

CURSO *ONLINE* DE CIBERSEGURIDAD__

Taller 3

Unidad 3. Aspectos avanzados de ciberseguridad



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 **incibe**_

INSTITUTO NACIONAL DE CIBERSEGURIDAD



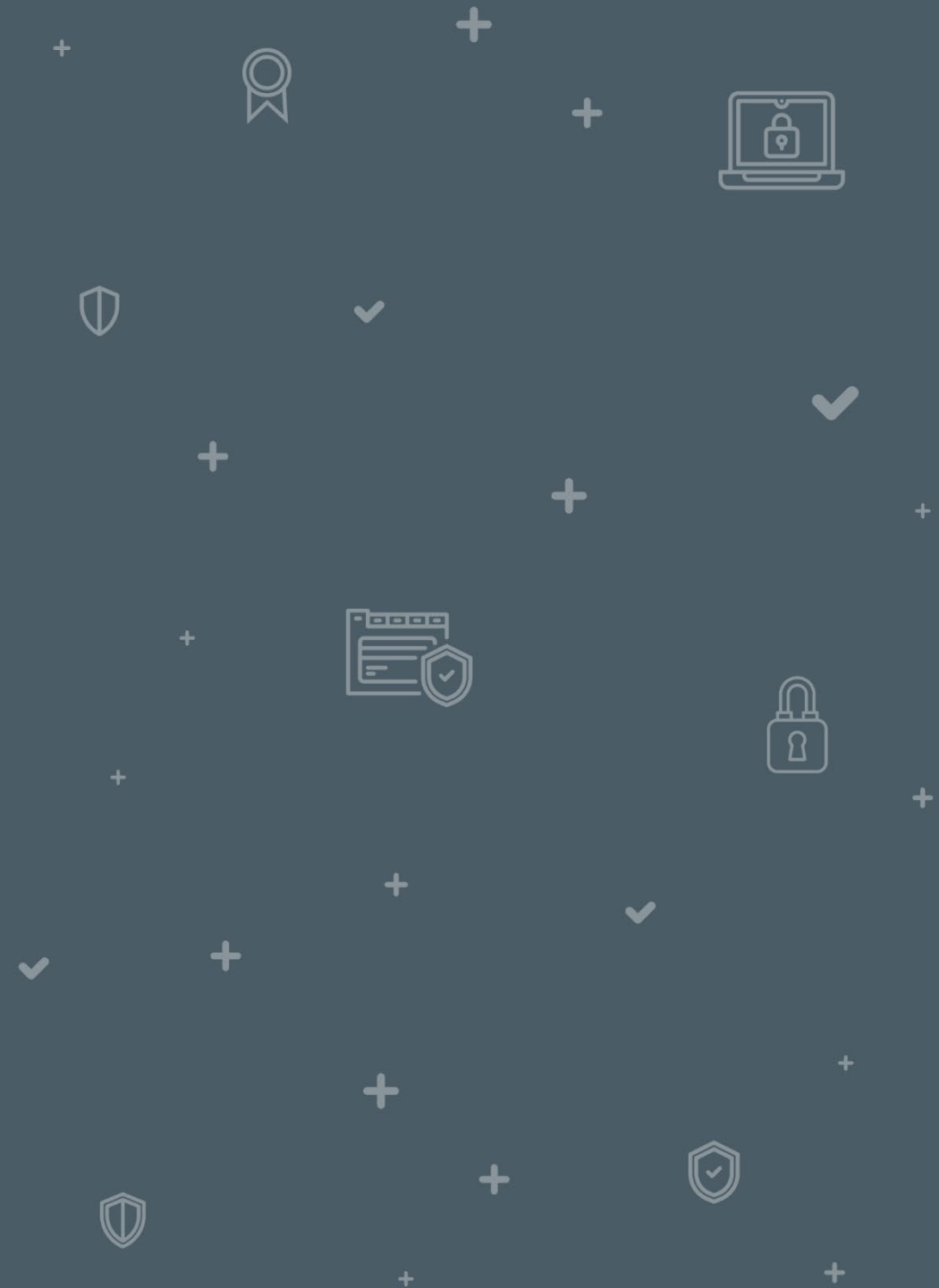
Contenidos

1	EL ANÁLISIS DE VULNERABILIDADES	3
2	INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS	5
3	ENUNCIADO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD	29
4	SOLUCIONARIO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD	31

Duración total del taller: 20 minutos.

EL ANÁLISIS DE VULNERABILIDADES

1

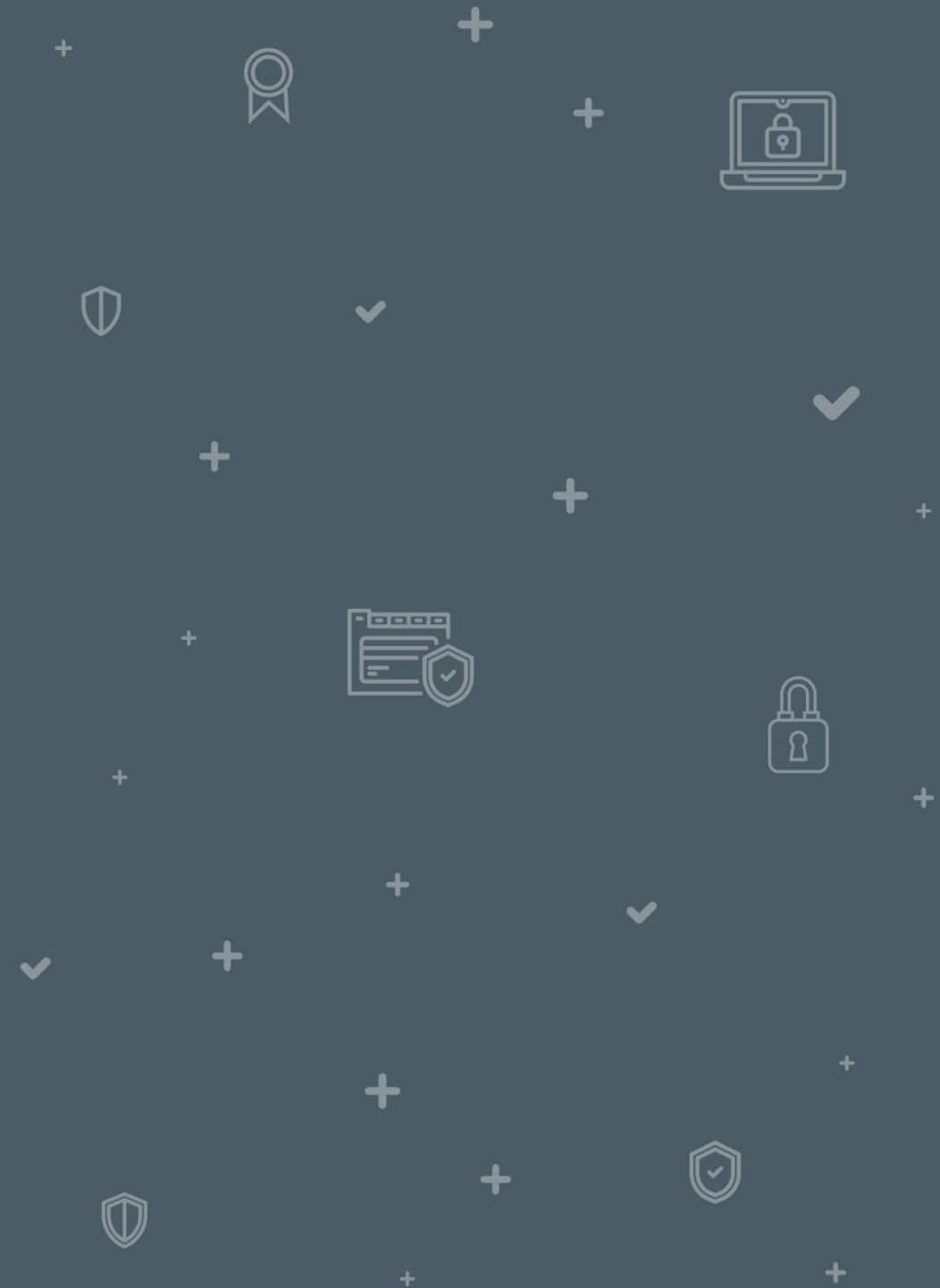


EL ANÁLISIS DE VULNERABILIDADES

En este ejercicio práctico, vas a aprender a instalar la herramienta OpenVas en la máquina virtual Kali Linux. Además, vas a conocer cómo actualizar las CVEs o vulnerabilidades y las NVT de OpenVas (*Network vulnerability test* o, dicho de otra manera, la base de datos de las pruebas realizadas por OpenVas para descubrir vulnerabilidades). Para ello, crearás la tarea de escaneo y, finalmente, interpretarás los resultados del análisis de una determinada vulnerabilidad, de la que investigarás su impacto.

INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

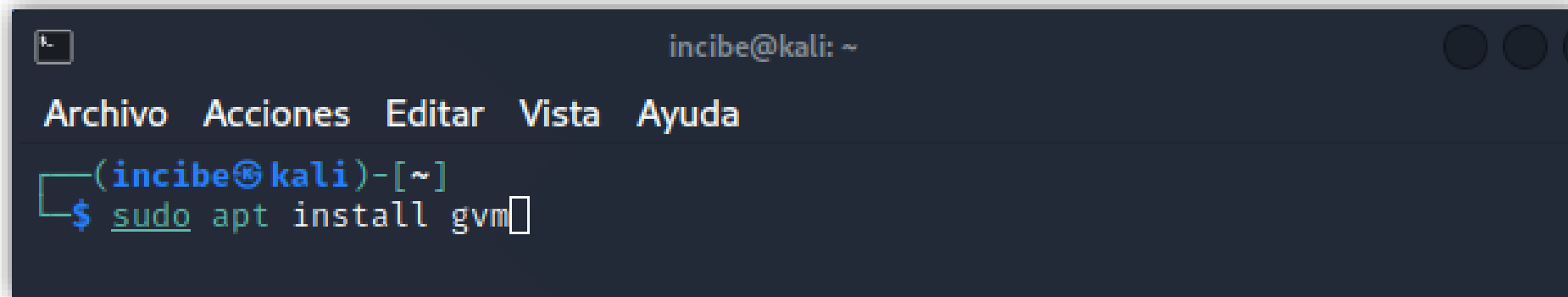
2



2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

Instala OpenVAS en tu máquina virtual Kali Linux. Además, crea tu usuario y contraseña y actualiza las vulnerabilidades (CVEs) y las pruebas de vulnerabilidades de red (NVTs).

- Abre una terminal en Kali Linux e introduce el comando «**sudo apt install gvm**».

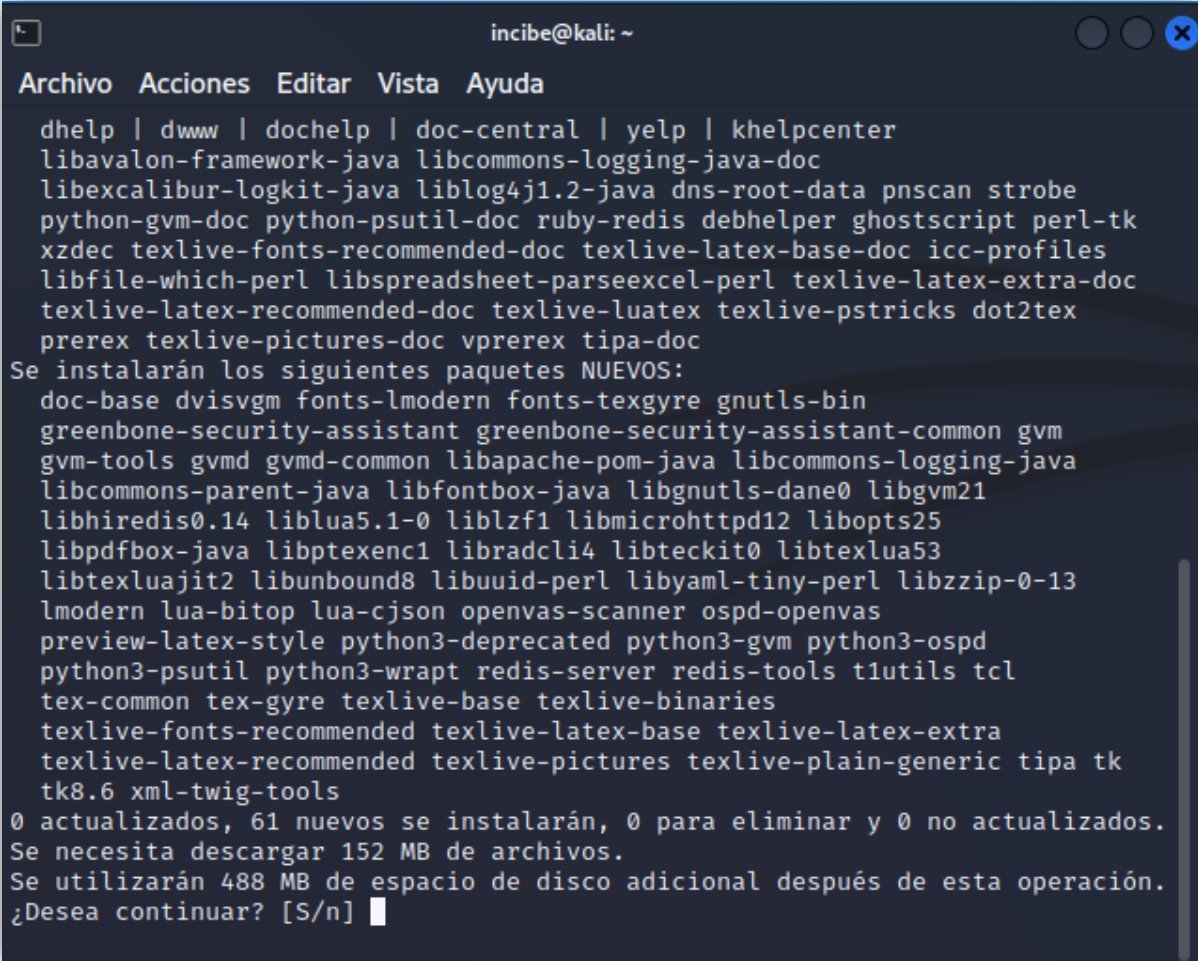


```
incibe@kali: ~  
Archivo Acciones Editar Vista Ayuda  
(incibe@kali)-[~]  
$ sudo apt install gvm
```

Ilustración 1: Comando «sudo apt install gvm».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- A continuación, observaremos una pregunta en la última línea de código de la siguiente imagen. Haz clic en «Enter» para confirmar o pulsa la letra S y selecciona «Enter».



```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
dhhelp | dwww | dochelp | doc-central | yelp | khelpcenter
libavalon-framework-java libcommons-logging-java-doc
libexcalibur-logkit-java liblog4j1.2-java dns-root-data pnsnscan strobe
python-gvm-doc python-psutil-doc ruby-redis debhelper ghostscript perl-tk
xzdec texlive-fonts-recommended-doc texlive-latex-base-doc icc-profiles
libfile-which-perl libspreadsheet-parseexcel-perl texlive-latex-extra-doc
texlive-latex-recommended-doc texlive-luatex texlive-pstricks dot2tex
prerex texlive-pictures-doc vprerex tipa-doc
Se instalarán los siguientes paquetes NUEVOS:
doc-base dvisvgm fonts-lmodern fonts-texgyre gnutls-bin
greenbone-security-assistant greenbone-security-assistant-common gvm
gvm-tools gvmd gvmd-common libapache-pom-java libcommons-logging-java
libcommons-parent-java libfontbox-java libgnutls-dane0 libgvm21
libhiredis0.14 liblua5.1-0 liblzf1 libmicrohttpd12 libopts25
libpdfbox-java libptexenc1 libradcli4 libteckit0 libtexlua53
libtexluajit2 libunbound8 libuuid-perl libyaml-tiny-perl libzip-0-13
lmodern lua-bitop lua-cjson openvas-scanner ospd-openvas
preview-latex-style python3-deprecated python3-gvm python3-ospd
python3-psutil python3-wrapt redis-server redis-tools t1utils tcl
tex-common tex-gyre texlive-base texlive-binaries
texlive-fonts-recommended texlive-latex-base texlive-latex-extra
texlive-latex-recommended texlive-pictures texlive-plain-generic tipa tk
tk8.6 xml-twig-tools
0 actualizados, 61 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 152 MB de archivos.
Se utilizarán 488 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ilustración 2: Última línea de código que indica ¿Desea continuar? Sí/No.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Ahora, introduce el comando «**sudo gvm-setup**».

```
Running mktexlsr /var/lib/texmf ... done.  
Building format(s) --all.  
This may take some time ... done.  
  
(incibe@kali)-[~]  
$ sudo gvm-setup
```

```
Archivo Acciones Editar Vista Ayuda  
tl-paper: setting paper size for dvipdfmx to a4: /var/lib/texmf/dvipdfmx/dvipdfmx-paper.cfg  
tl-paper: setting paper size for xdvi to a4: /var/lib/texmf/xdvi/XDvi-paper  
tl-paper: setting paper size for pdftex to a4: /var/lib/texmf/tex/generic/tex-ini-files/pdftexconfig.tex  
Configurando tex-gyre (20180621-3.1) ...  
Configurando python3-deprecated (1.2.13-2) ...  
Configurando libhiredis0.14:amd64 (0.14.1-2) ...  
Configurando libgnutls-dane0:amd64 (3.7.2-5) ...  
Configurando libpdfbox-java (1:1.8.16-2) ...  
Configurando doc-base (0.11.1) ...  
Registering 34 doc-base files ...  
Configurando libgvm21:amd64 (21.4.3-1) ...  
Configurando preview-latex-style (12.2-1) ...  
Configurando libcommons-parent-java (43-1) ...  
Configurando texlive-plain-generic (2021.20211217-1) ...  
Configurando libcommons-logging-java (1.2-2) ...  
Configurando texlive-latex-base (2021.20211217-1) ...  
Configurando redis-tools (5:6.0.16-1) ...  
Configurando texlive-latex-recommended (2021.20211217-1) ...  
Configurando texlive-pictures (2021.20211217-1) ...  
Configurando python3-osspd (21.4.4-1) ...  
Configurando lmodern (2.004.5-6.1) ...  
Configurando texlive-fonts-recommended (2021.20211217-1) ...  
Configurando tipa (2:1.3-21) ...  
Configurando gnutls-bin (3.7.2-5) ...  
Configurando gvm-common (21.4.4-1) ...  
Configurando texlive-latex-extra (2021.20211217-1) ...  
Configurando redis-server (5:6.0.16-1) ...  
update-rc.d: We have no instructions for the redis-server init script.  
update-rc.d: It looks like a non-network service, we enable it.  
redis-server.service is a disabled or a static unit not running, not starting it.  
Configurando gvm (21.4.4-1) ...  
Configurando python3-gvm (21.10.0-1) ...  
Configurando greenbone-security-assistant (21.4.3-1) ...  
greenbone-security-assistant.service is a disabled or a static unit not running, not starting it.  
Configurando openvas-scanner (21.4.3-1) ...  
Configurando ospd-openvas (21.4.3-1) ...  
ospd-openvas.service is a disabled or a static unit not running, not starting it.  
Configurando gvm-tools (21.10.0-1) ...  
Configurando gvm (21.4.3) ...  
Procesando disparadores para mailcap (3.70+nmul) ...  
Procesando disparadores para fontconfig (2.13.1-4.2) ...  
Procesando disparadores para kali-menu (2021.4.2) ...  
Procesando disparadores para desktop-file-utils (0.26-1) ...  
Procesando disparadores para libc-bin (2.33-1) ...  
Procesando disparadores para man-db (2.9.4-4) ...  
Procesando disparadores para tex-common (6.17) ...  
Running updmap-sys. This may take some time ... done.  
Running mktexlsr /var/lib/texmf ... done.  
Building format(s) --all.  
This may take some time ... done.  
  
(incibe@kali)-[~]  
$ sudo gvm-setup
```


2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Espera a que finalice la carga. Después, aparecerá la evolución de la descarga en modo texto de la siguiente forma:

```
(incibe@kali)-[~]
$ sudo gvm-setup

[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] Creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE

[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-oss
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '842a23bc-c79d-404f-bc35-081162f359fb'.
[*] Define Feed Import Owner
```

Ilustración 4: Pantalla resultante de la ejecución del comando «sudo gvm-setup».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

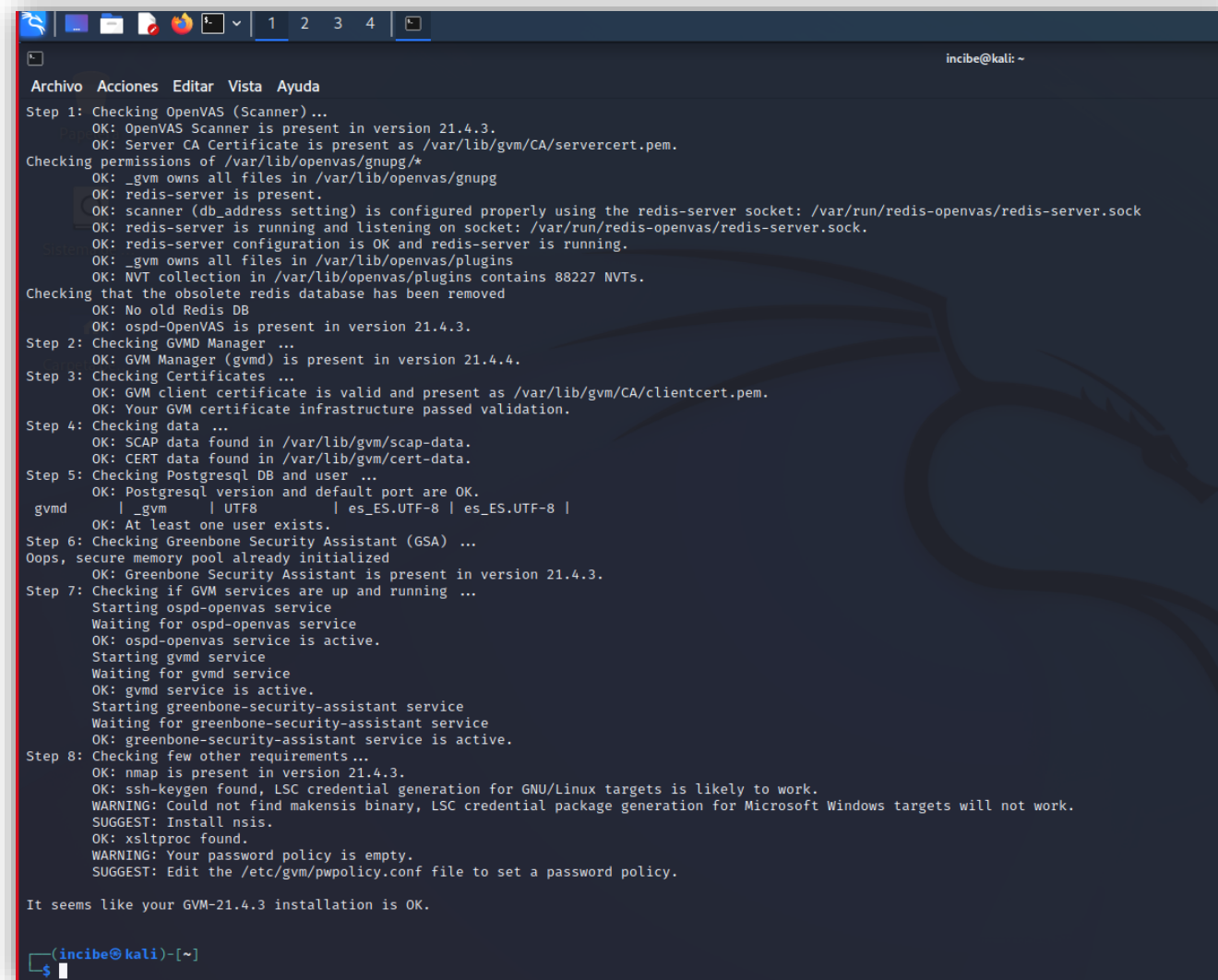
- A continuación, introduce el comando «**sudo gvm-check-setup**».

```
incibe@kali: ~  
[+] GVM feeds updated  
[*] Checking Default scanner  
[*] Modifying Default Scanner  
Scanner modified.  
[+] Done  
[*] Please note the password for the admin user  
[*] User created with password '842a23bc-c79d-404f-bc35-081162f359fb'.  
[>] You can now run gvm-check-setup to make sure everything is correctly configured  
  
(incibe@kali)-[~]  
$ sudo gvm-check-setup  
gvm-check-setup 21.4.3  
Test completeness and readiness of GVM-21.4.3  
Step 1: Checking OpenVAS (Scanner) ...  
OK: OpenVAS Scanner is present in version 21.4.3.  
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.  
Checking permissions of /var/lib/openvas/gnupg/*  
OK: _gvm owns all files in /var/lib/openvas/gnupg/*  
OK: redis-server is present.  
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock  
OK: redis-server is running and listening on socket: /var/run/redis-openvas/redis-server.sock.  
OK: redis-server configuration is OK and redis-server is running.  
OK: _gvm owns all files in /var/lib/openvas/plugins  
OK: NVT collection in /var/lib/openvas/plugins contains 88227 NVTs.  
Checking that the obsolete redis database has been removed  
OK: No old Redis DB  
OK: osdp-OpenVAS is present in version 21.4.3.  
Step 2: Checking GVM Manager ...  
OK: GVM Manager (gvm) is present in version 21.4.4.  
Step 3: Checking Certificates ...  
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.  
OK: Your GVM certificate infrastructure passed validation.  
Step 4: Checking data ...  
OK: SCAP data found in /var/lib/gvm/scap-data.  
OK: CERT data found in /var/lib/gvm/cert-data.  
Step 5: Checking PostgreSQL DB and user ...  
OK: PostgreSQL version and default port are OK.  
gvm | _gvm | UTF8 | es_ES.UTF-8 | es_ES.UTF-8 |  
OK: At least one user exists.  
Step 6: Checking Greenbone Security Assistant (GSA) ...  
Oops, secure memory pool already initialized  
OK: Greenbone Security Assistant is present in version 21.4.3.  
Step 7: Checking if GVM services are up and running ...  
Starting osdp-openvas service  
Waiting for osdp-openvas service  
OK: osdp-openvas service is active.  
Starting gvm service  
Waiting for gvm service
```

```
[>] You can now run gvm-check-setup to make sure everything is correctly c  
  
(incibe@kali)-[~]  
$ sudo gvm-check-setup  
[sudo] password for incibe:  
gvm-check-setup 21.4.3  
Test completeness and readiness of GVM-21.4.3  
Step 1: Checking OpenVAS (Scanner) ...  
OK: OpenVAS Scanner is present in version 21.4.3.  
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert  
Checking permissions of /var/lib/openvas/gnupg/*
```

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- La carga se habrá realizado correctamente.



```
incibe@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Step 1: Checking OpenVAS (Scanner)...  
OK: OpenVAS Scanner is present in version 21.4.3.  
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.  
Checking permissions of /var/lib/openvas/gnupg/*  
OK: _gvm owns all files in /var/lib/openvas/gnupg  
OK: redis-server is present.  
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock  
OK: redis-server is running and listening on socket: /var/run/redis-openvas/redis-server.sock.  
OK: redis-server configuration is OK and redis-server is running.  
OK: _gvm owns all files in /var/lib/openvas/plugins  
OK: NVT collection in /var/lib/openvas/plugins contains 88227 NVTs.  
Checking that the obsolete redis database has been removed  
OK: No old Redis DB  
OK: ospd-OpenVAS is present in version 21.4.3.  
Step 2: Checking GVM Manager ...  
OK: GVM Manager (gvm) is present in version 21.4.4.  
Step 3: Checking Certificates ...  
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.  
OK: Your GVM certificate infrastructure passed validation.  
Step 4: Checking data ...  
OK: SCAP data found in /var/lib/gvm/scap-data.  
OK: CERT data found in /var/lib/gvm/cert-data.  
Step 5: Checking PostgreSQL DB and user ...  
OK: PostgreSQL version and default port are OK.  
gvm | _gvm | UTF8 | es_ES.UTF-8 | es_ES.UTF-8 |  
OK: At least one user exists.  
Step 6: Checking Greenbone Security Assistant (GSA) ...  
Oops, secure memory pool already initialized  
OK: Greenbone Security Assistant is present in version 21.4.3.  
Step 7: Checking if GVM services are up and running ...  
Starting ospd-openvas service  
Waiting for ospd-openvas service  
OK: ospd-openvas service is active.  
Starting gvm service  
Waiting for gvm service  
OK: gvm service is active.  
Starting greenbone-security-assistant service  
Waiting for greenbone-security-assistant service  
OK: greenbone-security-assistant service is active.  
Step 8: Checking few other requirements ...  
OK: nmap is present in version 21.4.3.  
OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.  
WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work.  
SUGGEST: Install nsis.  
OK: xsltproc found.  
WARNING: Your password policy is empty.  
SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.  
  
It seems like your GVM-21.4.3 installation is OK.  
  
(incibe@kali)~  
$
```

Ilustración 6: Pantalla resultante de la ejecución del comando «sudo gvm-check-setup».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

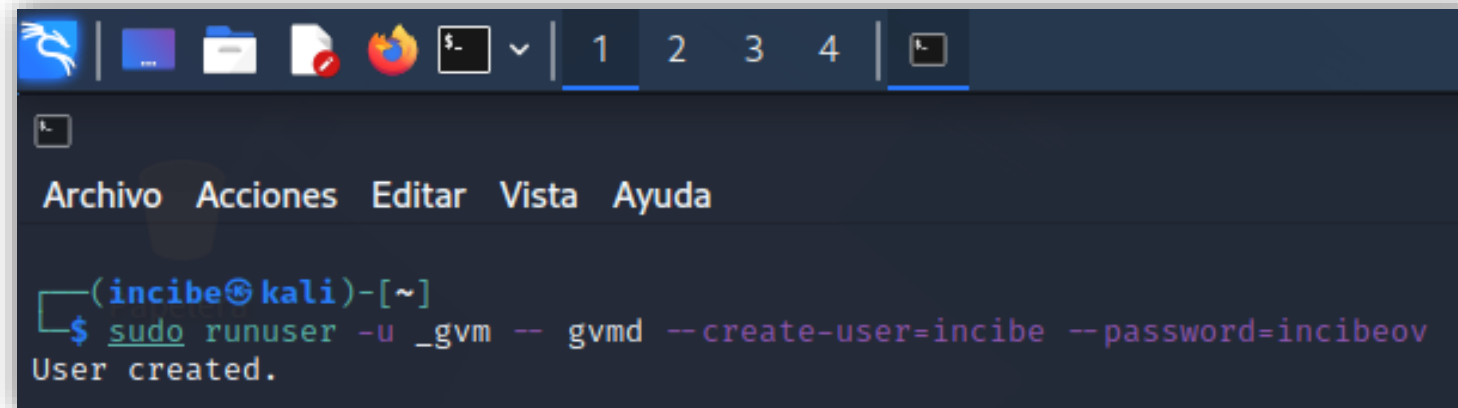
- A continuación, introduce el comando «**sudo gvm-start**» para iniciar el servicio.

```
(incibe@kali)-[~]  
$ sudo gvm-start  
[i] GVM services are already running  
  
(incibe@kali)-[~]  
$
```

Ilustración 7: Comando «sudo gvm-start».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Una vez iniciado, escribe el comando «**sudo runuser -u _gvm -- gvm --create-user=incibe --password=incibeov**». Las opciones «**--create-user=**» y «**--password=**» son para crear un usuario en este programa, por lo que los textos que hemos puesto de «incibe» e «incibeov» son los datos de usuario que nosotros hemos generado, pero tú puedes poner los que elijas.



```
(incibe@kali)-[~]  
$ sudo runuser -u _gvm -- gvm --create-user=incibe --password=incibeov  
User created.
```

Ilustración 8: Comando «sudo runuser -u _gvm -- gvm --create-user=incibe --password=incibeov».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Cuando hagas clic en «Enter» al crear tu usuario y contraseña, la terminal mostrará un aviso de redirección automática a una página web del navegador.

```
-openvas.log --lock-file-dir /var/lib/openvas
15812 /usr/bin/python3 /usr/bin/osspd-openvas --config /etc/gvm/osspd-openvas.conf --log-confi
-openvas.log --lock-file-dir /var/lib/openvas

feb 01 13:43:23 kali systemd[1]: Starting OSPd Wrapper for the OpenVAS Scanner (osspd-openvas)...
feb 01 13:43:23 kali systemd[1]: Started OSPd Wrapper for the OpenVAS Scanner (osspd-openvas).

[>] Opening Web UI (https://127.0.0.1:9392) in: 5 ... 4 ... 3 ... 2 ... 1 ...

(incibe@kali)~$
```

```
Archivo Acciones Editar Vista Ayuda
CPU: 11ms
CGroup: /system.slice/greenbone-security-assistant.service
├─15872 /usr/bin/gsad --listen=127.0.0.1 --port=9392
└─15873 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

feb 01 13:43:29 kali systemd[1]: Starting Greenbone Security Assistant (gsad)...
feb 01 13:43:29 kali gsad[15871]: Oops, secure memory pool already initialized
feb 01 13:43:29 kali systemd[1]: Started Greenbone Security Assistant (gsad).

* gvm.service - Greenbone Vulnerability Manager daemon (gvm)
Loaded: loaded (/lib/systemd/system/gvm.service; disabled; vendor preset: disabled)
Active: active (running) since Tue 2022-02-01 13:43:24 CET; 5s ago
Docs: man:gvm(8)
Process: 15811 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/osspd/osspd.sock --listen-group=gvm (code=exited, status=0/SUCCESS)
Main PID: 15816 (gvmd)
Tasks: 4 (limit: 4613)
Memory: 764.6M
CGroup: /system.slice/gvm.service
├─15816 "gvmd: Waiting for incoming connections"
├─15848 "gvmd: Syncing SCAP: Updating CVEs"
├─15851 sh -c "xsl_split -s40MB split.xml 66 head -n 2 split-00.xml > head.xml 66 echo "/>] Opening Web UI (https://127.0.0.1:9392) in: 5 ... 4 ... 3 ... 2 ... 1 ...

(incibe@kali)~$
```

Ilustración 9: Pantalla resultante de la ejecución de «Enter».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- En el navegador aparecerá el siguiente aviso debido a que el certificado SSL de la página está caducado. No obstante, como es una página de confianza ejecutada por nosotros mismos, nos lo saltaremos. Haz clic en «Advanced» («Avanzado»).

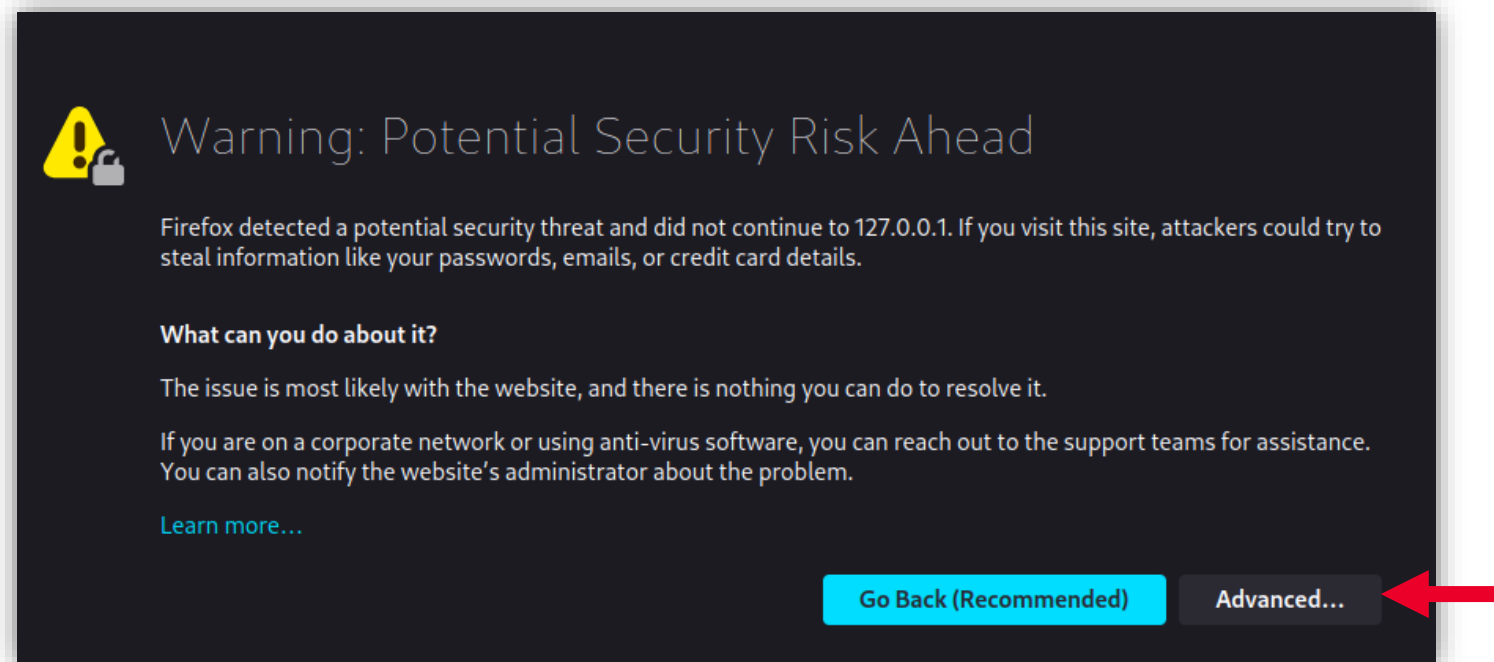
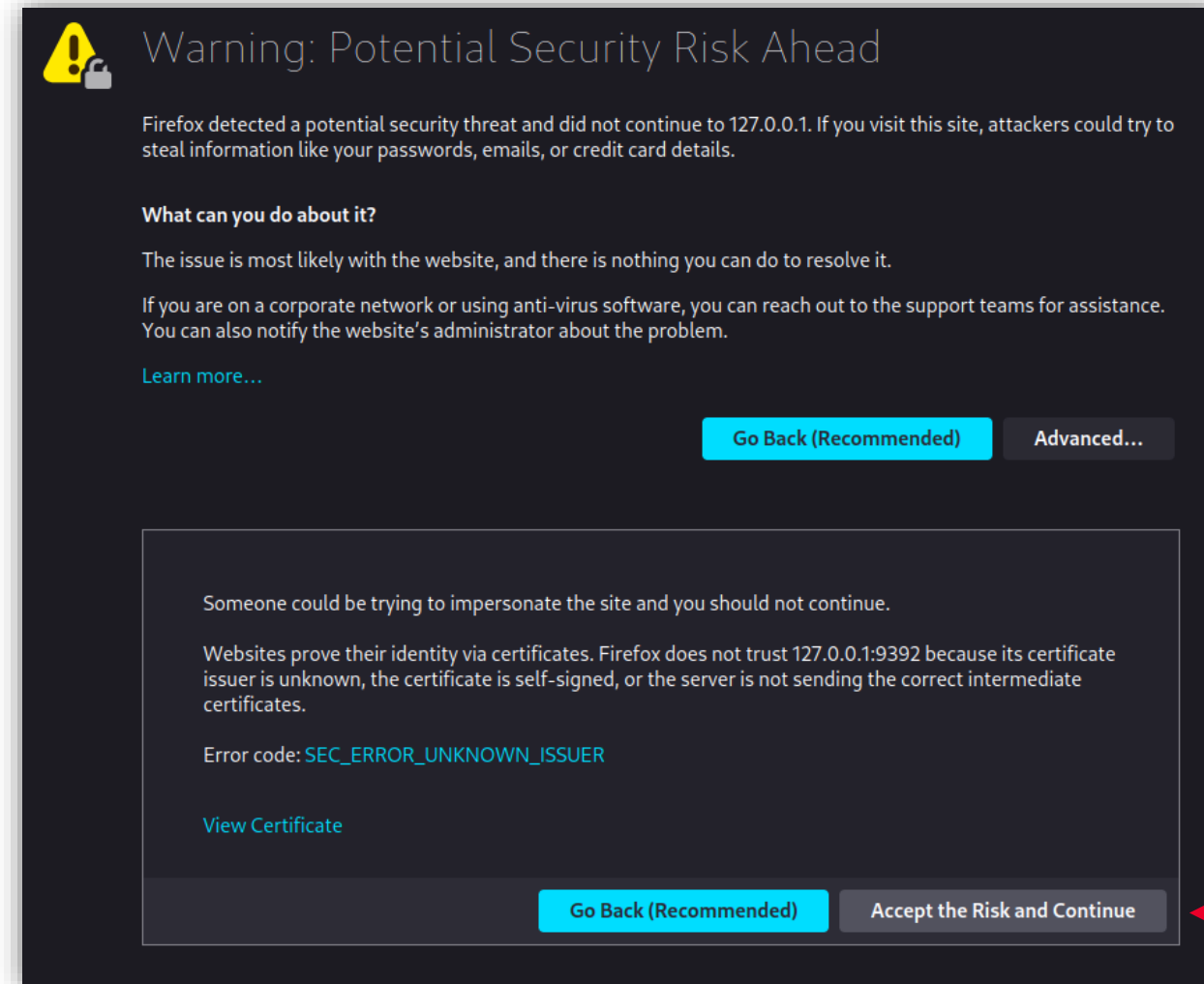


Ilustración 10: Ventana emergente que indica «Riesgo potencialmente peligroso».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Haz clic en «*Accept the risk and continue*» o «Aceptar el riesgo y continuar».

Ilustración 11: Ventana emergente que indica «Aceptar el riesgo y continuar».



2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- A continuación, aparecerá la página de inicio de Greenbone, propietaria de OpenVAS. Deberás introducir el usuario y contraseña que hayas creado previamente. En nuestro caso, «usuario: INCIBE» y «contraseña: incibeov».

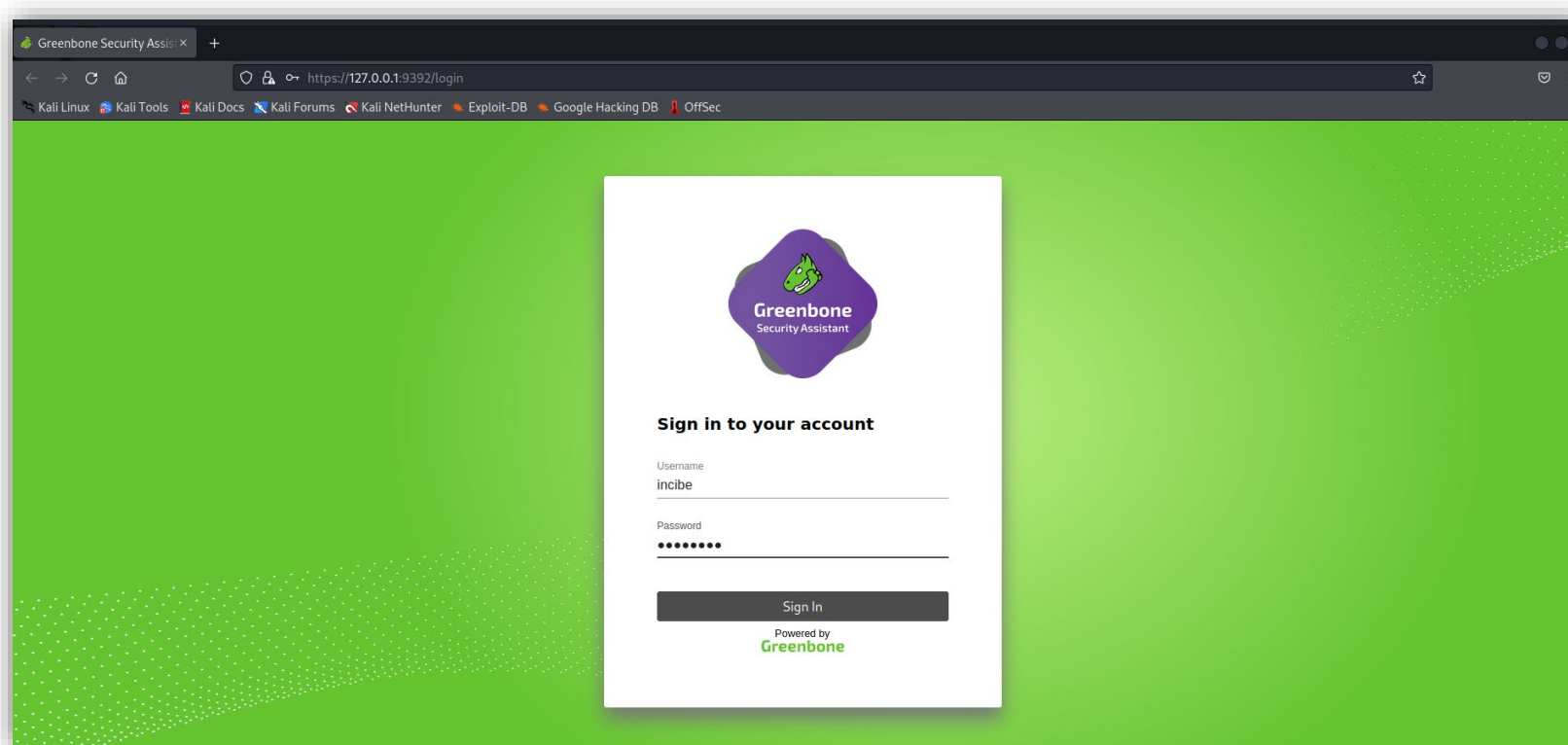


Ilustración 12: Página de inicio de Greenbone.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Esta es la página de inicio de OpenVAS.

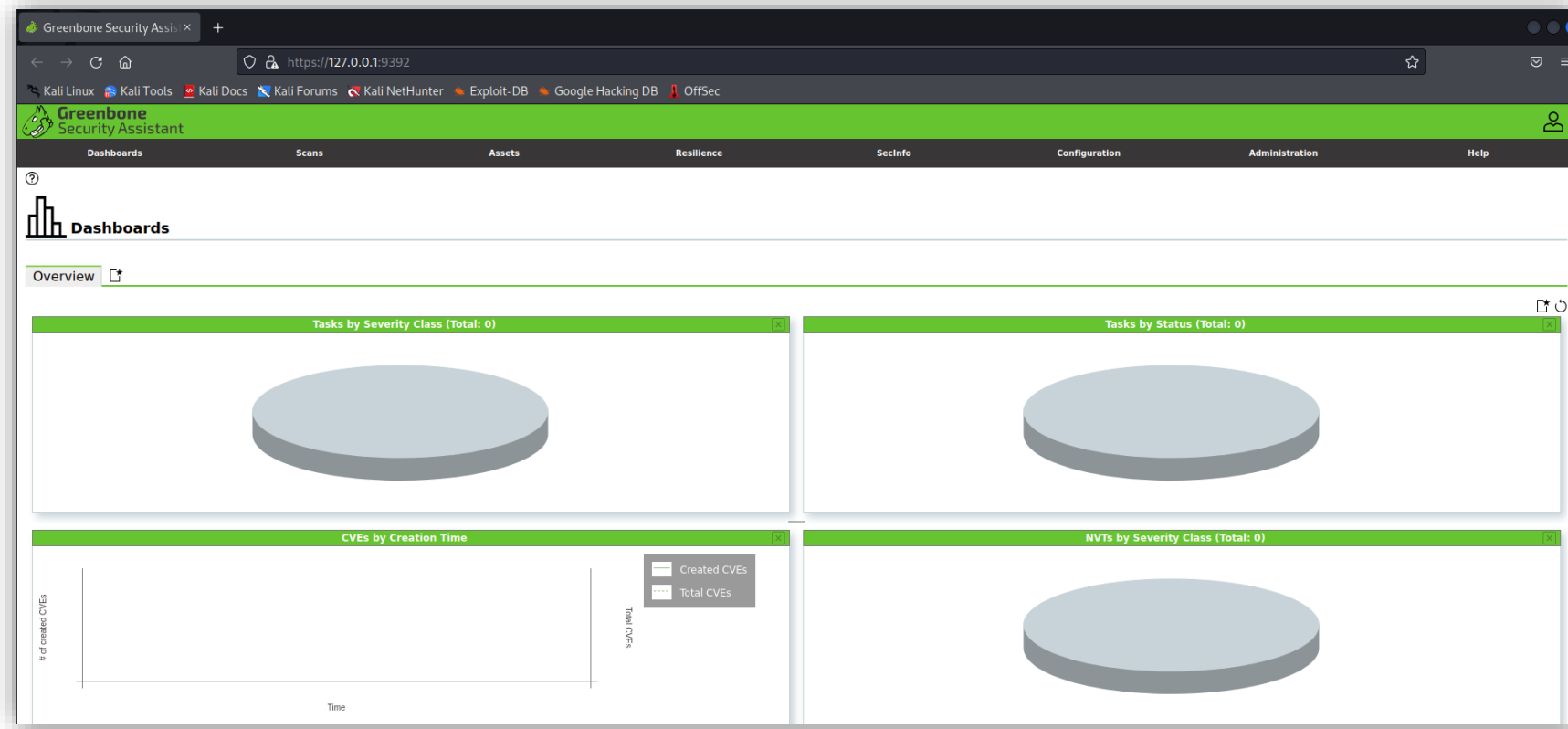


Ilustración 13: Página de inicio de OpenVAS.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- A continuación, regresa al terminal de comandos de Kali Linux y actualiza el servicio «**gym**» con el comando «**sudo gvm-feed-update**» para actualizar tanto las vulnerabilidades (CVEs) como las pruebas de vulnerabilidades de red (NVT) de openVAS.

```
(incibe@kali)~$ sudo gvm-feed-update
[*] Updating GVM feeds
[*] Updating NVT (Network Vulnerability Tests feed from Greenbone Security Feed/Community Feed)
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.

receiving incremental file list
█
```

Ilustración 14: Comando «sudo gvm-feed-update».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Vuelve de nuevo al navegador Firefox donde está la página de OpenVAS local. En ella puedes visualizar tanto las vulnerabilidades (CVEs) como las pruebas de vulnerabilidades de red (NVT).

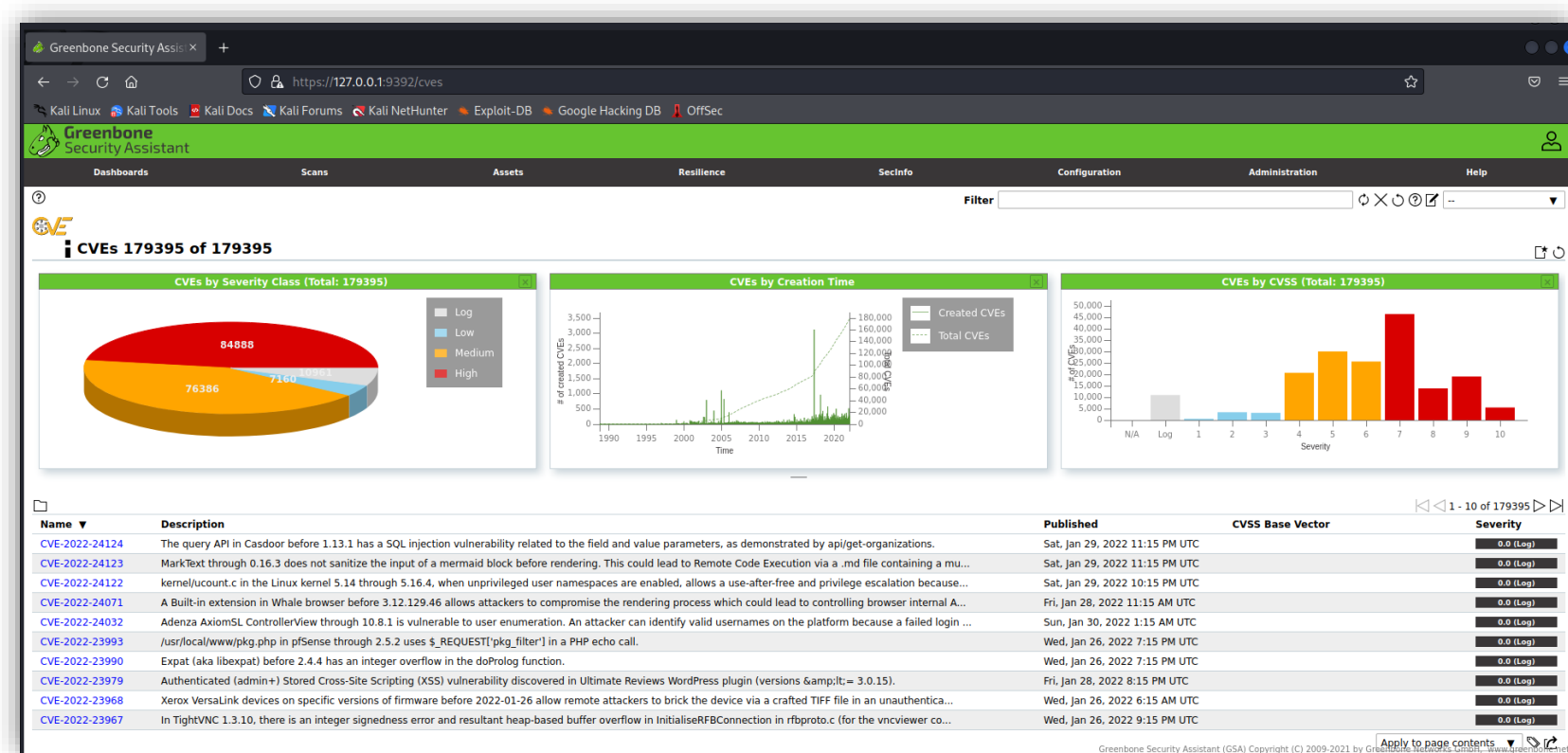


Ilustración 15: Vulnerabilidades (CVEs) que muestra OpenVAS.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

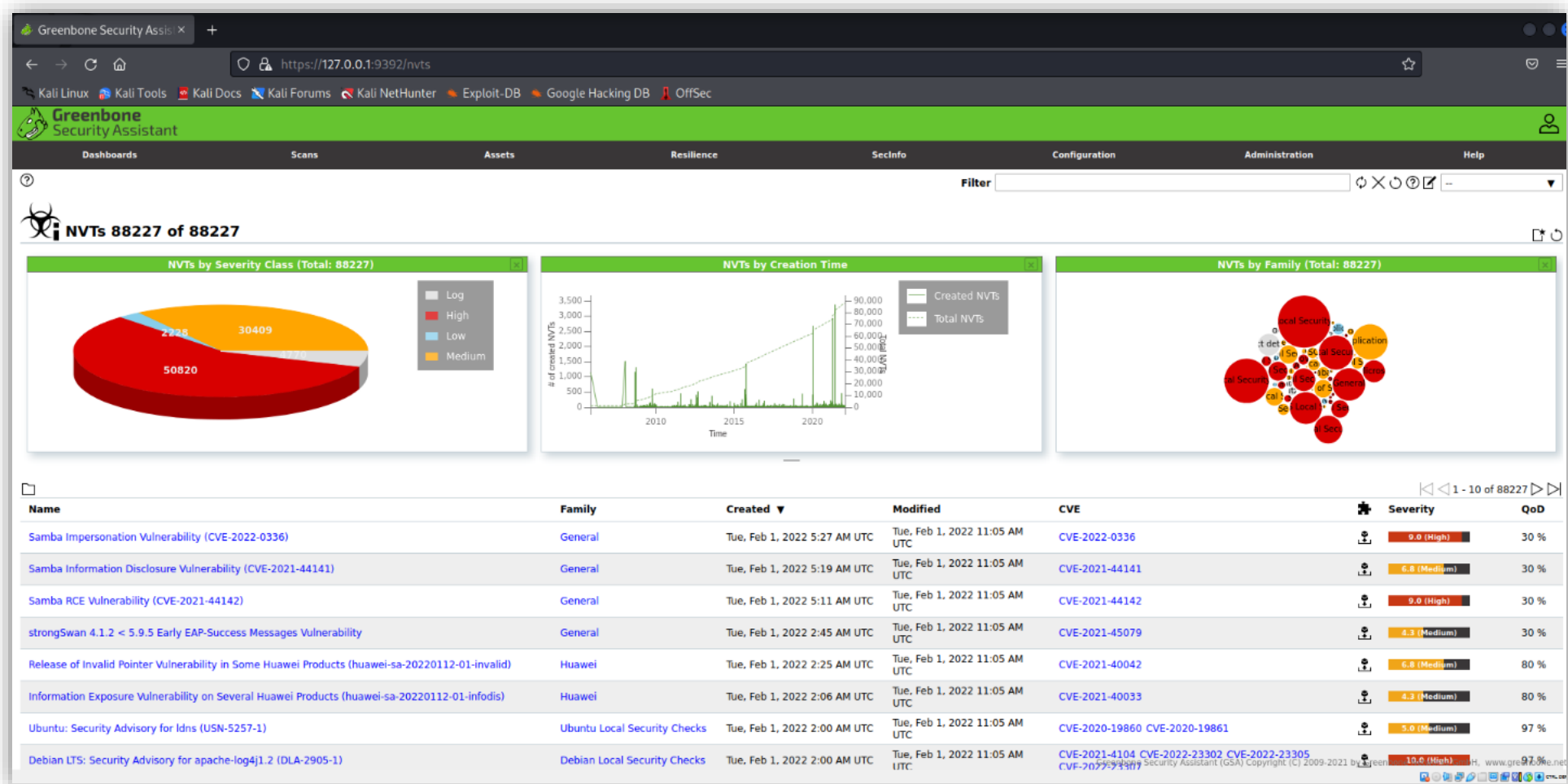
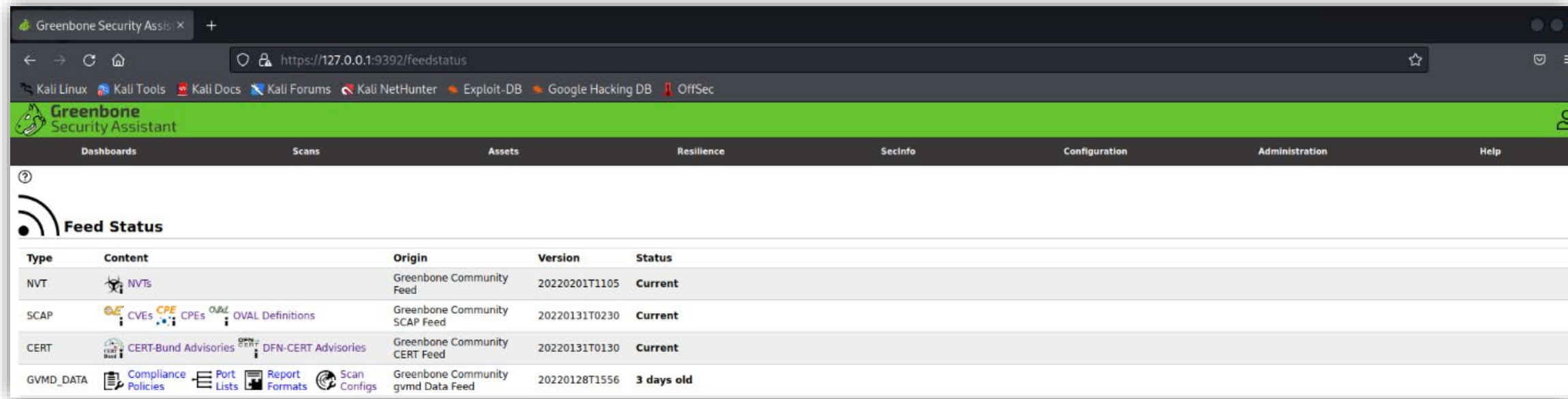


Ilustración 16: Vulnerabilidades de red (NVT) que muestra OpenVAS.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS



Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20220201T1105	Current
SCAP	CVEs CPEs OVAL Definitions	Greenbone Community SCAP Feed	20220131T0230	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20220131T0130	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20220128T1556	3 days old

Ilustración 17: Estado de las principales bases de datos de OpenVAS.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Ahora, crea una nueva tarea de escaneo. Para ello, dentro de la ventana «Scans», selecciona «Task».

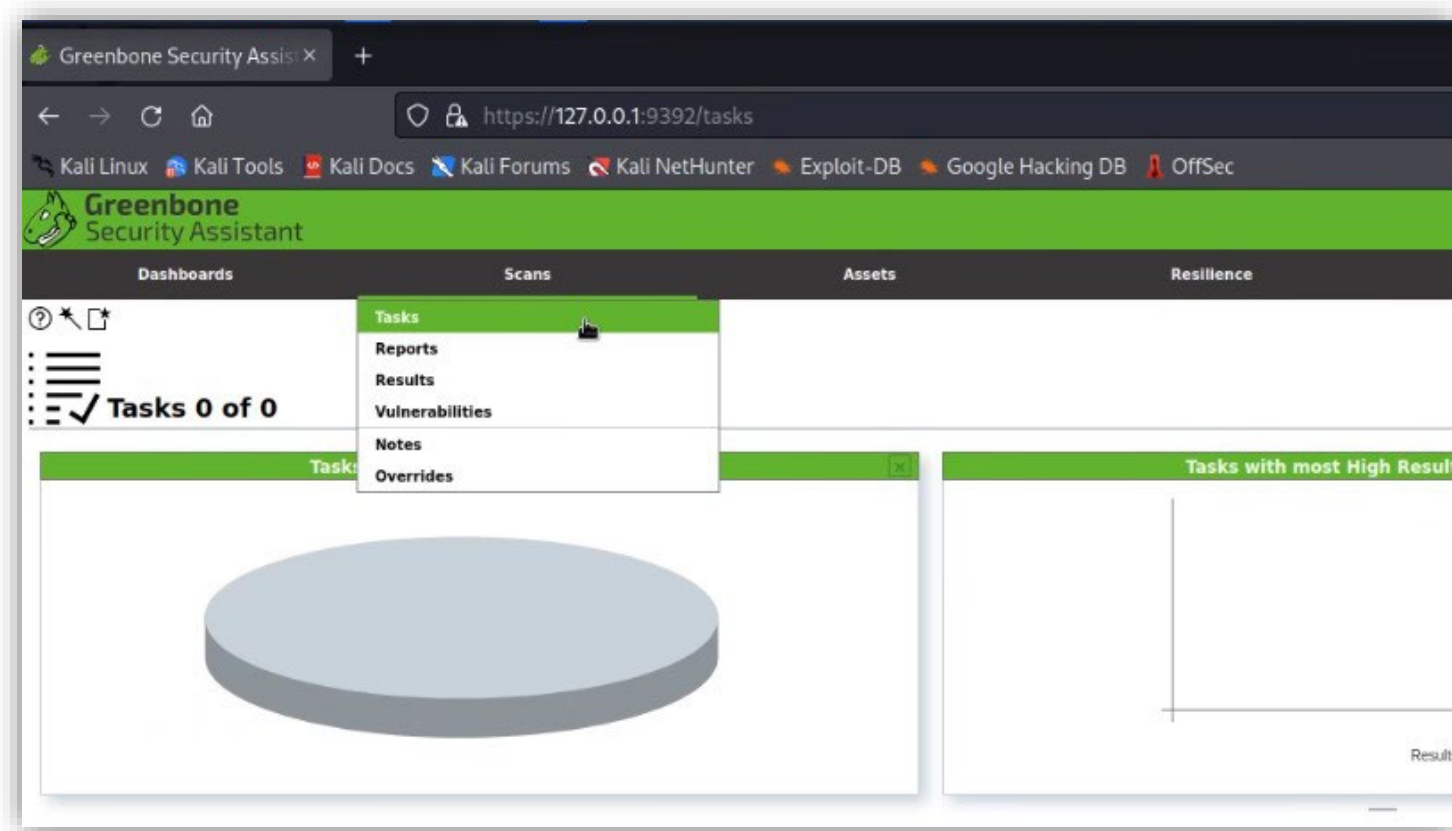


Ilustración 18: Creación de una nueva tarea de escaneo.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Después, en el símbolo de la varita mágica, selecciona «Task Wizard».

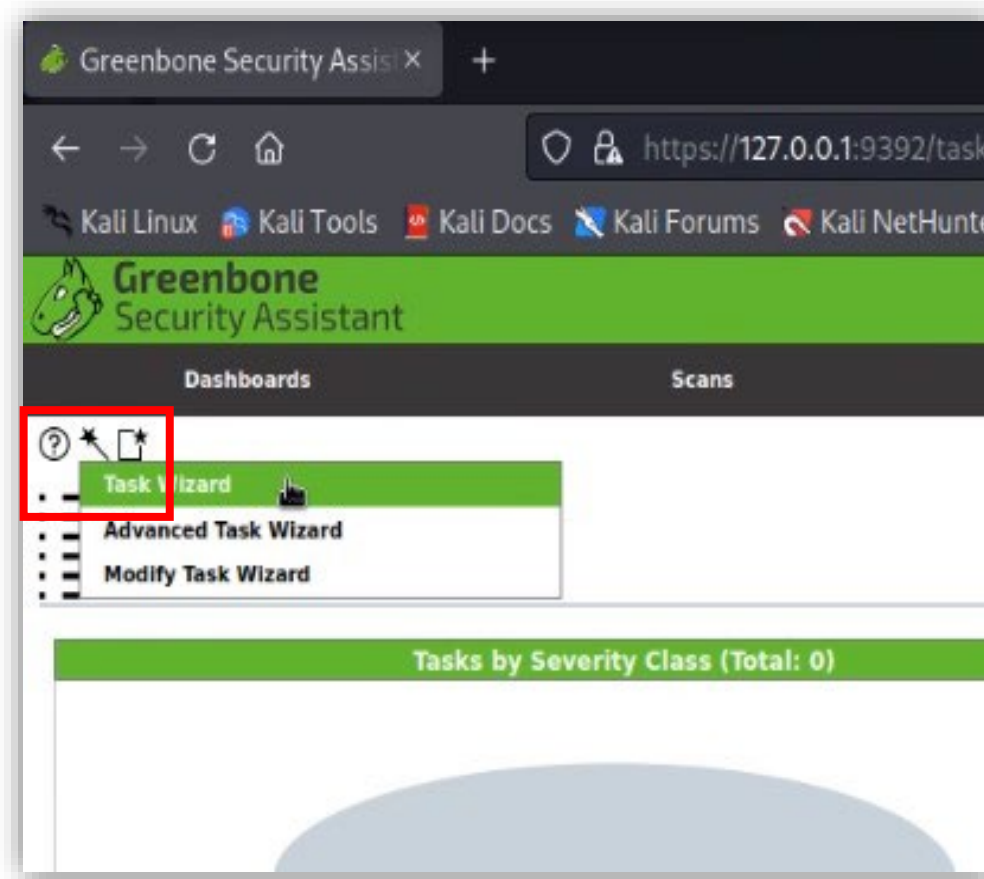
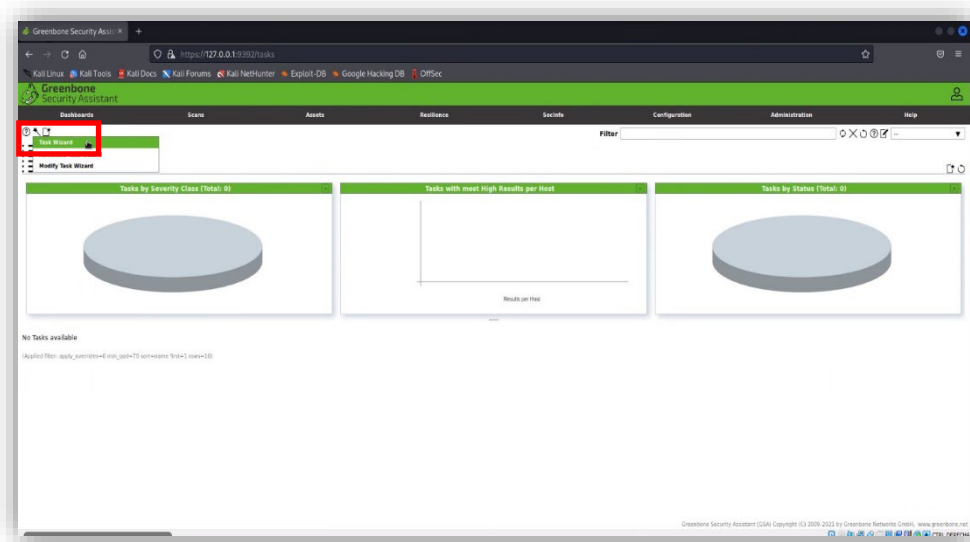


Ilustración 19: Localización del botón «Task Wizard».

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Introduce la dirección IP de la máquina víctima que, al igual que en la práctica anterior, será la IP que vimos anteriormente. En nuestro caso, «10.0.2.5». Verás que aparece la tarea de escaneo creada y comenzará el escaneo.

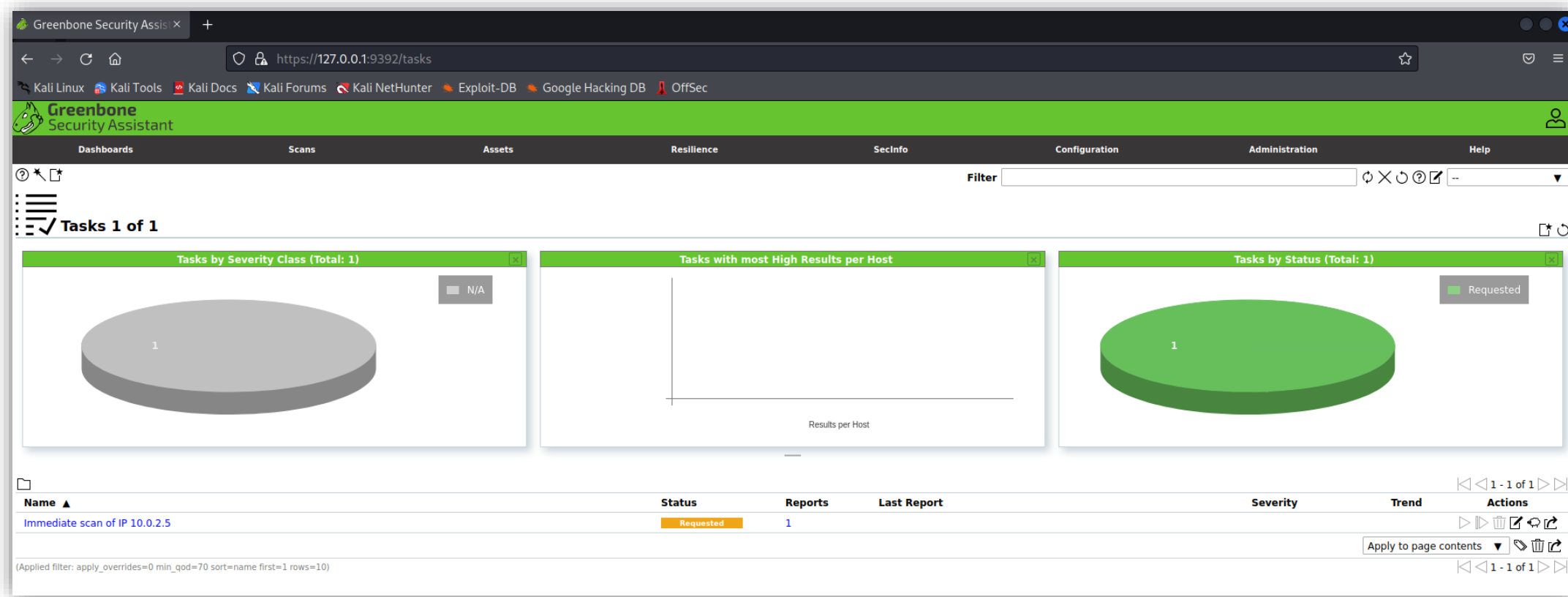


Ilustración 20: Dirección IP de la máquina víctima.

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

- Mientras se realiza el escaneo, aparecerán en diferentes pestañas los resultados obtenidos.

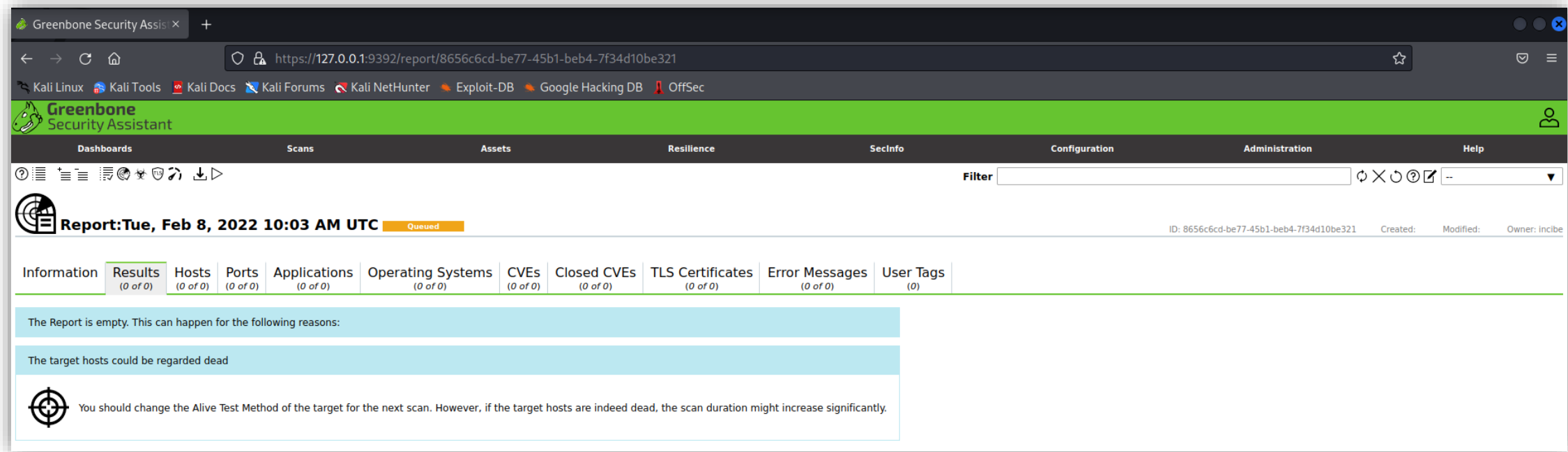


Ilustración 21: Resultados obtenidos tras introducir la dirección IP.

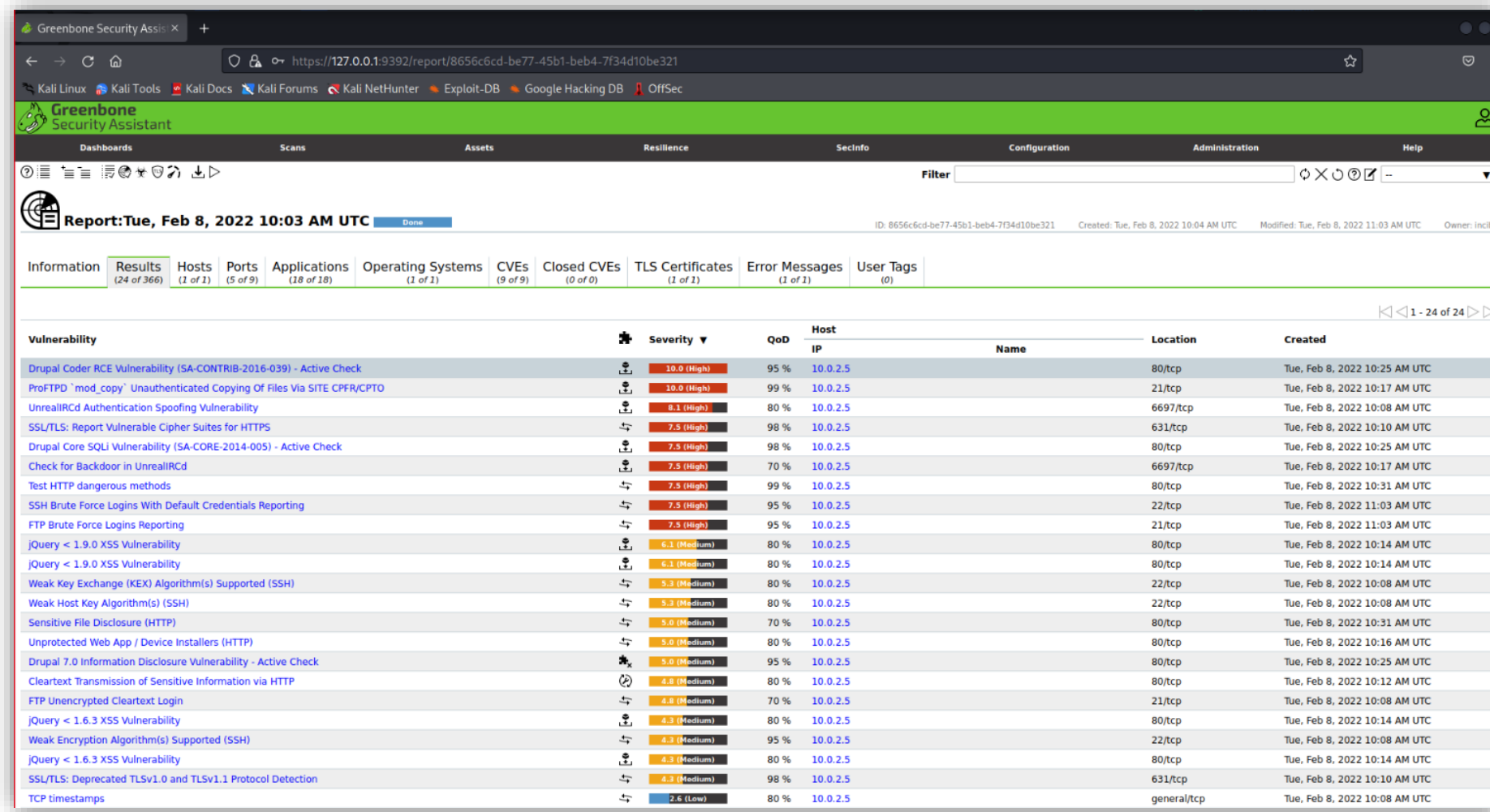
2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

En la pestaña «*Results*», verás todas las vulnerabilidades que han sido detectadas.

Por ejemplo, algunas de estas vulnerabilidades son:

- Fuente: [Vulnerabilidad en el módulo mod_copy en ProFTPD \(CVE-2015-3306\)](#).
- Fuente: [Vulnerability Details: CVE-2015-3306](#).
- Fuente: [ProFTPD module mod_copy](#).

2 INSTALACIÓN Y CONFIGURACIÓN DE OPENVAS

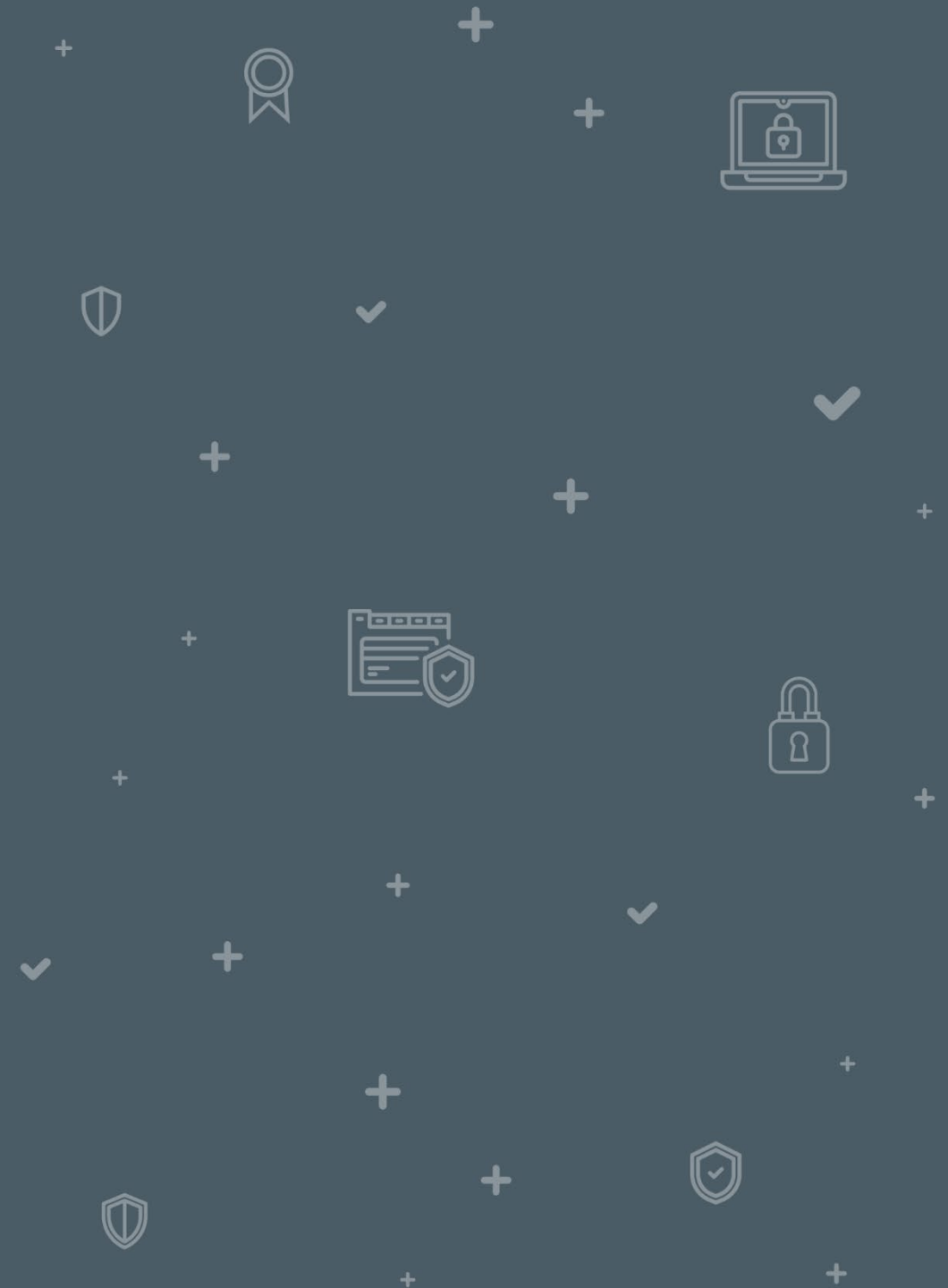


Vulnerability						
	Severity	QoD	Host IP	Name	Location	Created
Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check	10.0 (High)	95 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:25 AM UTC
ProFTPD 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPTO	10.0 (High)	99 %	10.0.2.5		21/tcp	Tue, Feb 8, 2022 10:17 AM UTC
UnrealIRCd Authentication Spoofing Vulnerability	9.1 (High)	80 %	10.0.2.5		6697/tcp	Tue, Feb 8, 2022 10:08 AM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	10.0.2.5		631/tcp	Tue, Feb 8, 2022 10:10 AM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	7.5 (High)	98 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:25 AM UTC
Check for Backdoor in UnrealIRCd	7.5 (High)	70 %	10.0.2.5		6697/tcp	Tue, Feb 8, 2022 10:17 AM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:31 AM UTC
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	10.0.2.5		22/tcp	Tue, Feb 8, 2022 11:03 AM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	10.0.2.5		21/tcp	Tue, Feb 8, 2022 11:03 AM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:14 AM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:14 AM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	10.0.2.5		22/tcp	Tue, Feb 8, 2022 10:08 AM UTC
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	10.0.2.5		22/tcp	Tue, Feb 8, 2022 10:08 AM UTC
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:31 AM UTC
Unprotected Web App / Device Installers (HTTP)	5.0 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:16 AM UTC
Drupal 7.0 Information Disclosure Vulnerability - Active Check	5.0 (Medium)	95 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:25 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:12 AM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.0.2.5		21/tcp	Tue, Feb 8, 2022 10:08 AM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:14 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	95 %	10.0.2.5		22/tcp	Tue, Feb 8, 2022 10:08 AM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	10.0.2.5		80/tcp	Tue, Feb 8, 2022 10:14 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.0.2.5		631/tcp	Tue, Feb 8, 2022 10:10 AM UTC
TCP timestamps	2.6 (Low)	80 %	10.0.2.5		general/tcp	Tue, Feb 8, 2022 10:08 AM UTC

Ilustración 22: Vulnerabilidades que han sido detectadas en la pestaña «Results».

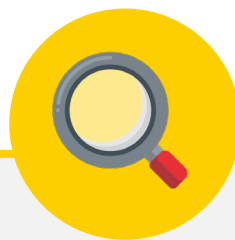
3

ENUNCIADO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD





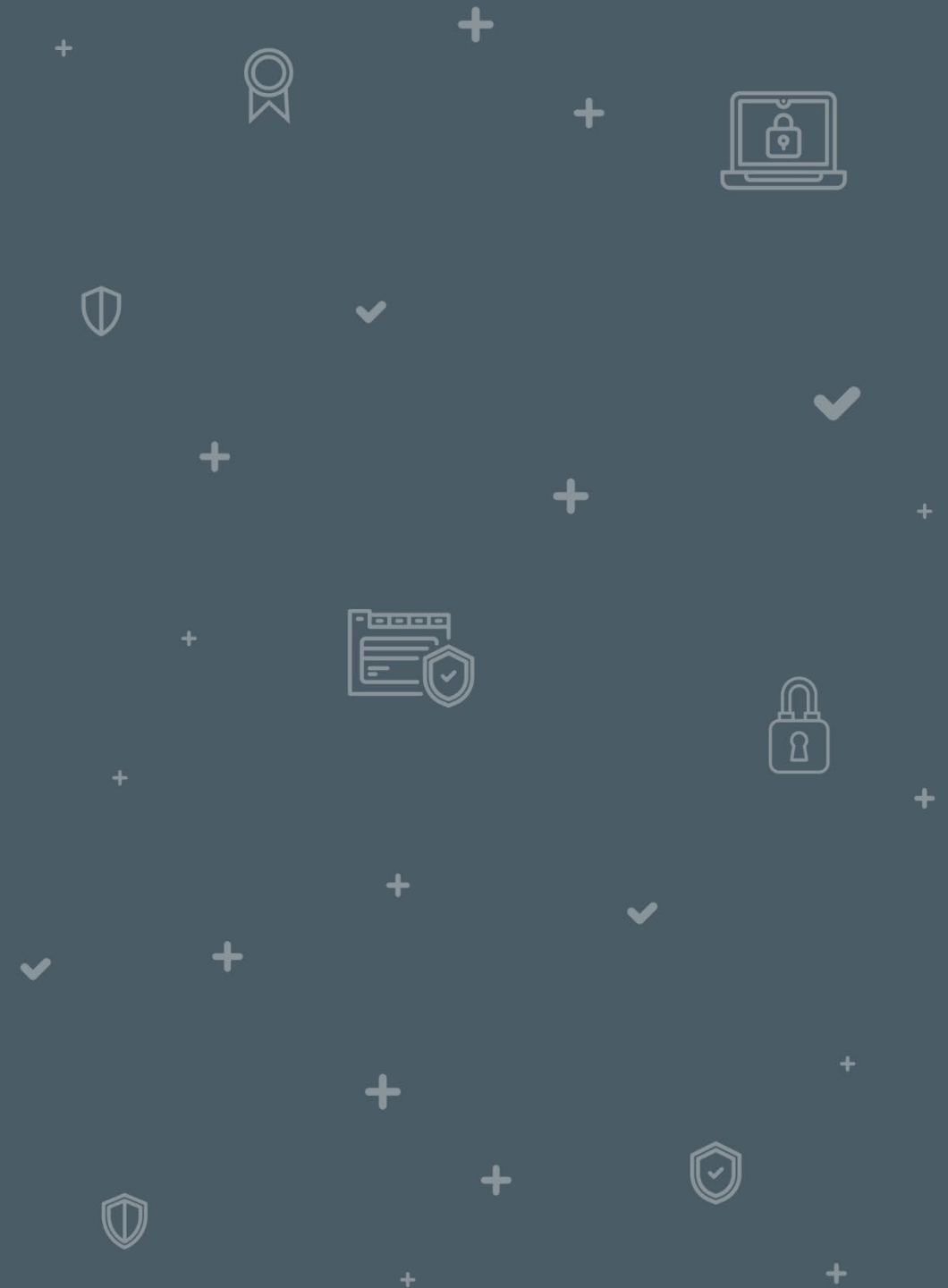
ENUNCIADO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD



Ahora, busca entre las CVEs la vulnerabilidad CVE-2015-3306 e investiga sobre ella y el impacto que ha tenido.

4

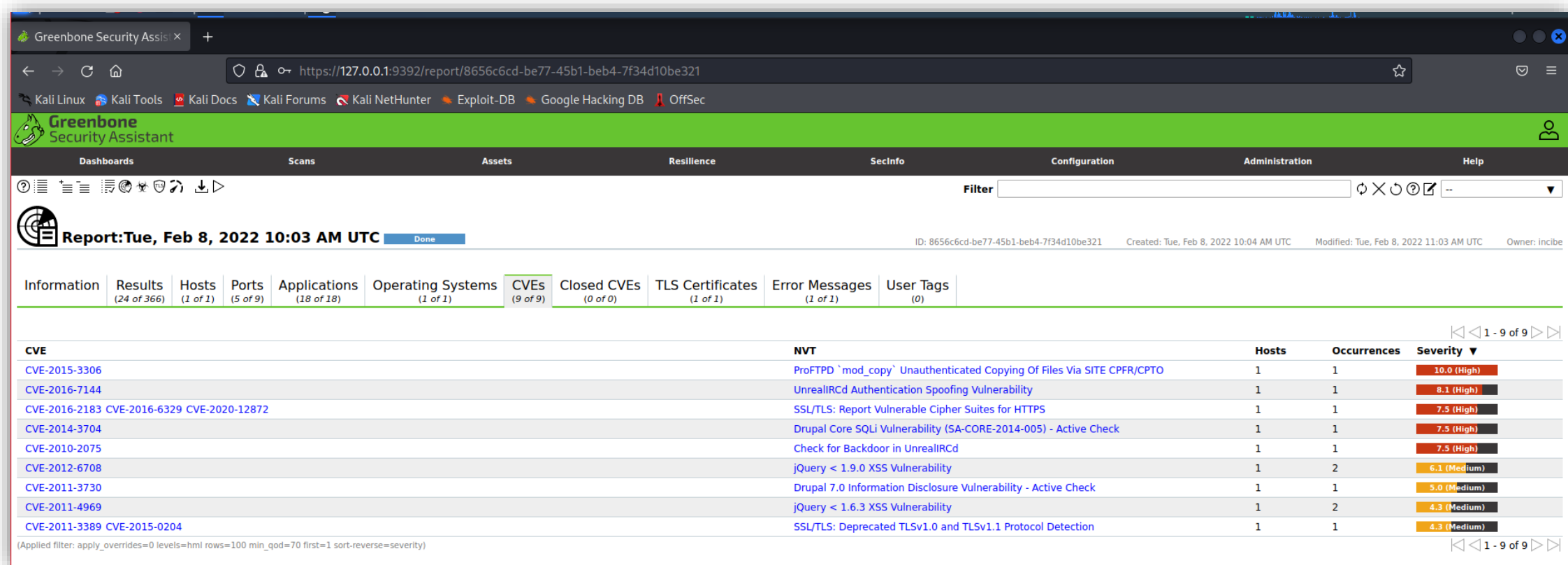
SOLUCIONARIO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD



4 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD

Ahora, busca entre las CVEs la vulnerabilidad CVE-2015-3306 e investiga sobre ella y el impacto que ha tenido.

- En la pestaña «CVEs» aparecen las diferentes vulnerabilidades que se han detectado.



CVE	NVT	Hosts	Occurrences	Severity
CVE-2015-3306	ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO	1	1	10.0 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	8.1 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	1	7.5 (High)
CVE-2014-3704	Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	1	1	7.5 (High)
CVE-2010-2075	Check for Backdoor in UnrealIRCd	1	1	7.5 (High)
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	1	2	6.1 (Medium)
CVE-2011-3730	Drupal 7.0 Information Disclosure Vulnerability - Active Check	1	1	5.0 (Medium)
CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	1	2	4.3 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse=severity)

Ilustración 23: Vulnerabilidades detectadas en CVEs.

4 SOLUCIONARIO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD

- Haz clic en la vulnerabilidad CVE-2015-3306 para conocer más información sobre ella.

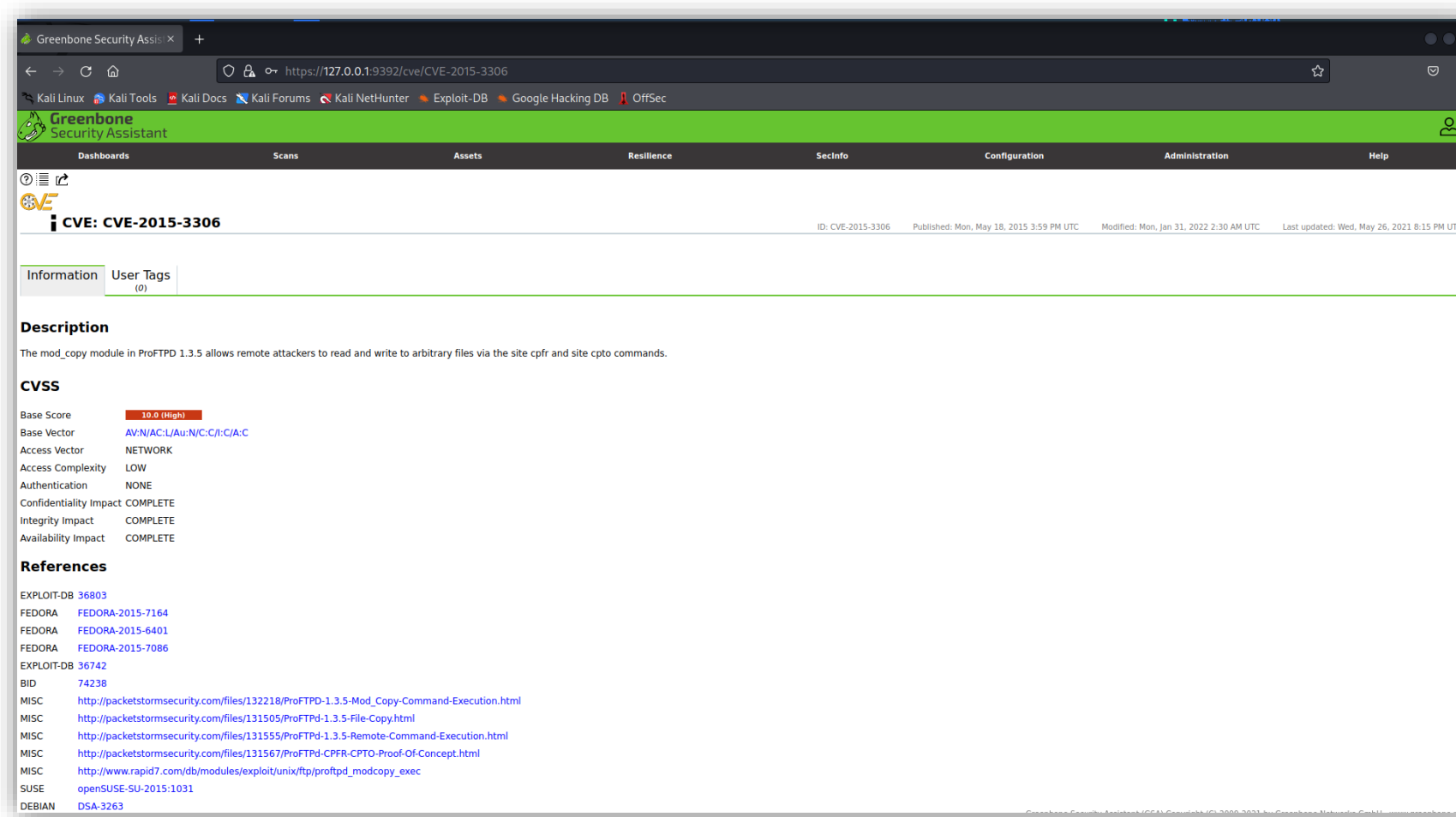


Ilustración 24: Más información sobre la vulnerabilidad CVE-2015-3306 .

SOLUCIONARIO EJERCICIO PRÁCTICO 1: EL ANÁLISIS DE UNA DETERMINADA VULNERABILIDAD

- Si buscas en Internet más información acerca de la vulnerabilidad, verás que se trata de una vulnerabilidad en el módulo mod_copy en ProFTPD 1.3.5, un servidor FTP que permite la transferencia de archivos de un dispositivo a otro.
- El módulo mod_copy permite a los atacantes remotos leer y escribir en ficheros arbitrarios a través de los comandos «**site cpfr**» y «**site cpto**», es decir, cualquier usuario no autenticado (aprovechar esta vulnerabilidad no requiere autenticación) puede aprovechar estos comandos para realizar copias de archivos desde cualquier parte del sistema de archivos hacia el destino que él mismo elija.
- El comando «**site cpfr**» especifica el archivo o directorio de origen que se utilizará para copiar de un lugar a otro directamente en el servidor, mientras que el comando «**site cpto**» especifica el archivo o directorio de destino.
- Esta vulnerabilidad compromete la integridad, existiendo una pérdida completa de la protección del sistema; la confidencialidad, existiendo una divulgación total de la información y la disponibilidad del sistema, existiendo un cierre total del recurso afectado, permitiendo al atacante hacer que el recurso no esté disponible.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

