -P /usr/share/wordlists/wifite.txt 192.168.29.224 ssh -s 1111”



And we got the password “butterfly” lets login through ssh with the credentials as

Username : jamesbond

Password : butterfly

And just like that we got the access to the machine through ssh

Step-5

Privilege escalation

Tried ‘sudo su’ command to get root privilege and got denied the error shows as follows

“user jamesbond is not allowed to execute ‘/bin/su’ as root on hacker school ”

Lets check for any misconfigured sudo permissions by using sudo-l

And we found /usr/bin/ftp which means we can use that path to escalate privileges the commands are as follows

“Sudo ftp && !/bin/sh” and we got root privileges you can check by using ‘whoami’ command

Conclusion:

The JohnWick CTF required a methodical approach combining file analysis, metadata inspection, and privilege enumeration to achieve the final flag. Initial reconnaissance with tools such as exiftool revealed embedded metadata that guided subsequent steps, while sudo -l exposed a misconfigured privilege that enabled escalation to a privileged shell. The exercise demonstrates the importance of thorough enumeration and the value of seemingly minor artifacts in forensic analysis. These findings reinforce best practices for secure system configuration and metadata hygiene in production environments.