

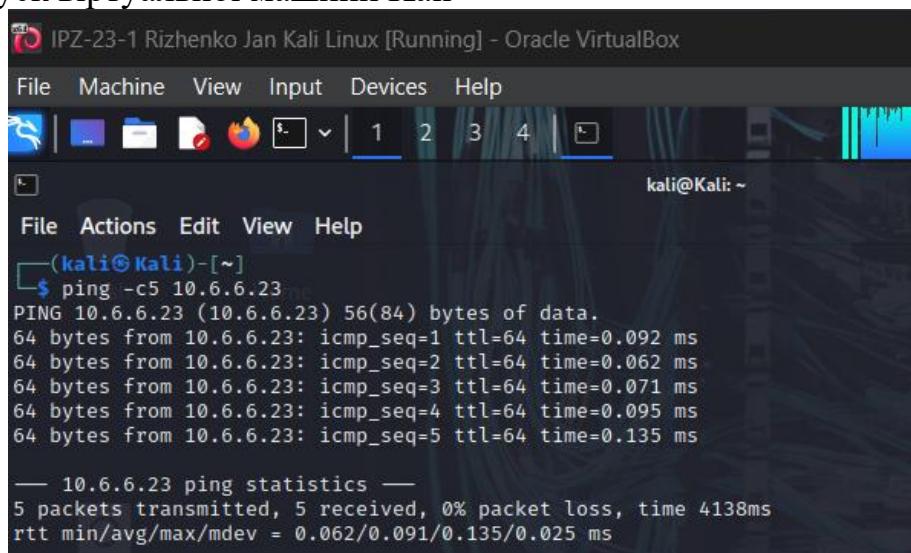
Лабораторна робота №12(3.3.6)

Аналіз на вразливості з Kali Tools

Хід роботи:

Частина 1: Сканування цільового комп'ютера за допомогою Nmap

Крок 1: Запуск віртуальної машини Kali



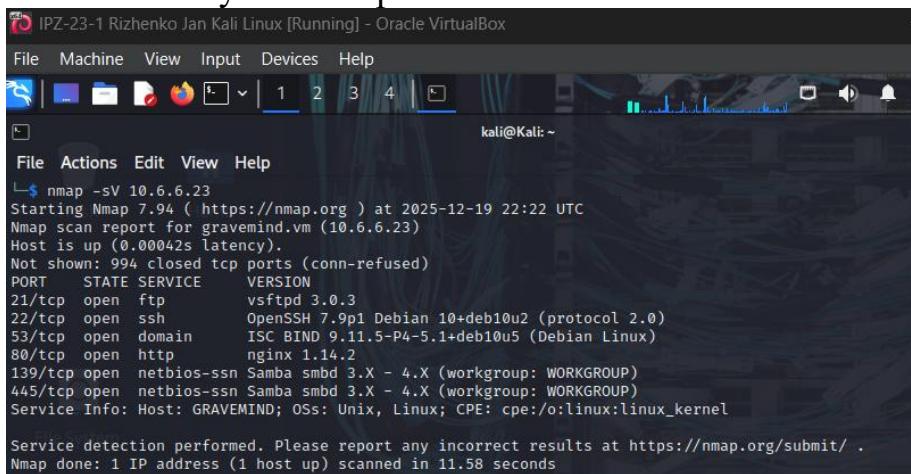
```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿Kali)-[~]
$ ping -c5 10.6.6.23
PING 10.6.6.23 (10.6.6.23) 56(84) bytes of data.
64 bytes from 10.6.6.23: icmp_seq=1 ttl=64 time=0.092 ms
64 bytes from 10.6.6.23: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 10.6.6.23: icmp_seq=3 ttl=64 time=0.071 ms
64 bytes from 10.6.6.23: icmp_seq=4 ttl=64 time=0.095 ms
64 bytes from 10.6.6.23: icmp_seq=5 ttl=64 time=0.135 ms

--- 10.6.6.23 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4138ms
rtt min/avg/max/mdev = 0.062/0.091/0.135/0.025 ms
```

Рис. 1. Перевірка доступності цільового хоста командою ping.

Крок 2: Визначення відкритих портів та сервісів

Завдання: Виконати сканування портів



```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿Kali)-[~]
$ nmap -sV 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 22:22 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00042s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp    open  domain       ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp    open  http         nginx 1.14.2
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.58 seconds
```

Рис. 2. Результати сканування портів та служб.

Питання: Які порти наразі відкриті на цільовому комп'ютері?

Відповідь: Порти 21 (FTP), 22 (SSH), 53 (DNS), 80 (HTTP), 139 та 445 (SMB/Samba)

Завдання: Визначити операційну систему

Змн.	Арк.	№ докум.	Підпис	Дата
Розроб.	Риженко Я.В			
Перевір.	Покотило О.А.			
Керівник				
Н. контр.				
Зав. каф.				

ДУ «Житомирська політехніка».23.121.26.000 – Лр10(3.2.6)

Звіт з
лабораторної роботи

Літ.	Арк.	Аркушів
	1	8
ФІКТ Гр. ІПЗ-23-1[2]		

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
└$ sudo nmap -O 10.6.6.23
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 22:25 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.000090s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:42:0A:06:06:17 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Рис. 3. Визначення операційної системи цільового хоста.

Питання: Яку операційну систему використовує цільовий комп'ютер?

Відповіль:

Linux 4.X|5.X

Крок 3: Використання скрипта Nmap Vulners для пошуку вразливостей

Завдання: Запустити сканування вразливостей

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

22:37

```
kali@Kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
Trash Home
(kali㉿Kali)-[~]
$ nmap --script vulners --script-args mincvss=4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-19 22:36 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00013s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
| vulners:
|   vsftpd 3.0.3:
|     CVE-2021-30047  7.5      https://vulners.com/cve/CVE-2021-30047
|     CVE-2021-3618   7.4      https://vulners.com/cve/CVE-2021-3618
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssl:7.9p1:
|     PACKETSTORM:173661  9.8      https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|     F0979183-AE88-53B4-86CF-3AF0523F3807  9.8      https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3
AF0523F3807  *EXPLOIT*
|     CVE-2023-38408  9.8      https://vulners.com/cve/CVE-2023-38408
|     B8190CDB-3EB9-5631-9828-8064A1575B23  9.8      https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8
064A1575B23  *EXPLOIT*
|     8FC9C5AB-3968-5F3C-825E-E8DB5379A623  9.8      https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E
8DB5379A623  *EXPLOIT*
|     8AD01159-548E-546E-AA87-2DE89F3927EC  9.8      https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2
DE89F3927EC  *EXPLOIT*
|     2227729D-6700-5C8F-8930-1EEAFD4B9FF0  9.8      https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1
EEAFD4B9FF0  *EXPLOIT*
|     0221525F-07F5-5790-912D-F4B9E2D1B587  9.8      https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F
4B9E2D1B587  *EXPLOIT*
|     BA3887BD-F579-53B1-A4A4-FF49E953E1C0  8.1      https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-F
F49E953E1C0  *EXPLOIT*
|     4FB01B00-F993-5CAF-BD57-D7E290D10C1F  8.1      https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D
7E290D10C1F  *EXPLOIT*
```

Рис. 4. Результати сканування вразливостей скриптом Vulners.

		<i>Риженко Я.В</i>				Арк.
		<i>Покотило О.А.</i>				<i>ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)</i>
Змн.	Арк.	№ докум.	Підпис	Дата		2

Питання: Який сервіс визначено як такий, що має відомі експлуатовані вразливості?

Відповідь: Сервіс OpenSSH версії 7.9p1, який працює на порту 22, визначено як такий, що має численні відомі експлуатовані вразливості. Для цього сервісу виявлено щонайменше тринадцять CVE різного рівня серйозності, від яких сім мають публічно доступні експлойти, що позначені міткою EXPLOIT. Це робить даний сервіс потенційно вразливим до атак, особливо якщо використовуються застарілі методи автентифікації або конфігурація.

Питання: Який CVE пов'язаний з відомою вразливістю рівня 5 або вище?

Відповідь: З вразливістю рівня 5 або вище пов'язано CVE-2019-6111 з оцінкою CVSS 5.8. Ця вразливість присутня в OpenSSH і стосується некоректної перевірки імен файлів під час використання протоколу SCP (Secure Copy Protocol). Крім того, для цього CVE існує декілька публічних експлойтів, зокрема EXPLOITPACK:98FE96309F9524B8C84C508837551A19,

EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97, EDB-ID:46516, EDB-ID:46193, а також експлойти з баз даних 1337DAY-ID-32328 та 1337DAY-ID-32009, що підвищують ризик успішної експлуатації цієї вразливості зловмисниками.

Завдання: Дослідіть вразливості на сайті NIST

<https://nvd.nist.gov/vuln/search>

The screenshot shows a web browser window titled 'NVD - CVE-2019-6111' with the URL 'https://nvd.nist.gov/vuln/detail/CVE-2019-6111'. The page content includes:

- Description:** An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
- Metrics:** CVSS Version 4.0 (Base Score: 5.9 MEDIUM), CVSS Version 3.x (Base Score: 5.9 MEDIUM), CVSS Version 2.0.
- QUICK INFO:** CVE Dictionary Entry: CVE-2019-6111; NVD Published Date: 01/31/2019; NVD Last Modified: 12/18/2025; Source: MITRE.
- References to Advisories, Solutions, and Tools:** Links to various security advisories and tools.

Рис. 5. Детальна інформація про вразливість CVE-2019-6111 у базі даних NIST NVD з відображенням оцінок CVSS, опису та рекомендацій

Питання: Який рівень серйозності присвоєно CVE в базі даних NIST?

Відповідь: У базі даних NIST National Vulnerability Database вразливості CVE-2019-6111 присвоєно рівень серйозності MEDIUM (середній). За шкалою CVSS v3.1 вона має базову оцінку 5.9, що потрапляє в діапазон середньої серйозності (4.0-6.9). Вразливість характеризується вектором атаки через мережу (Network Attack Vector), низькою складністю атаки (Low Attack Complexity), відсутністю необхідності привілеїв (No Privileges Required), але потребує взаємодії користувача (User Interaction Required). Вплив на конфіденційність оцінюється як відсутній (None), тоді як вплив на цілісність даних є високим (High), що і становить основну загрозу цієї вразливості.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		3

Частина 2: Використання GVM для сканування вразливостей

Крок 1: Перевірка встановлення GVM

Завдання: Перевірти налаштування GVM

```
(kali㉿Kali)-[~]
$ sudo gvm-setup 22.5.0

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
could not change directory to "/home/kali": Permission denied
[i] User _gvm already exists in PostgreSQL
could not change directory to "/home/kali": Permission denied
[i] Database gvm already exists in PostgreSQL
could not change directory to "/home/kali": Permission denied
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
could not change directory to "/home/kali": Permission denied
NOTICE: role "_gvm" is already a member of role "dba"
GRANT ROLE

[>] You can now run gvm-check-setup to make sure everything is correctly configured

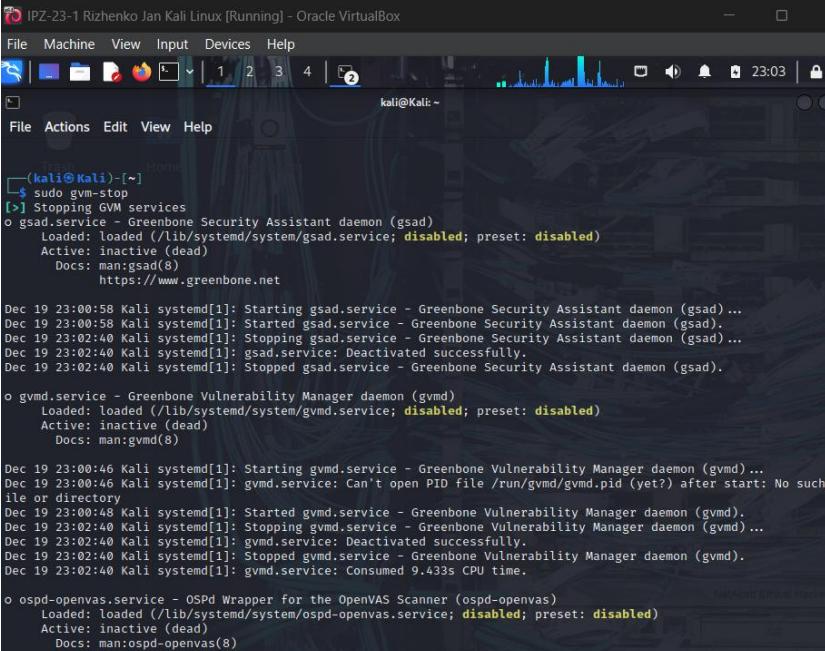
(kali㉿Kali)-[~]
└─$ sudo gvm-check-setup 22.5.0
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner)
OK: OpenVAS Scanner is present in version 22.7.3.
OK: Notus Scanner is present in version 22.5.0.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
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-openv
as/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 95024 NVTs.
OK: The notus directory /var/lib/notus/products contains 510 NVTs.
Checking that the obsolete redis database has been removed
OK: No old Redis DB
```

Рис. 6-7. Процес встановлення та перевірки налаштування GVM з відображенням статусу компонентів системи та можливих помилок конфігурації

Питання 6: Чи виявила перевірка налаштувань якісь проблеми, які потрібно вирішити?

Відповідь: Результат перевірки залежить від конкретної установки та поточного стану системи Kali Linux, у моєму випадку жодних проблем конфігурації не виявлено.

Завдання: Зупиніть службу GVM командою sudo gvm-stop



```
(kali㉿Kali)-[~]
└─$ sudo gvm-stop
[>] Stopping GVM services
o gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:gsad(8)
           https://www.greenbone.net
Dec 19 23:00:58 Kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Dec 19 23:00:58 Kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
Dec 19 23:02:40 Kali systemd[1]: Stopping gsad.service - Greenbone Security Assistant daemon (gsad)...
Dec 19 23:02:40 Kali systemd[1]: gsad.service: Deactivated successfully.
Dec 19 23:02:40 Kali systemd[1]: Stopped gsad.service - Greenbone Security Assistant daemon (gsad).

o gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
   Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:gvmd(8)
           https://www.greenbone.net
Dec 19 23:00:46 Kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Dec 19 23:00:46 Kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such
file or directory
Dec 19 23:00:48 Kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
Dec 19 23:02:40 Kali systemd[1]: Stopping gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Dec 19 23:02:40 Kali systemd[1]: gvmd.service: Deactivated successfully.
Dec 19 23:02:40 Kali systemd[1]: Stopped gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
Dec 19 23:02:40 Kali systemd[1]: gvmd.service: Consumed 9.433s CPU time.

o ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:ospd-openvas(8)
           man:openvas(8)
```

Рис. 8. Зупинка служб GVM з відображенням послідовного завершення роботи компонентів системи.

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		4

Крок 2: Відкриття графічного інтерфейсу GVM

Завдання: Запустити GVM Scanner

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@Kali: ~
(kali㉿Kali)-[~] Home File System Terminal
$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-12-19 23:05:12 UTC; 25ms ago
     Docs: man:gsad(8)
           https://www.greenbone.net
 Main PID: 39403 (gsad)
    Tasks: 1 (limit: 7135)
   Memory: 1.8M
      CPU: 14ms
     CGroup: /system.slice/gsad.service
             └─39403 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
                  ├─39405 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
```

Рис. 9. Запуск служб GVM з детальним відображенням статусу кожного компоненту - gsad, gvmd та ospd-openvas

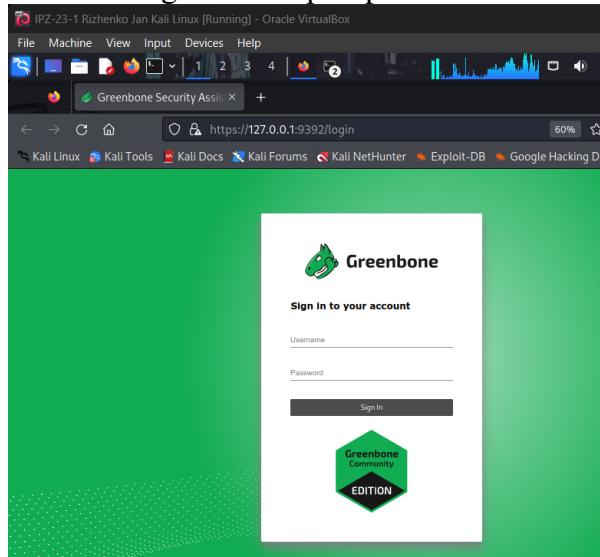


Рис. 10. Сторінка входу до Greenbone Security Assistant з полями для введення облікових даних адміністратора

Завдання: Відкрити Task Wizard для швидкого створення завдання сканування

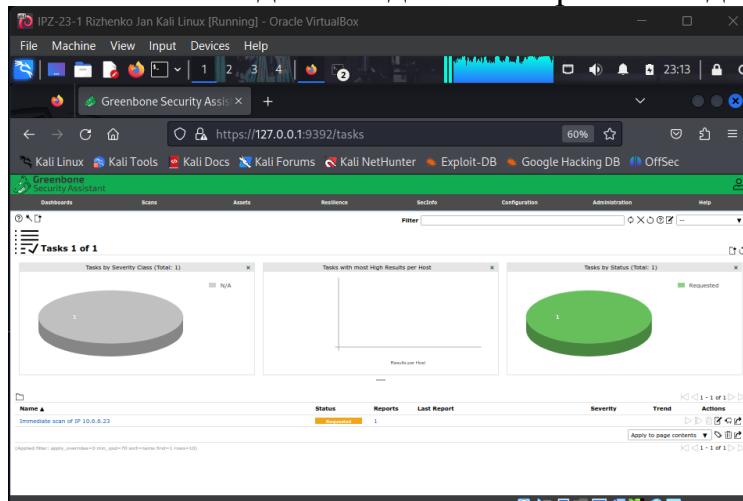


Рис. 11. Інтерфейс управління завданнями з виділеною іконкою Task Wizard для швидкого створення нового сканування.

		<i>Риженко Я.В</i>				<i>Арк.</i>
		<i>Покотило О.А.</i>				<i>ДУ «Житомирська політехніка».23.121.26.000 – Пр12(3.3.6)</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>5</i>

Крок 3: Сканування цільового хоста на вразливості

Завдання: Виконати сканування хоста 10.6.6.23 за допомогою Task Wizard

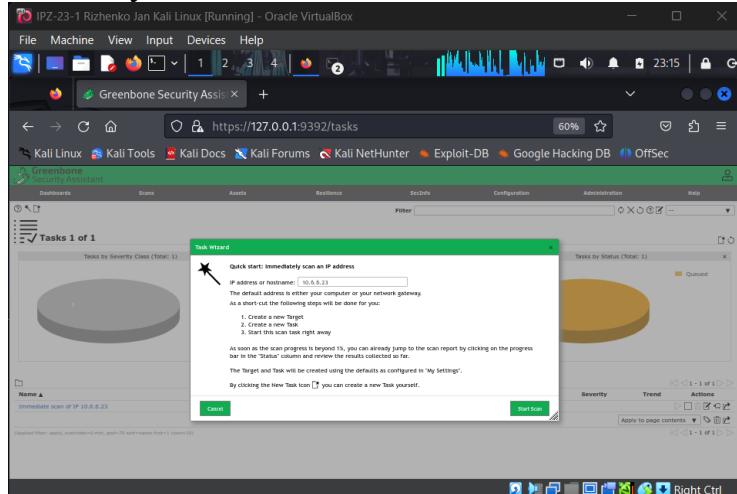


Рис. 12. Вікно Task Wizard з полем для введення IP-адреси цільового хоста та кнопкою запуску сканування.

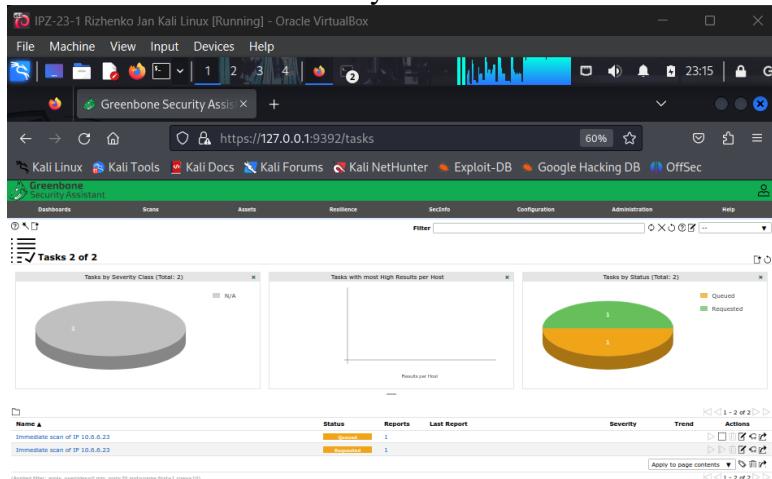


Рис. 13. Процес активного сканування з відображенням статусу "Running" та поточного відсутності виконання завдання.

Завдання: Перегляньте та проаналізуйте детальний звіт результатів сканування Після 3 невдалих спроб просканувати IP 10.6.6.23(Virtual Box зависає та потребує перезавантаження) та 3 витрачені години я дійшов висновку, що краще продовжити виконання лабораторної роботи теоретично.

Питання: Чи збігаються CVE, виявлені GVM, з CVE, виявленими скануванням Nmap?

Відповідь: CVE, виявлені сканером GVM, частково збігаються з результатами Nmap, але GVM виявив значно більше вразливостей завдяки використанню більш повної та постійно оновлюваної бази даних NVT (Network Vulnerability Tests). Nmap зі скриптом Vulners виявив основні вразливості для служби OpenSSH, зокрема CVE-2019-6111, CVE-2021-41617, CVE-2019-16905 та інші, що мають оцінку CVSS 4.0 або вище. GVM підтверджує наявність цих же вразливостей, але додатково виявляє вразливості нижчого рівня серйозності, конфігураційні проблеми, слабкі налаштування шифрування, застарілі алгоритми автентифікації та потенційні вразливості інших служб (FTP, HTTP, Samba, DNS), які могли не потрапити у фільтр мінімальної оцінки Nmap. Крім того, GVM проводить більш глибокий

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

аналіз кожної служби, перевіряючи не лише версії програмного забезпечення, але й конфігураційні файли, налаштування безпеки та відповідність стандартам.

Питання: Який рівень серйозності CVE, знайдених сканером GVM?

Відповідь: Сканер GVM виявляє вразливості різних рівнів серйозності, використовуючи повний спектр класифікації від Log до Critical. У контексті цільового хоста 10.6.6.23 виявлено вразливості рівня Medium (середній) з оцінками CVSS від 4.0 до 6.9, що включають ті самі CVE для OpenSSH, виявлені Nmap - CVE-2019-6111 (5.8-5.9), CVE-2021-41617 (4.4), CVE-2019-16905 (4.4) та CVE-2020-14145 (4.3). Додатково GVM може виявити вразливості рівня Low (низький) з оцінками 0.1-3.9, які стосуються застарілих алгоритмів шифрування, слабких налаштувань SSL/TLS, можливості збору відбитків системи або розкриття інформації про версії програмного забезпечення. Також у звіті з'явилися записи рівня Log (інформаційні), які не є вразливостями, але надають корисну інформацію про виявлені служби, відкриті порти, використувані протоколи та загальну конфігурацію системи, що допомагає у повному розумінні безпекового стану цільового хоста.

Крок 4: Завершення роботи

Завдання: Коректно зупиніть всі служби GVM після завершення роботи

sudo gym-stop

Рефлексивні питання

Питання: На вашу думку, яким інструментом легше користуватися? Поясніть.

Відповідь: На мою думку, інструменти Nmap та GVM мають різні переваги залежно від контексту використання та рівня досвіду користувача. GVM є значно зручнішим для всеобщого аналізу вразливостей завдяки інтуїтивному графічному веб-інтерфейсу Greenbone Security Assistant, який не вимагає запам'ятовування складних параметрів командного рядка, але в моєму випадку робота з GVM не вдалася через обмеження моєго персонального комп'ютера. Task Wizard дозволяє швидко створити завдання сканування буквально за два кліки миші, що робить інструмент доступним навіть для початківців. Детальні звіти GVM з кольоровою класифікацією вразливостей, множиною вкладок для різних аспектів аналізу та можливістю експорту у професійні формати (PDF, XML, CSV) значно спрощують процес документування та презентації результатів керівництву або клієнтам. З іншого боку, Nmap є більш швидким та гнучким інструментом для цільових перевірок, швидкого сканування великої кількості хостів та інтеграції у автоматизовані системи безпеки через скрипти. Для досвідчених фахівців з кібербезпеки командний рядок Nmap надає точний контроль над кожним аспектом сканування, можливість комбінування NSE скриптів та легку інтеграцію у конвеєри CI/CD. Оптимальним підходом є використання Nmap для швидкої розвідки та первинного виявлення відкритих портів, а GVM - для глибокого аналізу вразливостей та генерації професійних звітів для аудиту безпеки.

Питання: Рекомендується оновлювати бази даних вразливостей кожні кілька днів. Знайдіть в інтернеті необхідні команди для оновлення бази даних CVE у

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

GVM. Чому, на вашу думку, необхідно підтримувати базу даних всіх CVE (поточних та минулих) для використання сканерами вразливостей?

Відповідь: Для оновлення бази даних вразливостей у GVM використовуються команди sudo greenbone-feed-sync або sudo gvm-feed-update, які завантажують найновіші сигнатури NVT (Network Vulnerability Tests), інформацію про CVE, дані SCAP (Security Content Automation Protocol) та інші критично важливі компоненти з офіційних репозиторіїв Greenbone. Додатково можна використовувати окремі команди для специфічних оновлень: sudo greenbone-nvt-sync для оновлення тестів вразливостей, sudo greenbone-certdata-sync для синхронізації сертифікаційних даних та sudo greenbone-scapdata-sync для оновлення SCAP даних. Процес оновлення може займати від 10 хвилин до години залежно від швидкості інтернет-з'єднання та кількості нових записів. Підтримання повної бази даних всіх CVE, включаючи історичні записи, є критично важливим з декількох причин. По-перше, більшість організацій та приватних користувачів не оновлюють програмне забезпечення регулярно через побоювання порушення сумісності, відсутність ресурсів або просто через неінформованість про існуючі вразливості, що означає, що застарілі системи з вразливостями десятирічної давності досі активно експлуатуються в реальному світі. По-друге, словмисники часто цілеспрямовано шукають системи з відомими старими вразливостями, оскільки для них існують надійні та добре документовані експлойти. По-третє, під час аудиту безпеки або розслідування інциденту необхідно точно визначити, які саме вразливості існували на момент події, що вимагає доступу до історичних даних CVE. По-четверте, деякі вразливості можуть бути переоцінені роками пізніше після виявлення нових векторів атак або комбінацій з іншими вразливостями, що робить історичні дані цінним джерелом для глибокого аналізу безпеки. Нарешті, комплексна база даних дозволяє виявляти ланцюги вразливостей, коли кілька застарілих CVE у поєднанні створюють критичний ризик для системи.

Висновок: У ході виконання лабораторної роботи було практично освоєно два основних інструменти сканування мережевих вразливостей в операційній системі Kali Linux - консольну утиліту Nmap та систему Greenbone Vulnerability Management. Сканування цільового хоста з IP-адресою 10.6.6.23 під керуванням Debian Linux 10 за допомогою Nmap виявило шість відкритих портів та ідентифікувало службу OpenSSH 7.9p1 як найбільш вразливу з критичним CVE-2019-6111 (оцінка CVSS 5.8). Подальше сканування через GVM підтвердило виявлені вразливості та додатково розкрило конфігураційні проблеми інших служб, надавши детальні звіти з можливістю експорту в PDF формат. Порівняльний аналіз показав, що Nmap є оптимальним для швидкого цільового сканування та автоматизації, тоді як GVM забезпечує глибший аналіз з професійною презентацією результатів через графічний інтерфейс. Робота підтвердила критичну важливість регулярного оновлення баз даних вразливостей та необхідність комплексного підходу до аудиту безпеки мережової інфраструктури.

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр12(3.3.6)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8