

# Thompson\_THM

## Enumeration

```
# FOund a apache main page on port 8080

# Used default credentials tomcat:s3cret to login

# Uploaded a war msfvenom payload and ran multi handler

# Got a shell
```

## Nmap

```
nmap -p22,8080,8009 $ip -sS -sV -A -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 08:29 EDT
Nmap scan report for 10.10.208.145
Host is up (0.48s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|  2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|  256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_ 256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http     Apache Tomcat 8.5.5
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/8.5.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1  202.08 ms 10.4.0.1
2  ... 3
4  466.41 ms 10.10.208.145

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 41.52 seconds
```

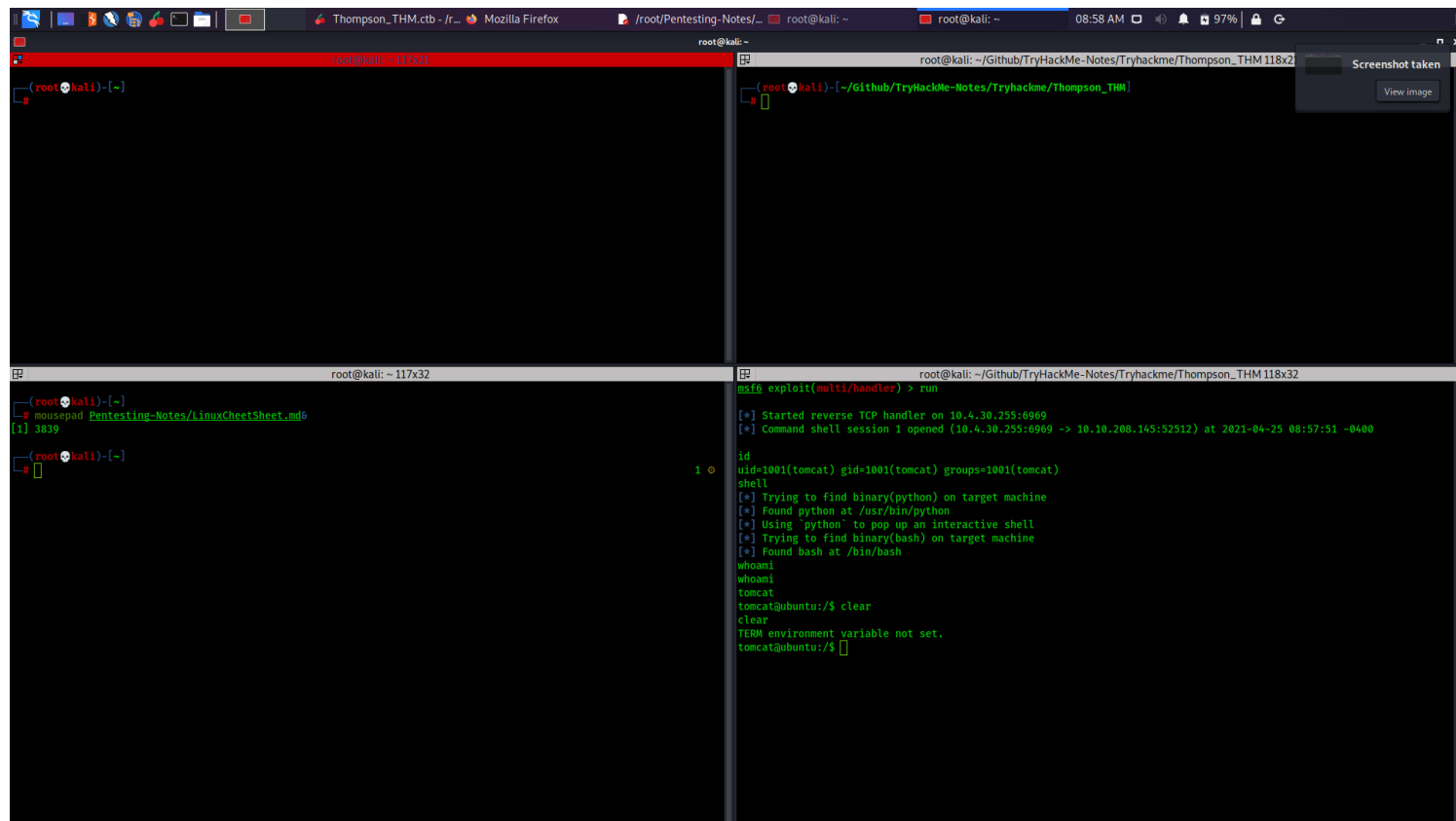
## SSH:22

## Tomcat:8080

```
# Logged in /manager using default credenrials

# Uploaded a war msfvenom payload
```

# ran multi handler and got a shell



#

## Exploitation

## Post Exploitation

# We get user flag

# We Now See a cronjob running in a id.sh file being run by root and we can write to that file so we will just spawn a root shell from there

The screenshot displays a Kali Linux terminal window with multiple tabs open at the top, including "Thompson\_THM.ctb - /r-...", "TryHackMe | Thompson ...", "/root/Pentesting-Notes | root@kali: ~", "root@kali: ~/Github/Try...", and "O9:05 AM". The active terminal session is on the "root@kali: ~/Github/TryHackMe-Notes/Tryhackme/Thompson\_THM" tab.

The user has logged in as tomcat on an Ubuntu machine. The terminal shows the following commands and output:

```
tomcat@ubuntu:/home/jack$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    cd /home/jack && bash id.sh
```

After editing the crontab, the user runs `ls` and `id.sh test.txt user.txt`. Then, they run `ls -la`, which produces the following output:

```
total 48
drwxr-xr-x 4 jack jack 4096 Aug 23 2019 .
drwxr-xr-x 3 root root 4096 Aug 14 2019 ..
-rw-r--r-- 1 root root 1476 Aug 14 2019 .bash_history
-rw-r--r-- 1 jack jack 220 Aug 14 2019 .bash_logout
-rw-r--r-- 1 jack jack 3771 Aug 14 2019 .bashrc
-rwx----- 2 jack jack 4096 Aug 14 2019 .cache
-rwxr-xr-x 1 jack jack 26 Aug 14 2019 id.sh
drwxr-xr-x 2 jack jack 4096 Aug 14 2019 .nano
-rw-r--r-- 1 jack jack 655 Aug 14 2019 .profile
-rw-r--r-- 1 jack jack 0 Aug 14 2019 .sudo_as_admin_successful
-rw-r--r-- 1 root root 39 Apr 25 06:05 test.txt
-rw-r--r-- 1 jack jack 33 Aug 14 2019 user.txt
-rw-r--r-- 1 root root 183 Aug 14 2019 .wget-hsts
tomcat@ubuntu:/home/jack$
```

```
# we write a reverse shell code of bash and get a root shell back
```

## Loot

## Credentials

## # Tomcat Manager

tomcat:s3cret

## Flags

```
# User flag
```

39400c90bc683a41a8935e4719f181bf

```
# Root Flag
```

d89d5391984c0450a95497153ae7ca3a