

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

Objetivos

Utilice varias fuentes útiles para investigar más a fondo las vulnerabilidades.

- Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)
- Parte 2: Explorar las enumeraciones de debilidades comunes (CWE)
- Parte 3: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)
- Parte 4: Investigar las vulnerabilidades en el sistema común de puntuación de vulnerabilidades (CVSS)

Aspectos básicos/Situación

En una práctica de laboratorio anterior, encontró varias vulnerabilidades después de escanear un sistema de destino. Ahora utilizará varias fuentes ampliamente disponibles para profundizar en los detalles de las vulnerabilidades. Asignará e investigará las vulnerabilidades en la lista de vulnerabilidades y exposiciones comunes (CVE), la enumeración de debilidades comunes (CWE), la base de datos nacional de vulnerabilidades del NIST y el sistema de puntuación de vulnerabilidades comunes (CVSS).

Recursos necesarios

- Computadora con conexión a Internet

Instrucciones

Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)

Paso 1: Explore CVE.

NO TIENE QUE COLOCAR CAPTURAS EN ESTE PASO 1

- a. Inicie el sitio web de CVE y vaya a www.cve.org.
 - b. Lea la descripción general del programa CVE.
 - 1) Seleccione **About > Overview** en el menú.
 - 2) Vea el video de descripción general del programa CVE.
 - 3) Consulte los podcasts disponibles para obtener información más detallada sobre el programa CVE.
- ¿Cuál es la misión del programa CVE?

Identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas.

¿Quién asigna los ID de CVE?

Las autoridades de numeración de CVE (CNA)

¿Cuáles son los dos objetivos principales del programa CVE?

Escalar el programa para una adopción y cobertura más amplias, y producir más registros CVE más rápidamente (más cerca del tiempo real).

¿Quién opera la CVE?

MITRE Corporation con financiación del Departamento de Seguridad Nacional de EE. UU. (DHS) y el Componente de administración de vulnerabilidades (VMC) de la Agencia de seguridad de infraestructura y ciberseguridad (CISA).

Paso 2: Utilice el programa CVE para recopilar información sobre las vulnerabilidades.

En una práctica de laboratorio anterior, analizó un sistema de destino en busca de vulnerabilidades. La lista de vulnerabilidades encontradas arrojó los siguientes seis CVE:

- CVE-2021-41617

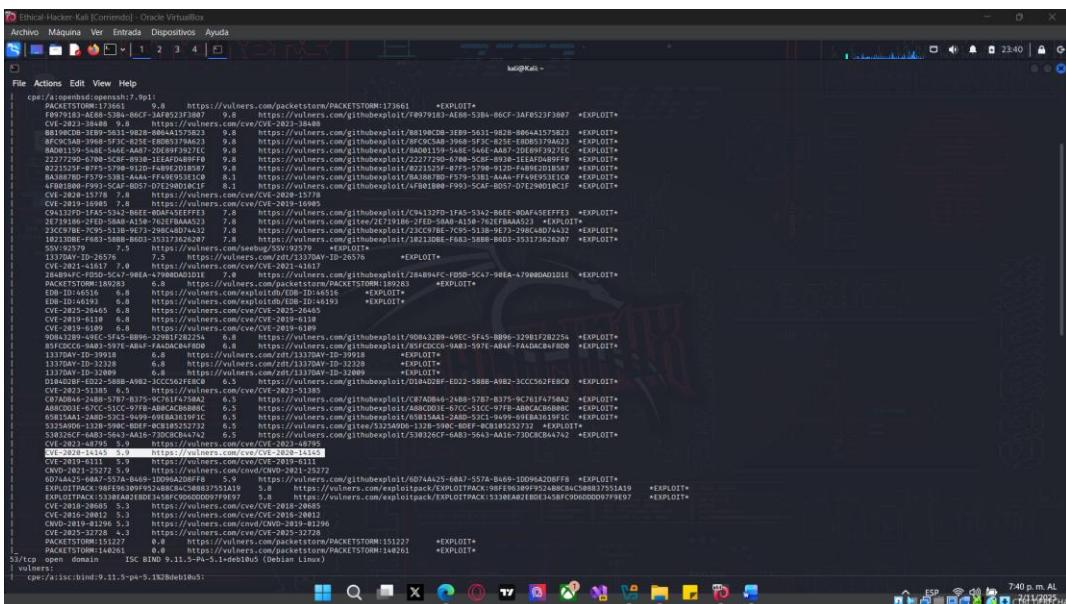
```

ethical-hacker-Kali [Comiendo] - Oracle VirtualBox
Archivo Maquina Ver Entrada Dispositivos Ayuda
kali㉿Kali ~
File Actions Edit View Help
cve /root/cve/outputs/cve-2021-41617.9p1:
PACKETSTORM:173661 9.8 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT+
F0979183-AE8B-5384-86CF-3AF0523F3807 9.8 https://vulners.com/githubexploit/F0979183-AE8B-5384-86CF-3AF0523F3807 *EXPLOIT+
CVE-2023-38488 9.8 https://vulners.com/cve/CVE-2023-38488
B8C95C0B-5646-546E-A875-E80853792023 9.8 https://vulners.com/githubexploit/B8C95C0B-5646-546E-A875-E80853792023 *EXPLOIT+
B8D01159-548E-546E-AA87-2D089F3927EC 9.8 https://vulners.com/githubexploit/B8D01159-548E-546E-AA87-2D089F3927EC *EXPLOIT+
2227729D-70B-5CBF-B930-1EEAFD499F0 9.8 https://vulners.com/githubexploit/2227729D-70B-5CBF-B930-1EEAFD499F0 *EXPLOIT+
A83887BD-548E-546E-AA87-2D089F3927EC 9.8 https://vulners.com/githubexploit/A83887BD-548E-546E-AA87-2D089F3927EC *EXPLOIT+
BA3887BD-548E-546E-AA87-2D089F3927EC 8.3 https://vulners.com/githubexploit/BA3887BD-548E-546E-AA87-2D089F3927EC *EXPLOIT+
4FB01B80-1993-5CAF-BD57-D7E290D08C1F 8.1 https://vulners.com/githubexploit/4FB01B80-1993-5CAF-BD57-D7E290D08C1F *EXPLOIT+
CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
CVE-2020-15779 7.8 https://vulners.com/cve/CVE-2020-15779
C94132FD-F5A5-5342-BEEE-00DAFA5EEFF13 7.8 https://vulners.com/githubexploit/C94132FD-F5A5-5342-BEEE-00DAFA5EEFF13 *EXPLOIT+
2E71918B-7FED-58AB-A150-762F8AA5A23 7.8 https://vulners.com/cve/2E71918B-7FED-58AB-A150-762F8AA5A23 *EXPLOIT+
23CC978E-C959-513B-9E73-299C48D74432 7.8 https://vulners.com/githubexploit/23CC978E-C959-513B-9E73-299C48D74432 *EXPLOIT+
1031370DAY-ID-35317363287 7.8 https://vulners.com/githubexploit/1031370DAY-ID-35317363287 *EXPLOIT+
SSV92579 7.5 https://vulners.com/seebug/SSV92579 *EXPLOIT+
1337DAY-ID-26576 7.5 https://vulners.com/zot/1337DAY-ID-26576 *EXPLOIT+
...
2A4B94FC-1D99-547E-47980D42D1D 7.0 https://vulners.com/githubexploit/2A4B94FC-1D99-547E-47980D42D1D *EXPLOIT+
PACKETSTORM:189283 6.8 https://vulners.com/packetstorm/189283 *EXPLOIT+
E0B-ID:46516 6.8 https://vulners.com/exploitdb/E0B-ID:46516 *EXPLOIT+
E0B-ID:46516 6.8 https://vulners.com/exploitdb/E0B-ID:46516 *EXPLOIT+
CVE-2023-36465 6.8 https://vulners.com/cve/CVE-2023-36465 *EXPLOIT+
CVE-2019-6118 6.8 https://vulners.com/cve/CVE-2019-6118
CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109
9084-597E-546E-546E-BB96-32981F2B2284 6.8 https://vulners.com/githubexploit/9084-597E-546E-546E-BB96-32981F2B2284 *EXPLOIT+
85FCDC6-9A07-597E-AB4F-FA0AC08C8FB08 6.8 https://vulners.com/githubexploit/85FCDC6-9A07-597E-AB4F-FA0AC08C8FB08 *EXPLOIT+
1337DAY-ID-39918 6.8 https://vulners.com/zot/1337DAY-ID-39918 *EXPLOIT+
1337DAY-ID-33220 6.8 https://vulners.com/githubexploit/1337DAY-ID-33220 *EXPLOIT+
1337DAY-ID-33220 6.8 https://vulners.com/githubexploit/1337DAY-ID-33220 *EXPLOIT+
1337DAY-ID-32809 6.8 https://vulners.com/githubexploit/1337DAY-ID-32809 *EXPLOIT+
D184028F-ID22-5888-A9B2-3CC562F8C0 6.5 https://vulners.com/githubexploit/D184028F-ID22-5888-A9B2-3CC562F8C0 *EXPLOIT+
CVE-2023-5138 6.5 https://vulners.com/cve/CVE-2023-5138
CVE-2018-14145 5.9 https://vulners.com/cve/CVE-2018-14145
CVE-2018-14145 5.9 https://vulners.com/cve/CVE-2018-14145
CVE-2018-14145 5.9 https://vulners.com/cve/CVE-2018-14145
CVE-2018-14145 5.9 https://vulners.com/cve/CVE-2018-14145
6074A425-60A7-557A-B469-1D096A28BF8 5.9 https://vulners.com/githubexploit/6074A425-60A7-557A-B469-1D096A28BF8 *EXPLOIT+
EXPLOITPACK:98F9E6309F924B8C04C308837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98F9E6309F924B8C04C308837551A19 *EXPLOIT+
EXPLOITPACK:5330E0A2E8D2345B1C9D0000979E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330E0A2E8D2345B1C9D0000979E97 *EXPLOIT+
CVE-2018-20812 5.3 https://vulners.com/cve/CVE-2018-20812
CVE-2018-20812 5.3 https://vulners.com/cve/CVE-2018-20812
CNVD-2019-01296 5.3 https://vulners.com/cnv/CNVD-2019-01296
CNVD-2019-01296 5.3 https://vulners.com/cnv/CNVD-2019-01296
PACKETSTORM:151227 0.8 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT+
PACKETSTORM:140261 0.8 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT+
53/tcp open domain ISC BIND 9.11.5-p4-5.1+deb10u5 (Debian Linux)
| vulnless:
| cpe:/a:isc:bind:9.11.5-p4-5.1+deb10u5:

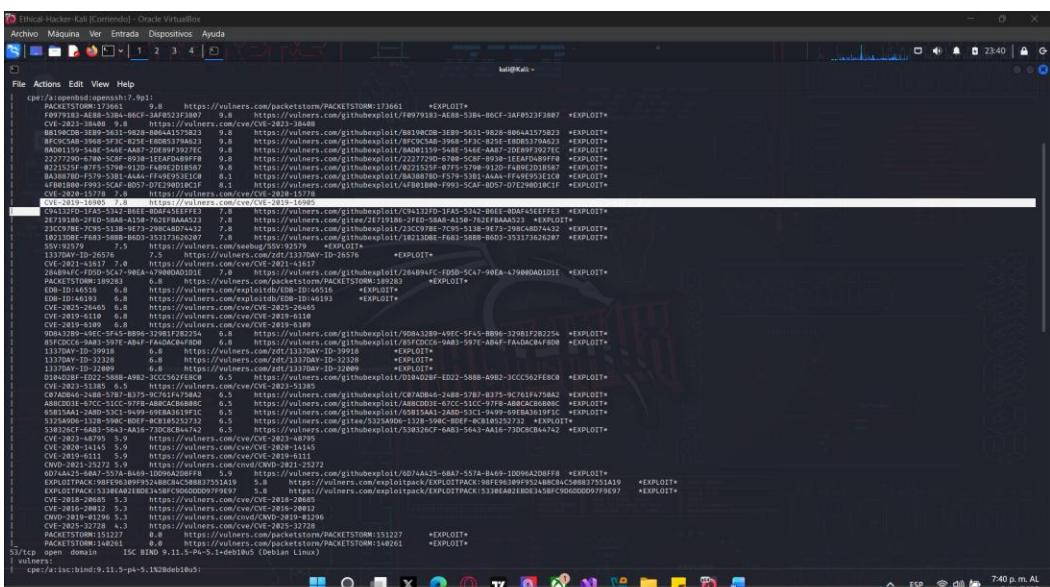
```

- CVE-2020-14145

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades



- CVF-2019-16905



- CVE-2010-6111

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

Ethical-Hacker-Kali-Commands - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Actions Edit View Help

```
c:\\>cd\\pentest\\exploits\\7-pwn  
c:\\>python3 exploit.py -r https://vulnern.com/packetstorm/PACKETSTORM1173661 *EXPLOIT*  
F997913B-AE8B-5B6A-86C7-3AF23F3807 9.8 https://vulnern.com/github/exploit/F997913B-AE8B-5B6A-86C7-3AF23F3807 *EXPLOIT*  
CVE-2021-31488 9.8 https://vulnern.com/cve-2021-31488  
F0FC534B-3968-93C6-B25E-0BB63789A62 9.8 https://vulnern.com/github/exploit/F0FC534B-3968-93C6-B25E-0BB63789A62 *EXPLOIT*  
222729D-70B6-5C8F-11E46D49FF0 9.8 https://vulnern.com/github/exploit/222729D-70B6-5C8F-11E46D49FF0 *EXPLOIT*  
B2113E8F-73F5-192D-9071-000000000000 9.8 https://vulnern.com/github/exploit/B2113E8F-73F5-192D-9071-000000000000 *EXPLOIT*  
A4FB9393-9C4F-5C97-8057-07E29001C8 9.8 https://vulnern.com/github/exploit/A4FB9393-9C4F-5C97-8057-07E29001C8 *EXPLOIT*  
F493B808-7A80-5A8A-9000-000000000000 9.8 https://vulnern.com/github/exploit/F493B808-7A80-5A8A-9000-000000000000 *EXPLOIT*  
CVE-2020-16985 7.8 https://vulnern.com/cve-2020-16985  
F7713816-708C-5A84-415B-7262F8AA52 7.8 https://vulnern.com/github/exploit/F7713816-708C-5A84-415B-7262F8AA52 *EXPLOIT*  
23CC78E-70C9-513B-9E73-3F94B04432 7.8 https://vulnern.com/github/exploit/23CC78E-70C9-513B-9E73-3F94B04432 *EXPLOIT*  
S3373537-2000-5000-0000-000000000000 7.5 https://vulnern.com/github/exploit/S3373537-2000-5000-0000-000000000000 *EXPLOIT*  
CVE-2021-41637 7.0 https://vulnern.com/cve-2021-41637  
284494F4-F50D-5B84-A19A-79800AD1B1 7.0 https://vulnern.com/github/exploit/284494F4-F50D-5B84-A19A-79800AD1B1 *EXPLOIT*  
EDB-ID:45516 6.5 https://vulnern.com/exploit/EDB-ID:45516 *EXPLOIT*  
CVE-2023-26465 6.5 https://vulnern.com/cve-2023-26465  
CVE-2023-6112 6.5 https://vulnern.com/cve-2023-6112  
CVE-2023-5000 6.5 https://vulnern.com/cve-2023-5000  
NS0432B0-9043-8000-2961BF3B2250 6.0 https://vulnern.com/github/exploit/NS0432B0-9043-8000-2961BF3B2250 *EXPLOIT*  
3337DAY-ID-39913 6.0 https://vulnern.com/github/exploit/3337DAY-ID-39913 *EXPLOIT*  
3337DAY-ID-39914 6.0 https://vulnern.com/github/exploit/3337DAY-ID-39914 *EXPLOIT*  
3337DAY-ID-39915 6.0 https://vulnern.com/github/exploit/3337DAY-ID-39915 *EXPLOIT*  
D104028-E022-508B-A912-CCC552FEB0C 6.2 https://vulnern.com/github/exploit/D104028-E022-508B-A912-CCC552FEB0C *EXPLOIT*  
C7A8084A-7076-8735-9761f7a50a 6.2 https://vulnern.com/github/exploit/C7A8084A-7076-8735-9761f7a50a *EXPLOIT*  
55815A83-246D-5C13-9549-0984A83F9C 6.2 https://vulnern.com/github/exploit/55815A83-246D-5C13-9549-0984A83F9C *EXPLOIT*  
55233040-246D-5C13-9549-0984A83F9C 6.2 https://vulnern.com/github/exploit/55233040-246D-5C13-9549-0984A83F9C *EXPLOIT*  
CVE-2023-46795 5.9 https://vulnern.com/cve-2023-46795  
LVE-2023-0111 5.9 https://vulnern.com/cve-2023-0111  
0V4432AC-5574-8449-9000-000000000000 5.8 https://vulnern.com/github/exploit/0V4432AC-5574-8449-9000-000000000000 *EXPLOIT*  
EXPLOITPACK-9087-5574-8449-9000-000000000000 5.8 https://vulnern.com/exploitpack/EXPLOITPACK-9087-5574-8449-9000-000000000000 *EXPLOIT*  
CVE-2020-26865 5.8 https://vulnern.com/cve-2020-26865  
CVE-2023-27209 5.8 https://vulnern.com/cve-2023-27209  
CVE-2023-27210 6.3 https://vulnern.com/cve-2023-27210  
PACKETSTORM114261 6.0 https://vulnern.com/github/exploit/PACKETSTORM114261 *EXPLOIT*  
vulner  
c:\\>nc -l -p 9-11 -e /bin/sh -b0b0b0b0:  
c:\\>./a2
```

- CVE-2019-6110

- #### • CVE-2019-6109

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

COLOCAR CAPTURA DE PANTALLA EN TODOS LOS SIGUIENTES PUNTOS

- a. Ingrese la información **CVE-2021-41617** en la ventana de búsqueda y haga clic en **Find(Buscar)**.

¿Qué versiones de OpenSSH están sujetas a esta vulnerabilidad?

Ethical-Hacker-Kali [Corriendo] - Oracle VirtualBox

Archivo Maquina Ver Entrada Dispositivos Ayuda

New Tab [CVE-2021-41677_vulner](#) +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB CMSec

<https://www.vulners.com/cve/CVE-2021-41677>

VULNERS | Lucene search | Searching through 3M+ vulnerabilities and exploits

Start 30-day trial

Database Scanner Email Webhook Resources Plugins Pricing Contacts Settings

VULNERS > CVE > CVE-2021-41617

24 SEP 2021 10:15:07 REPORTED BY MITRE TYPE AD CVE WEB NVD.NIST.GOV 16 MEDIA MENTIONS 16880 VIEWS

ssh privilege escalation in OpenSSH

OpenSSH is vulnerable to privilege escalation before 8.0 when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

Show less ^

Get Started with AI Insights: Log in or Create an Account

Leverage the power of AI to quickly understand vulnerabilities, impacts, and exploitability

Try AI Insights

Related Detection Refs Social

T1 Reporter T1 Title T1 Published T1 Views T1 Family All 197

IBM Security Bulletin Security Bulletin: IBM Guardium Data Security Center is affected by m... 19 Jun 2025 Item 10680

Vulners AI Score 7.5 High risk

CVSS 2 4.4

CVSS 3.1 7

EPSS 0.00469

cve-2021-41677 openssl ssh privilege escalation security vulnerability

26 Sep 2021 19:15 Current

7.5 High risk

Sign in →

Versiones de la 6.2 a la 8.x, anteriores a la 8.8

¿Cuándo se actualizó por última vez este CVE?

14 de Febrero 2023.

- b. En la parte inferior de la página, haga clic en **CVE-2021-41617** para ver información adicional sobre la CVE de la base de datos nacional de vulnerabilidades (NVD) del NIST.

¿Cuál es la puntuación de gravedad de CVSS 3.x para esta CVE?

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

CVE-2021-41617

CVSS 2: 4.4

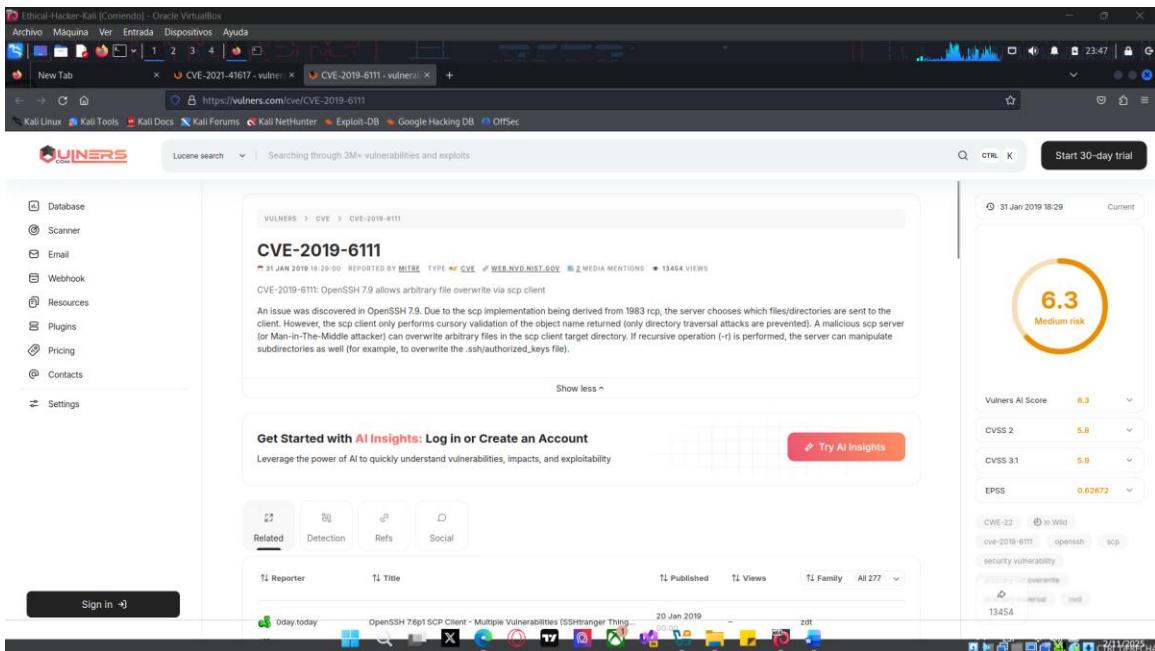
CVSS 3.1: 7

EPPS: 0.00469

7.0 ALTO

- c. Repita los pasos a y b. para revisar la información de las otras cinco CVE.

¿Cuál de estas CVE implica ataques de intermediario desde un servidor SCP malicioso?



CVE-2019-6111

CVSS 2: 5.8

CVSS 3.1: 5.9

EPPS: 0.63672

CVE-2019-6111

- d. En el sitio de CVE (www.cve.org), ingrese **CVE-2019-6111** en el cuadro de búsqueda y haga clic en **Find(Buscar)**.
- e. Desplácese hasta la parte inferior de la página CVE y haga clic en **CVE-2019-6111** para ver información adicional sobre el NVD.
- f. En la página NVD para **CVE-2019-6111**, desplácese hacia abajo hasta la sección **Weakness Enumeration**.

¿Qué ID de CWE está asociado con esta CVE?

CWE-22

The screenshot shows the CVE search results for the ID CVE-2019-6111. The main content area displays the following information:

- Registro CVE encontrado:** CVE-2019-6111, CNA: Corporación MITRE.
- Descripción:** Se describió un problema en OpenSSH 7.9. Debido a que la implementación de scp se deriva de 1983, el servidor elige qué archivos/directorios se envían al cliente. Sin embargo, el cliente scp solo realiza una validación superficial del nombre de objeto devuelto (solo se evitan los ataques transversales de directorio). Un servidor scp malfuncionando (o atacante Man-in-The-Middle) puede sobreescribir archivos arbitrarios en el directorio de destino del cliente scp. Si se realiza la operación recursiva (-r), el servidor también puede manipular subdirectorios (por ejemplo, para sobreescribir el archivo .ssh/authorized_keys).
- Otros resultados:** Mostrando 1 - 4 de 4 resultados de CVE-2019-6111.
- Filtros:** Mostrar: 25, Ordenar por: ID de CVE (nuevo a antiguo).

Registre esta ID de CWE para usar en la Parte 2.

- g. Repita los pasos del a al d. para obtener los ID de CWE asociados con las otras CVE devueltas.

¿Qué CWE están asociadas con cada una de las otras cinco CVE?

CWE-203, CWE-190, CWE-116, CWE-838

CVE-2021-41617 → NVD-CWE-Other (sin mapeo más específico).

CVE-2020-14145 → CWE-203 (Observable Discrepancy / side-channel).

CVE-2019-16905 → CWE-190 (Integer Overflow or Wraparound).

CVE-2019-6110 → CWE-838 (Argument Injection or Modification).

CVE-2019-6109 → CWE-116 (Improper Encoding or Escaping of Output).

Registre estas ID de CWE para usarlas en la Parte 2.

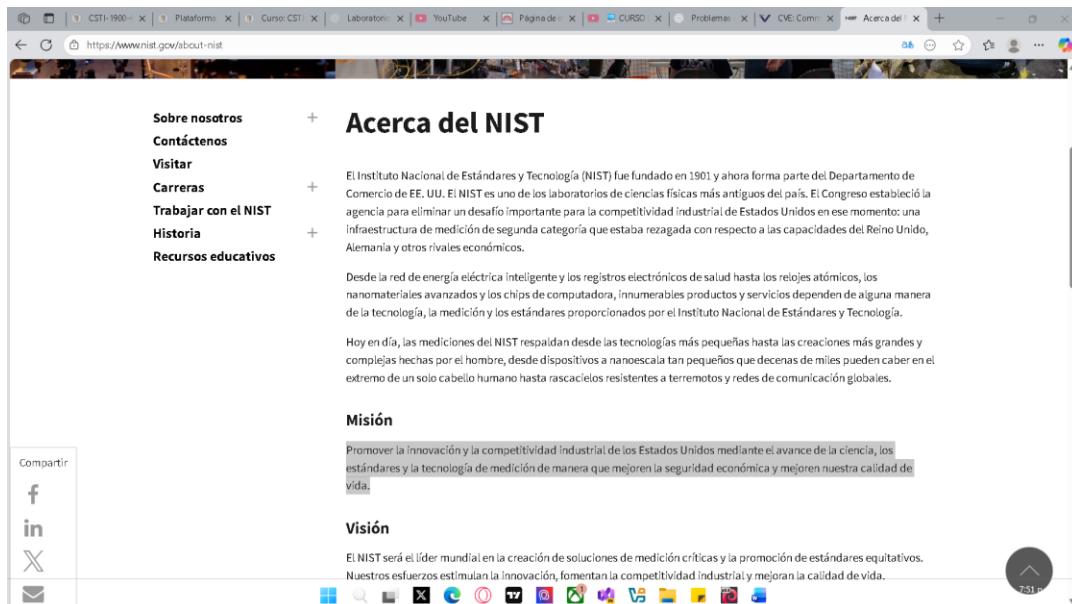
Parte 2: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)

Paso 1: Explore NIST.

- Inicie el sitio web de NIST navegando a <https://www.nist.gov>.
- Seleccione **About NIST > About Us** en el menú y revise la descripción general de NIST.

¿Cuál es la misión de NIST?

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades



The screenshot shows the 'Acerca del NIST' (About NIST) page. On the left, there's a sidebar with links like 'Sobre nosotros', 'Contáctenos', 'Visitar', 'Carreras', 'Trabajar con el NIST', 'Historia', and 'Recursos educativos'. Below this is a 'Compartir' (Share) section with icons for Facebook, LinkedIn, and Email. The main content area has a heading 'Acerca del NIST' and a paragraph about the institute's history and its role in advancing measurement science. It also includes sections for 'Misión' (Mission) and 'Visión' (Vision), both of which emphasize innovation and industrial competitiveness.

“Promover la innovación y la competitividad industrial de los Estados Unidos a través del avance de la ciencia, los estándares y la tecnología para mejorar la seguridad económica y la calidad de vida”.

c. Explore la base de datos nacional de vulnerabilidad (NVD)

- 1) Regrese a la página de inicio de NIST y seleccione **Topics > Information Technology** en el menú.
- 2) Seleccione **National Vulnerability Database** en la lista **Featured Content**.
- 3) Haga clic en **General** para ver y revisar la Información general sobre el NVD.

¿Cuál es la relación entre NVD y CVE?



The screenshot shows the 'General' page of the NVD. It features a sidebar with links for 'General', 'Vulnerabilidades', 'Métricas de vulnerabilidad', 'Productos', 'Desarrolladores', 'Póngase en contacto con NVD', 'Otros sitios', and 'Buscar'. The main content area has three circular icons: one for 'Una breve historia de la NVD' (with a stack of books icon), one for 'CVE y el proceso NVD' (with a maze icon), and one for 'Conteo de CNA y CVE' (with a calculator icon). Below these are sections for 'Información general' and 'Historia'. The 'Información general' section contains text about the NVD's purpose, history, and evolution, mentioning its creation in 1999 and its role as a government repository of vulnerabilities. The 'Historia' section provides a detailed timeline of the NVD's development.

El NVD realiza un escaneo de las CVE publicadas en el diccionario de CVE. El personal de NVD analiza las CVE y proporciona detalles adicionales.

4) Expanda el menú en **General** y haga clic en **NVD Dashboard**.

¿Cuántas vulnerabilidades de CVE contiene el NVD?

Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

The screenshot shows the NVD homepage. On the left, there's a sidebar with links like 'Metrics de vulnerabilidad', 'Productos', 'Desarrolladores', 'Póngase en contacto con NVD', 'Otros sitios', and 'Buscar'. The main content area has two large icons: one of a hand holding a sword-like tool over a shield, and another of a checkmark inside a circle. Below these are sections for 'Descripción de las páginas de detalles de vulnerabilidad' and 'Estados de vulnerabilidad'. A central box defines a vulnerability as 'Una debilidad en la lógica computacional (por ejemplo, el código) que se encuentra en los componentes de software y hardware que, cuando se explota, tiene un impacto negativo en la confidencialidad, integridad o disponibilidad.' It also mentions that mitigations involve changes to the specification or protocols. At the bottom, it notes the page was created on September 20, 2022, and last updated on August 3, 2023.

La respuesta varía. En el momento de escribir este curso: 211116

¿Cuál es la vulnerabilidad puntuada más reciente y cuál es la calificación CVSS?

The screenshot shows the NVD search results page. The search bar at the top contains the URL 'https://nvd.nist.gov/vuln/search#/nvd/home?resultType=records'. Below the search bar, there's a green button labeled 'VULNERABILIDADES'. The main title is 'Búsqueda de vulnerabilidades de NVD'. There are several buttons: 'Avanzado', 'Restablecer', and 'Mostrar estadísticas'. A search input field contains the placeholder 'Para una búsqueda de frases, use " "'. Below the search area, there's a pagination section with 'Artículos por página: 25' and a page number '1-25 de 316560'. The main content area displays a table of vulnerabilities:

Identificador	Información de CISA Kev	Fecha de publicación	CNA	Descripción
CVE-2025-9999	●	2025-09-05	arcinfo	Algunos elementos de carga útil de los mensajes enviados entre dos estaciones en una arquitectura de red no se verifican correctamente en la estación receptora, lo que permite a un atacante ejecutar comandos no autorizados en la aplicación.
CVE-2025-9998	●	2025-09-05	arcinfo	La secuencia de paquetes recibidos por un servidor de red no se comprueba correctamente. Un atacante podría aprovechar esta vulnerabilidad para enviar mensajes especialmente diseñados para forzar la detención de la aplicación.
CVE-2025-9997	●	2025-09-09	Schneider Electric SE	CWE-78: Existe una vulnerabilidad de neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo ('OS Command Injection') que podría causar la inyección de comandos en BLMon que se ejecuta en la consola del sistema operativo cuando se encuentra en una sesión SSH.

La respuesta variará, pero al momento de redactar este curso: CVE-2023-20990 con una gravedad CVSS de 4,4 MEDIA

- 5) Vuelva a la página de la base de datos nacional de vulnerabilidades <https://nvd.nist.gov/>.
- 6) Haga clic en **Vulnerability Metrics** en el menú a la izquierda de la página.

¿Qué método se utiliza para medir cualitativamente la gravedad de las vulnerabilidades?

The screenshot shows the NVD CVSS metrics page at <https://nvd.nist.gov/vuln-metrics/cvss#>. It features three tabs for CVSS v2.0, v3.x, and v4.0. Below the tabs is a section titled "Calificaciones cualitativas de gravedad" (Qualitative severity scales) with tables for each version. A note at the bottom states that NVD uses qualitative severity scales "Baja", "Media", and "Alta" for CVSS v2.0, while CVSS v3.x and v4.0 use the official ranges defined in their specifications.

Clasificaciones CVSS v2.0	Clasificaciones CVSS v3.x	Clasificaciones CVSS v4.0			
Severidad	Rango de puntuación de gravedad	Severidad	Rango de puntuación de gravedad	Severidad	Rango de puntuación de gravedad
Bajo	0.0-3.9	Bajo	0.0-3.9	Bajo	0.0-3.9
Medio	4.0-6.9	Medio	4.0-6.9	Medio	4.0-6.9
Alto	7.0-10.0	Alto	7.0-8.9	Alto	7.0-8.9
		Criticó	9.0-10.0	Criticó	9.0-10.0

**Nota: La especificación CVSS permite la aplicación de cadenas vectoriales que dan como resultado un 0.0 puntuación de gravedad. Sin embargo, el enriquecimiento NVD no evalúa las cadenas vectoriales CVSS que no tienen impactos. Por la definición de vulnerabilidad del programa CVE, no debe contarse un registro CVE que no afecte a la confidencialidad, integridad o disponibilidad.*

Información CVSS específica de NVD

Datos incompletos

Sistema de puntuación de vulnerabilidades comunes (CVSS)

¿Cuántas clasificaciones de gravedad tiene CVSS v3.0 y cuáles son?

The screenshot shows the NVD CVSS metrics page at <https://nvd.nist.gov/vuln-metrics/cvss#>. It features three tabs for CVSS v2.0, v3.x, and v4.0. Below the tabs is a section titled "Calificaciones cualitativas de gravedad" (Qualitative severity scales) with tables for each version. A note at the bottom states that NVD uses qualitative severity scales "Baja", "Media", and "Alta" for CVSS v2.0, while CVSS v3.x and v4.0 use the official ranges defined in their specifications.

Clasificaciones CVSS v2.0	Clasificaciones CVSS v3.x	Clasificaciones CVSS v4.0			
Severidad	Rango de puntuación de gravedad	Severidad	Rango de puntuación de gravedad	Severidad	Rango de puntuación de gravedad
Bajo	0.0-3.9	Bajo	0.0-3.9	Bajo	0.0-3.9
Medio	4.0-6.9	Medio	4.0-6.9	Medio	4.0-6.9
Alto	7.0-10.0	Alto	7.0-8.9	Alto	7.0-8.9
		Criticó	9.0-10.0	Criticó	9.0-10.0

**Nota: La especificación CVSS permite la aplicación de cadenas vectoriales que dan como resultado un 0.0 puntuación de gravedad. Sin embargo, el enriquecimiento NVD no evalúa las cadenas vectoriales CVSS que no tienen impactos. Por la definición de vulnerabilidad del programa CVE, no debe contarse un registro CVE que no afecte a la confidencialidad, integridad o disponibilidad.*

Información CVSS específica de NVD

Datos incompletos

Cinco. Son: Ninguna, Baja, Media, Alta y Crítica.

Reflexión

¿Cuál es la relación entre CVE, CWE, NVD y CVSS?

CVE identifica las vulnerabilidades,
CWE clasifica la causa o tipo de debilidad,
NVD amplía la información de las CVE con detalles y análisis,
y CVSS mide la gravedad de cada vulnerabilidad.

CVE enumera las vulnerabilidades que se han descubierto, CWE las clasifica, NVD proporciona detalles y CVSS proporciona calificaciones de gravedad.