PSP0201

Week 4

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

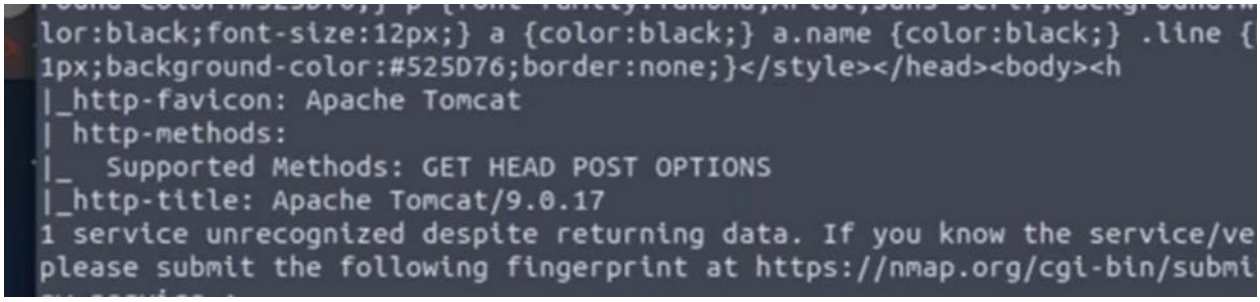
Day 12: Networking – Ready, set, elf

Tools used: Kali Linux and Firefox

Solution/walkthrough:

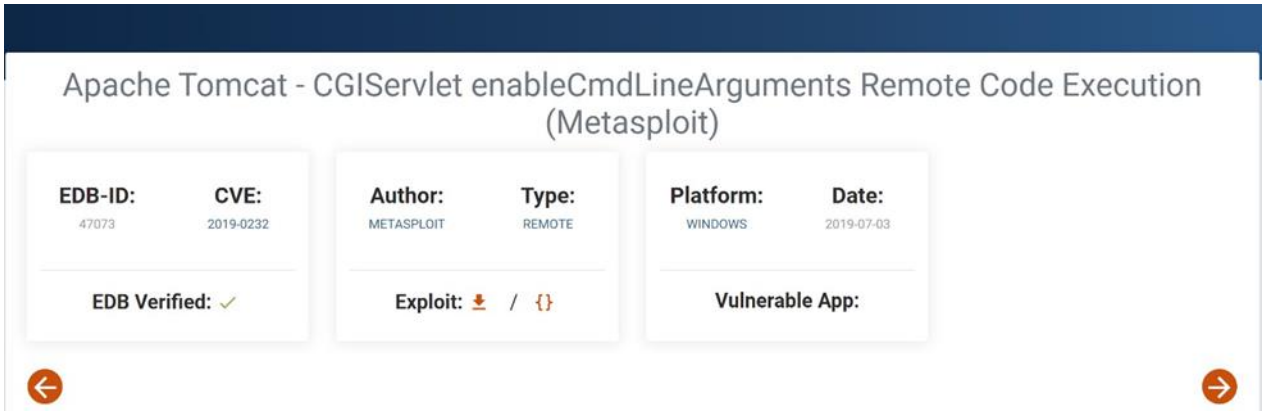
Question 1

We needed to find the info using nmap to find information like hosts, services, ports, and all other information as shown in the picture. Code used: nmap -sVC machine_IP. Under http-title, we found our web server version number.



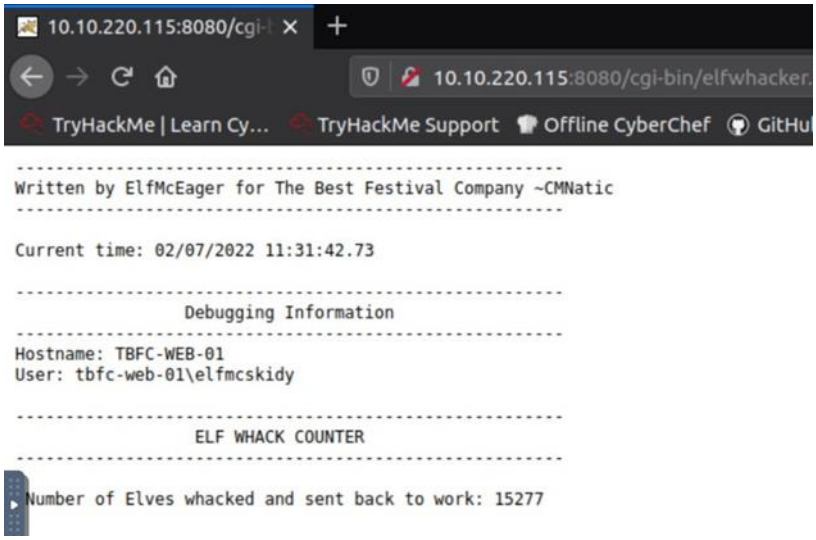
Question 2

We were asked for CVE number. From the website called exploit-db.com, we searched for the vulnerability of Apache Tomcat version 9.0.17 and found the CVE number of the vulnerability.

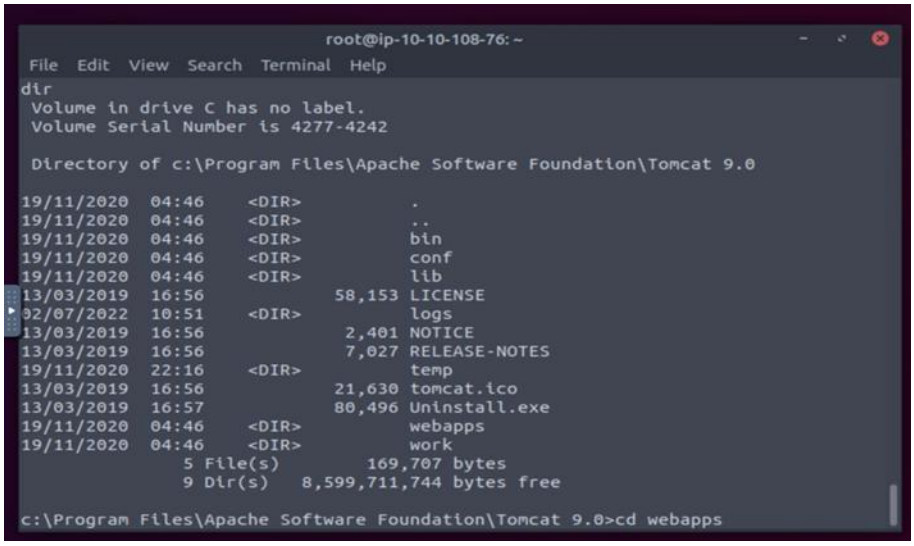


Question 3

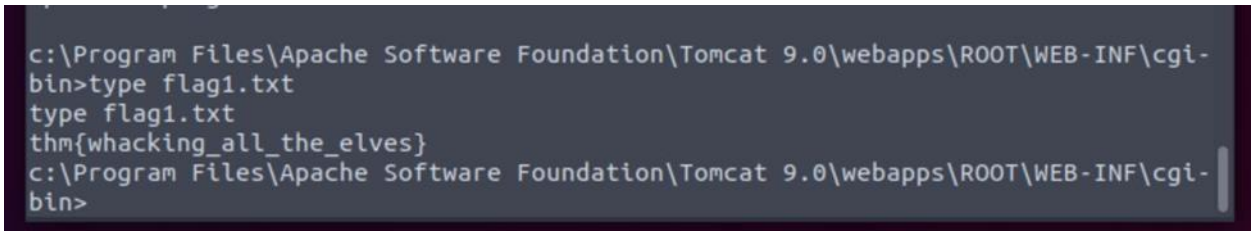
In this question we are asked to find the flag and what's written in it. We used port 8080 and we know the information that we needed was located in /cgi-bin/elfwhacker.bat.



Using the msfconsole command, we use the search command with the CVE number that we obtained. We enter use command with 0 to exploit the vulnerability of that CVE. Then, we set the Metasploit settings with our IP address as the value for LHOST and the remote PC IP address as value for RHOSTS. We also set the TARGETURI value with the location of the script. Then, we use the run command.

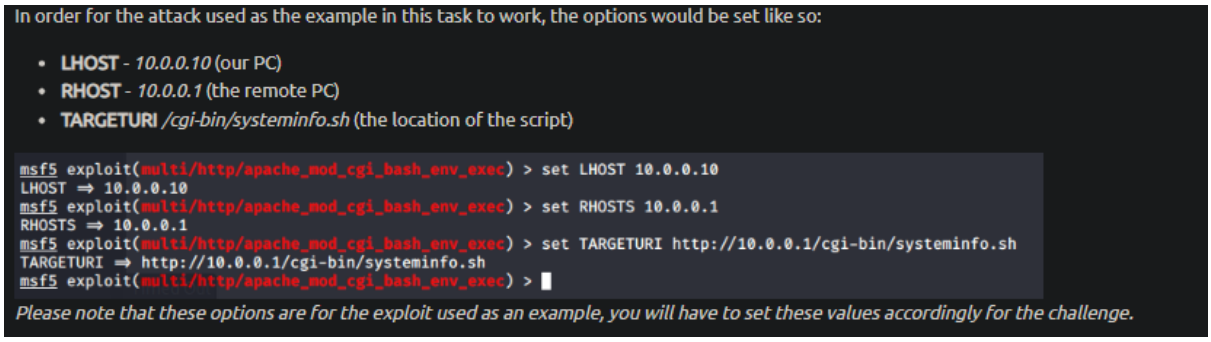


We dropped into a shell. Then, we found a text file named 'flag1.txt' under the cgi-bin directory. We displayed the file content and found our flag which is thm{whacking_all_the_elves}.



Question 4

After reading the instructions, we knew that the Metasploit settings that we had to set are LHOST and RHOST.



Thought Process/Methodology:

First, we did the nmap scan to find the information like ports, services and Apache version etc. For the vulnerability, we searched from the website named exploit- db, and there we got the CVE number. After that, with the port that we have obtained from the nmap scan, we looked for information that we needed which was located under /cgi-bin/elfwhacker.bat. Using msfconsole command, Using the msfconsole command, we use the search command with the CVE number that we obtained. We enter use command with 0 to exploit the vulnerability of that CVE. Then, we set the Metasploit settings with our IP address as the value for LHOST and the remote PC IP address as value for RHOSTS. We also set the TARGETURI value with the location of the script. Then, we use the run command. We dropped into a shell. Then, we found a text file named ‘flag1.txt’ under the cgi-bin directory. We displayed the file content and found our flag which is thm{whacking_all_the_elves}.