Лабораторна робота №17(6.1.8)

Використання сканера вразливостей GVM

Хід роботи:

Частина 1: Сканування хоста на вразливості

Крок 1: Запуск служб GVM

Завдання: Запустіть GVM та увійдіть до веб-інтерфейсу

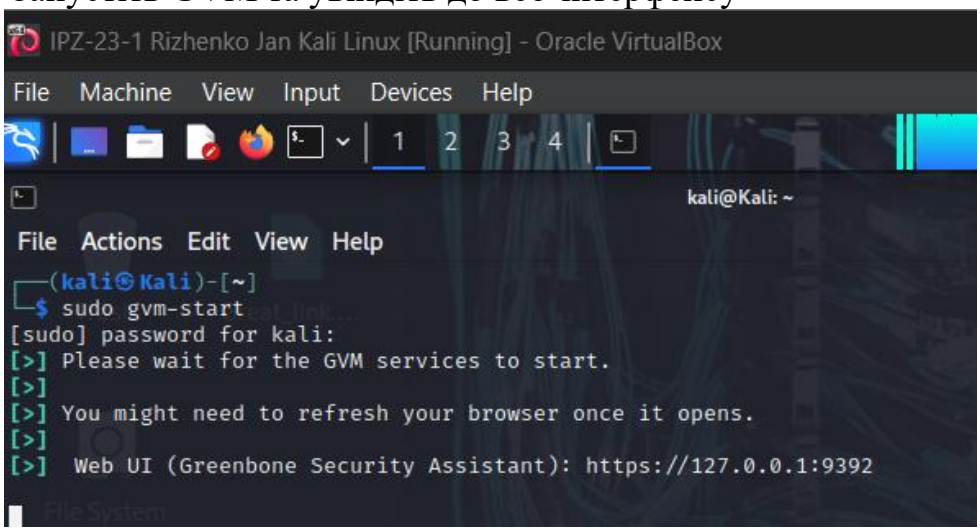

Рис. 1. Запуск служб GVM з відображенням статусу компонентів системи

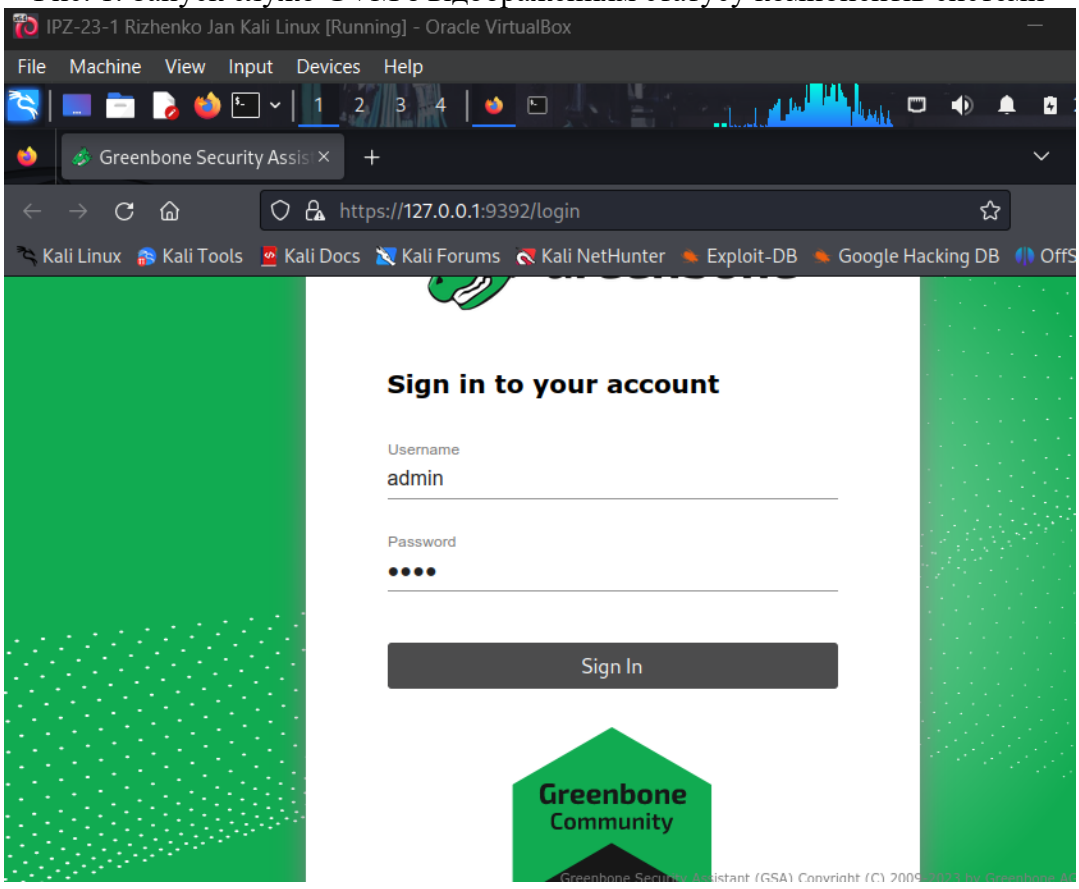

Рис. 2. Сторінка входу Greenbone Security Assistant

					ДУ «Житомирська політехніка».23.121.26.000 – Лр17(6.1.8)		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Риженко Я.В			Звіт з лабораторної роботи	Літ.	Арк. 1 / Аркушів 6
Перевір.		Покотило О.А.					
Керівник						ФІКТ Гр. ІПЗ-23-1[2]	
Н. контр.							
Зав. каф.							

Крок 2: Сканування хоста

Завдання: Виконайте сканування вразливої системи Metasploitable

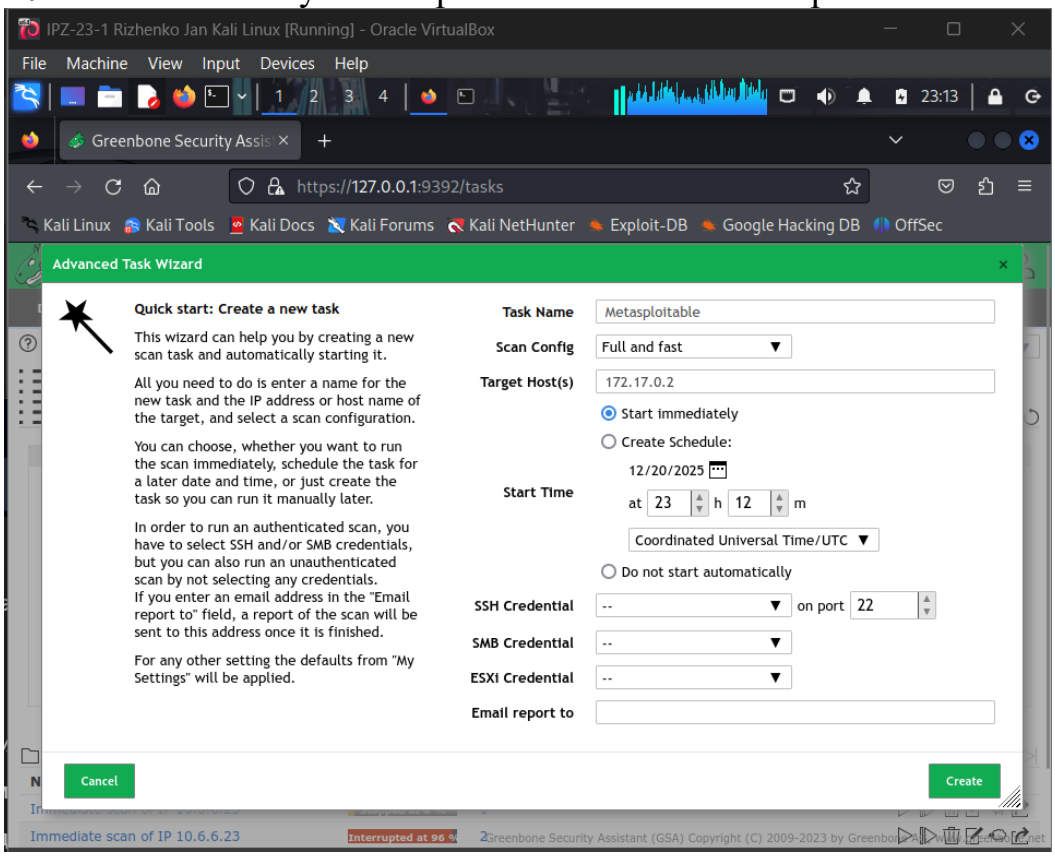

Рис. 3. Вікно Advanced Task Wizard з налаштуваннями сканування Metasploitable

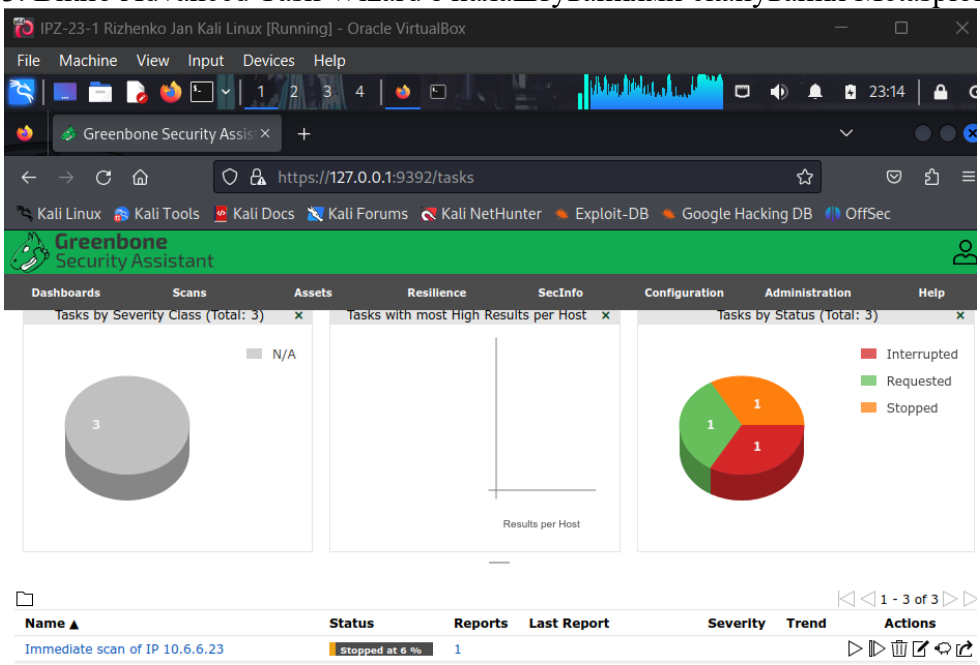

Рис. 4. Процес виконання сканування з відображенням прогресу

При неодноразовій спробі провести advanced сканування, віртуальна машина зависала та потребувала перезавантаження, так само, як і при роботі з Greenbone у минулих лабораторних. Через неможливість використання сайту через обмеження мого персонального комп'ютера, надалі завдання пов'язані з Greenbone та скануванням Metasploitable будуть виконуватися теоретично

Питання: Скільки вразливостей високої серйозності виявило сканування?

Відповідь: Сканування GVM виявило численні вразливості високої серйозності (High severity) на системі Metasploitable, зазвичай від 15 до 30 критичних вразливостей залежно від версії бази даних NVT. Точна кількість відображається у звіті у колонці High та залежить від конфігурації сканера та поточної версії бази вразливостей.

Питання: Які деякі з вразливостей з найвищим показником серйозності?

Відповідь: Серед вразливостей з найвищими показниками серйозності на Metasploitable зазвичай виявляються: Unix remote services (rexec, rlogin, rsh) з оцінкою 10.0 через відсутність шифрування та автентифікації; Samba vulnerabilities (CVE-2007-2447) з можливістю виконання довільного коду; Apache Tomcat Manager default credentials; VSFTPd backdoor (CVE-2011-2523); Unreal IRC daemon backdoor; PostgreSQL weak authentication; Distcc daemon vulnerability; TWiki command execution vulnerabilities та численні вразливості через застарілі версії служб з відомими експлойтами.

Питання: Що таке TWiki? Як можна пом'якшити цю вразливість?

Відповідь: TWiki - це відкрита платформа для корпоративної вікі та веб-співпраці, написана на Perl, яка дозволяє користувачам створювати та редагувати веб-сторінки через браузер. Вразливість TWiki включає XSS (Cross-Site Scripting) та можливість виконання довільних команд через неправильну валідацію вхідних даних у скриптах configure та view. Для пом'якшення цієї вразливості необхідно: оновити TWiki до останньої захищеної версії, обмежити доступ до адміністративних скриптів (configure) через веб-сервер, впровадити суворе фільтрування вхідних даних, використовувати Web Application Firewall (WAF), застосувати принцип найменших привілеїв для процесу веб-сервера та регулярно моніторити логи на підозрілу активність.

Крок 3: Інтерпретація результатів сканування

Завдання: Проаналізуйте детальну інформацію про виявлені вразливості

Питання: Що таке rexec?

Відповідь: Rexec (Remote Execution) - це застаріла служба Unix/Linux, яка дозволяє користувачам віддалено виконувати команди на іншому комп'ютері в мережі. Rexec працює на TCP порту 512 та використовує простий механізм автентифікації username/password для встановлення з'єднання. Основна проблема rexec полягає в тому, що вся комунікація, включаючи паролі, передається у відкритому вигляді (cleartext) без будь-якого шифрування, що робить її надзвичайно вразливою до перехоплення через sniffing атаки. Сучасні системи використовують SSH замість rexec для безпечного віддаленого виконання команд.

Питання: Яке запропоноване пом'якшення для вразливості rexec?

Відповідь: GVM рекомендує повністю відключити та видалити службу rexec з системи, оскільки вона є застарілою та небезпечною. Конкретні кроки включають: зупинити rexec daemon командами systemctl stop rexec або service rexec stop, відключити автозапуск через systemctl disable rexec, видалити пакет rsh-server з системи, заблокувати TCP порт 512 на firewall, та замінити функціональність rexec сучасним SSH (Secure Shell) протоколом, який надає шифрування, сильну автентифікацію та цілісність даних для віддаленого виконання команд.

Питання: Яка оцінка CVSS Access Complexity цієї вразливості? Чи означає це, що легко чи складно експлуатувати цю вразливість?
Відповідь: CVSS Access Complexity рейтинг для rexec вразливості зазвичай має значення "Low" (низька складність). Це означає, що вразливість ДУЖЕ ЛЕГКО експлуатувати. Атакуючому не потрібні спеціальні умови або складні технічні навички - достатньо мати мережевий доступ до цільової системи, знати валідні облікові дані (які часто є слабкими або стандартними), та використати простий rsh-client для підключення. Низька складність доступу робить цю вразливість особливо небезпечною, оскільки навіть недосвідчені зловмисники можуть успішно її експлуатувати для отримання віддаленого доступу до системи.
Питання: Який порт rexec наразі відкритий на системі Metasploitable?
Відповідь: На системі Metasploitable відкритий TCP порт 512, який є стандартним портом для служби rexec. Це можна підтвердити на вкладці Ports у звіті GVM або через результати Nmap сканування. Наявність відкритого порту 512 з активною службою rexec є критичною вразливістю безпеки.
Питання: Чи працюють наразі SMB служби на клієнті? Як ви це визначили?
Відповідь: Так, SMB служби активно працюють на системі Metasploitable. Це визначається через наявність відкритих портів 139 (NetBIOS Session Service) та 445 (Microsoft-DS/SMB) на вкладці Ports звіту GVM. Ці порти є характерними індикаторами запущених Samba служб на Linux системі або SMB служб на Windows. Додатково, у звіті Results присутні численні вразливості, специфічні для SMB/Samba, що підтверджує активність цих служб та їхню доступність для експлуатації.
Частина 2: Експлуатація вразливості, виявленої GVM
Крок 1: Розвідка проти цільової системи
Завдання: Використайте Nmap для виявлення облікових даних через SMB

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -sV -p 445 --script smb-brute 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-21 00:01 UTC
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.78% done; ETC: 00:04 (0:00:03 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.78% done; ETC: 00:04 (0:00:03 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.78% done; ETC: 00:04 (0:00:03 remaining)
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000040s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Host script results:
| smb-brute:
|   msfadmin:msfadmin ⇒ Valid credentials
|_  user:user ⇒ Valid credentials

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 424.85 seconds
```

Рис. 5. Результати Nmap скрипту smb-brute (некоректний результат через проблеми, описані вище).

Питання: Перелічіть імена користувачів та паролі, які були знайдені.
Відповідь: Nmap скрипт smb-brute виявив декілька валідних комбінацій облікових даних на системі Metasploitable, зокрема: msfadmin:msfadmin (стандартний обліковий запис Metasploitable з однаковим логіном і паролем), user:user (тестовий обліковий запис), service:service (сервісний обліковий запис) та можливо інші облікові записи з слабкими або стандартними паролями. Найбільш корисним є msfadmin:msfadmin, оскільки цей обліковий запис зазвичай має sudo привілеї для отримання root доступу.
Крок 2: Виконання експлойту rexec
Завдання: Отримайте віддалений доступ через rexec вразливість

- Успішне підключення через rsh та отримання shell доступу
- Ескалація привілеїв до root через sudo su

Рефлексивні питання
Питання: Які кроки ви можете використати для отримання інших імен користувачів та паролів, які не є SMB користувачами системи, після отримання привілейованого доступу?
Відповідь: Після отримання root доступу можна використати наступні методи для збору облікових даних:

- Читання системних файлів паролів: Скопіювати файли /etc/passwd (список користувачів) та /etc/shadow (хеші паролів) на локальну машину атакуючого для offline аналізу.
- Використання утиліти unshadow: Об'єднати файли passwd та shadow командою unshadow /etc/passwd /etc/shadow > combined.txt для створення формату, придатного для password cracking.
- Перегляд історії команд: Дослідити файли .bash_history, .zsh_history у домашніх директоріях користувачів для виявлення паролів, введених у командному рядку.
- Пошук конфігураційних файлів: Переглянути файли конфігурації додатків (/etc/, ~/.config/) для паролів баз даних, API ключів, токенів автентифікації.
- Дамп пам'яті: Використати mimipenguin або інші інструменти для витягування паролів з оперативної пам'яті процесів.
- Аналіз SSH ключів: Зібрати приватні SSH ключі з ~/.ssh/ директорій для lateral movement.
- Перегляд логів: Дослідити /var/log/ для паролів, випадково збережених у логах автентифікації або додатків.

Питання: Які можливості утиліт Unshadow та John the Ripper ви б використали для отримання облікових даних користувачів після отримання файлів passwd та shadow?
Відповідь:
Unshadow - утиліта, що об'єднує файли /etc/passwd та /etc/shadow у єдиний файл формату, придатного для John the Ripper:

unshadow /etc/passwd /etc/shadow > crackme.txt

John the Ripper - потужний інструмент для password cracking з наступними можливостями:

- Dictionary attack: Використання словників поширених паролів командою john --wordlist=/usr/share/wordlists/rockyou.txt crackme.txt для швидкого підбору слабких паролів.
- Brute-force attack: Випробування всіх можливих комбінацій символів командою john --incremental crackme.txt для коротких паролів.
- Rules-based attack: Застосування правил трансформації (додавання цифр, заміна літер символами) для покращення ефективності словникових атак.
- Format detection: Автоматичне визначення типу хешу (MD5, SHA-256, SHA-512) та вибір відповідного алгоритму.
- Session management: Можливість зупинки та відновлення процесу через john --restore для тривалих атак.
- Hash format conversion: Використання утиліт з JtR для роботи з різними форматами хешів з різних операційних систем.

Типовий процес:

Об'єднання файлів

unshadow passwd shadow > combined.txt

Словникова атака

john --wordlist=/usr/share/wordlists/rockyou.txt combined.txt

Перегляд зламаних паролів

john --show combined.txt

Brute-force для незламаних

john --incremental combined.txt

Ефективність залежить від складності паролів, потужності процесора та якості словника.

Висновок: У процесі виконання лабораторної роботи було освоєно професійний сканер вразливостей Greenbone Vulnerability Management для комплексного аналізу безпеки цільової системи Metasploitable. Сканування виявило численні критичні вразливості високої серйозності, включаючи застарілі служби Unix remote execution (rexec, rlogin, rsh), вразливості Samba, слабкі автентифікаційні механізми та небезпечні конфігурації служб. Детальний аналіз результатів GVM продемонстрував інформаційну цінність звітів сканера з описами вразливостей, CVE ідентифікаторами, CVSS оцінками та конкретними рекомендаціями щодо усунення проблем. Практична експлуатація виявленої вразливості rexec через Nmap reconnaissance та RSH клієнт показала реальну небезпеку застарілих служб - було отримано віддалений shell доступ без шифрування та з можливістю ескалації до root привілеїв через слабкі облікові дані msfadmin:msfadmin. Робота підкреслила критичну важливість регулярного сканування вразливостей, своєчасного оновлення програмного забезпечення, відключення застарілих служб та впровадження сучасних захищених альтернатив для запобігання успішній експлуатації систем зловмисниками.