Методичні вказівки
до лабораторної роботи №6
«Тестування інформаційної безпеки комп'ютерної системи або мережі»
з навчальної дисципліни вільного вибору
«Основи інформаційної та кібербезпеки»

Зміст заняття: Отримати знання та навички користування інструментами прихованого збору інформації з мережі або комп'ютерної системи.

Загальні відомості

Сучасні комп'ютерні системи і мережі зазнають тисяч різних атак, як ззовні так і зсередини. Тому актуальним на даний час є питання різностороннього підходу до питання захищеності: оцінки захищеності системи до зламу та запобігання його руйнівним наслідкам. Тести на проникнення є складовою частиною повного аудиту безпеки.

Етичний хакінг, також відомий як тестування на проникнення (пентест, *англ. penetration test, pentesting*), є актом злому / проникнення в систему або мережі за згодою користувача. Мета полягає в тому, щоб оцінити безпеку організації, використовуючи вразливості таким чином, як б зловмисники могли їх використати.

Багато великих IT-компаній сьогодні заохочують етичних хакерів грошима за уразливості, знайдені, наприклад, за допомогою програм Bug Bounty. На сайтах деяких компаній існують окремі розділи з конкретним переліком сум грошового винагороди, які залежать від ступеня критичності знайденої уразливості. Свої програми є у Google, Facebook, Microsoft і багатьох інших.

Існує три основних види пентестування:

- **Black Box** – в цьому випадку імітується атака від зловмисника, який з самого початку не має доступу до мережі компанії і нічого не знає про будову її IT-інфраструктури.
- **Gray Box** – тут атака ведеться від імені хакера, який вже щось знає про корпоративну мережу. Глибину цих знань ви визначаєте самі. Можливо, це колишній співробітник, клієнт або користувачі гостьової бездротової мережі.
- **White Box** – в цьому випадку у зловмисника є повний доступ до інфраструктури і права адміністратора.

Найпопулярнішою схемою є Black Box, так як вона ближче всього до реальної атаки.

Об'єктами тестів на проникнення є різні компоненти інформаційної інфраструктури: активне мережеве обладнання, сервери, робочі станції,інформаційні системи, бази даних. Завдання пентестера - виявити в них уразливості і з'ясувати можливість їх експлуатації.

1. Розгортання віртуальної лабораторії для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем

Одним з методів захисту є **тестування на проникнення**, завдяки якому можна виявити вразливі місця системи безпеки і вжити відповідних заходів.

Для підвищення ефективності навчання тестування на проникнення необхідне таке середовище, в якому можна буде практикуватися, нічого не порушуючи в реальній мережі. Це і є метою створення лабораторії для тестування. Пентест-лабораторія – це невелика локальна мережа, спеціально створена для реалізації всіх можливих атак, які можливі в реальному світі. Крім того у віртуальному середовищі можна більш ретельно відслідковувати поведінку кожної системи під час атаки. Це дає додаткові відомості про те, що і як ставить під загрозу безпеку системи.

Метою даної роботи є **створення віртуальної пентест-лабораторії** і демонстрація її працездатності на конкретних прикладах.

Для виконання лабораторної роботи необхідні:

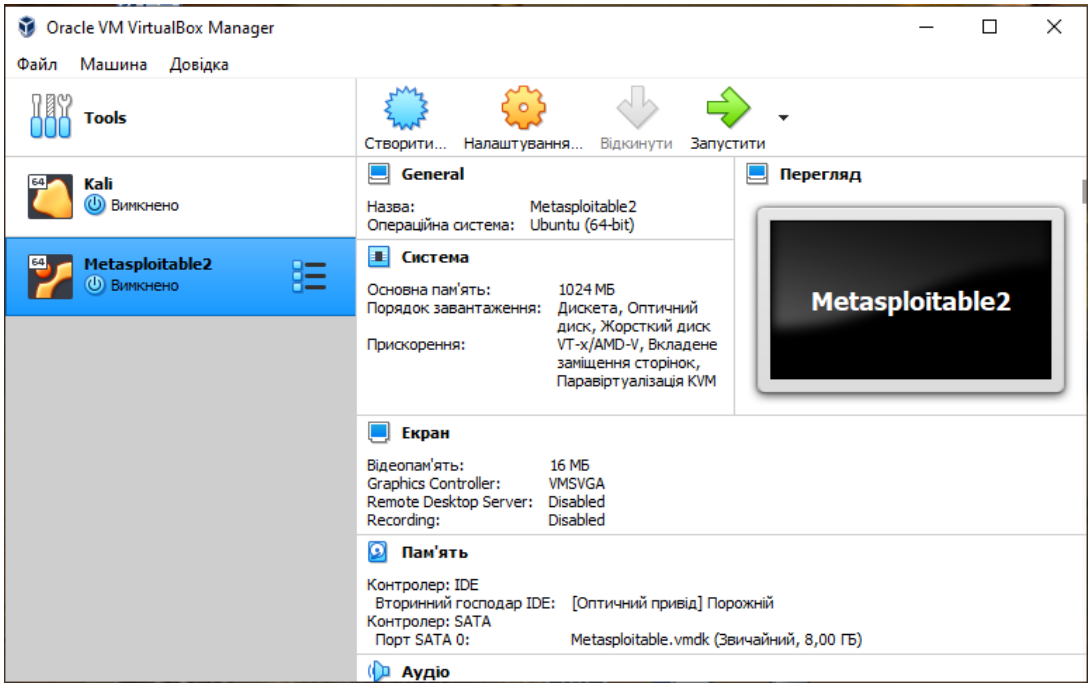
1. Засіб віртуалізації – **VirtualBox** або VMware;
2. Образ віртуальної машини для дослідження – **Metasploitable2**;
3. Образ віртуальної машини атакуючого – **Kali Linux**.

Вам знадобиться не менше 10-15 Гбайт вільного простору вінчестера, щоб запускати Калі Лінукс і віртуальну машину на одному хості. Плюс до того побільше оперативної пам'яті з непоганим процесором.

Підготовка до виконання лабораторної роботи:

1) Для виконання лабораторної роботи необхідно розгорнути інфраструктуру. Для цього потрібно завантажити і встановити середовище віртуалізації. Класичним рішенням є **Oracle VM VirtualBox** (https://www.virtualbox.org/), проте допускається використання аналогів (VMware …).

VirtualBox можливо завантажити з офіційного сайту virtualbox.org, це ПЗ розповсюджується як для операційних систем сімейства Windows так і Linux і MacOS. Детальні інструкції з інсталяції для операційної системи Linux знаходяться на тій же сторінці завантаження. Інсталяція для ОС Windows є абсолютно стандартною, але необхідно звернути увагу що під час інсталяції на короткий проміжок часу буде вимкнено доступ до мережі, це пов'язано з інсталяцією мережевих драйверів віртуальної машини.



2) Встановлюємо **віртуальну машину «жертви»**. У даній лабораторній роботі це **Metasploitable2** (Linux), що містить набір вразливих додатків.

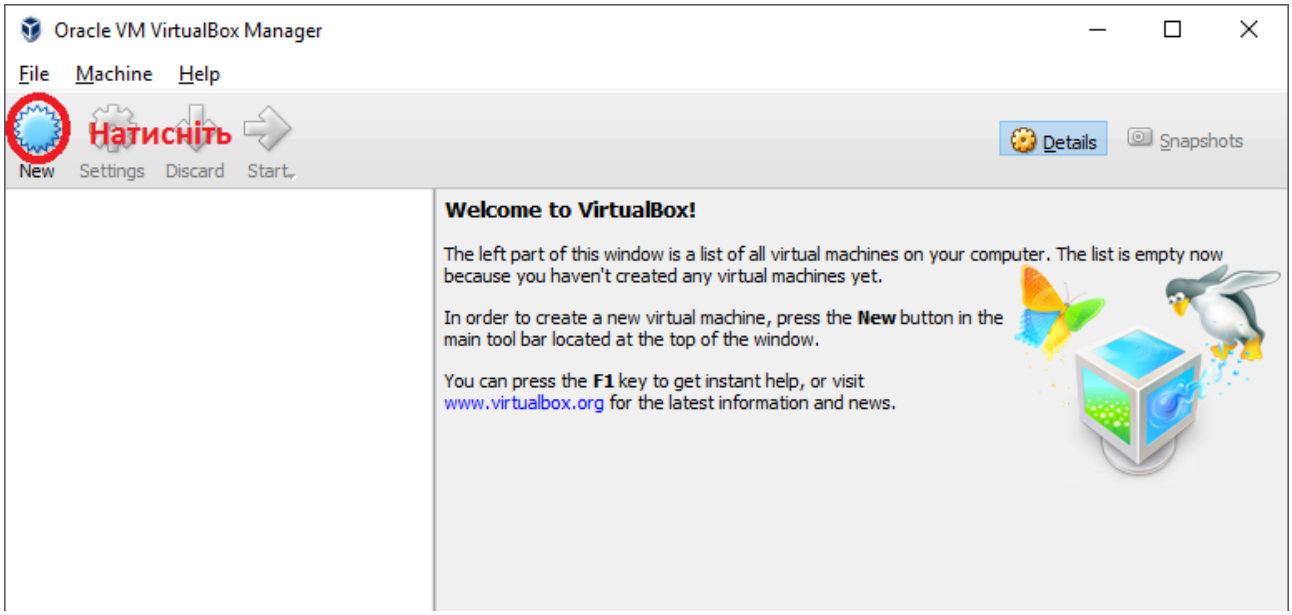
Metasploitable 2 – це спеціально підготовлена віртуальна машина, налаштована на демонстрацію максимальної кількості вразливостей за допомогою програми Metasploit Framework. Вона ідеально підходить для тренування як новачкам так і професіоналам пен-тесту.

На відміну від інших вразливих віртуальних машин, Metasploitable 2 фокусується на уразливостях в операційній системі Linux і мережевих сервісах, а не на окремих додатках. У встановленій ОС заздалегідь відкриті всі порти і присутні найбільш відомі уразливості, деякі з яких ви можете зустріти в реальному житті на діючих системах.

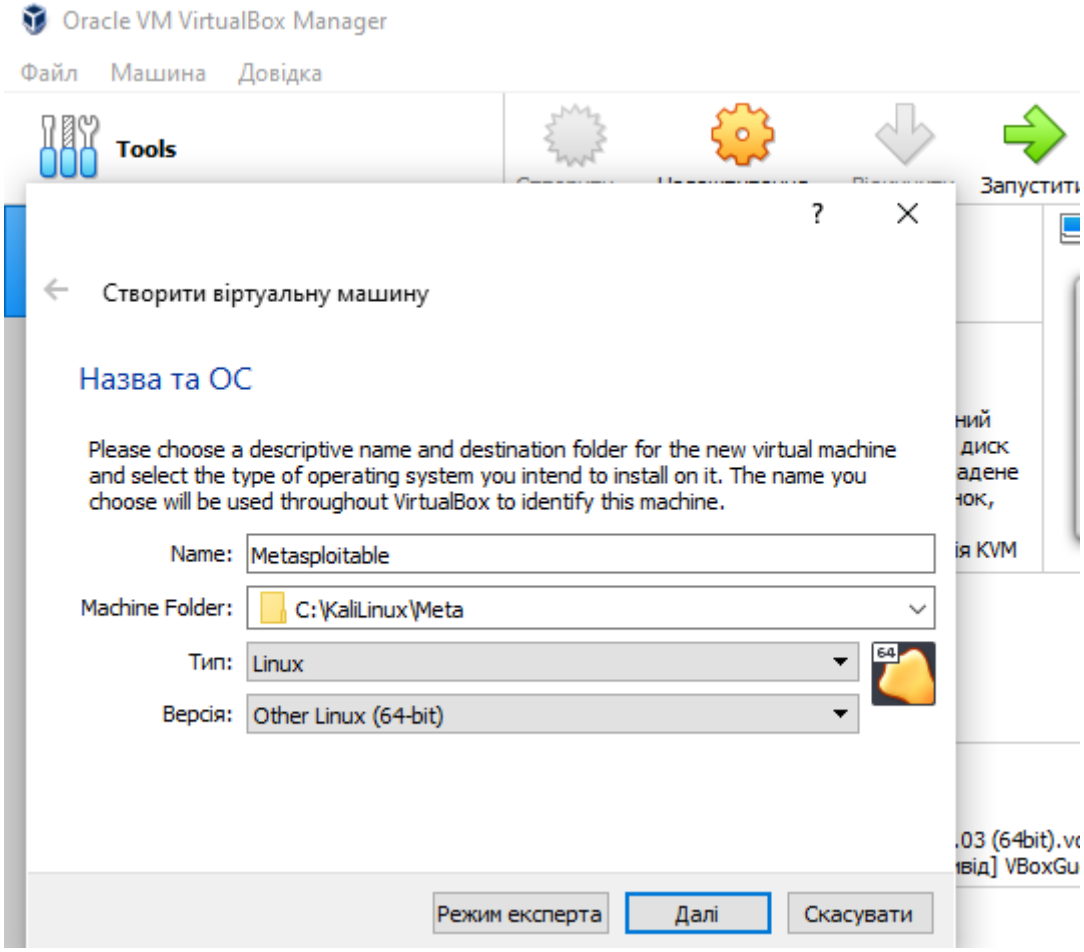
Для установки необхідно завантажити файл https://sourceforge.net/projects/metasploitable/ (~864 Мбайт). Усередині zip-архіву міститься файл з розширенням «vmdk» (Virtual Machine Disk), що містить образ Metasploitable2.

Інструкцію Metasploitable 2 Exploitability Guide можна знайти на офіційному сайті за посиланням https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

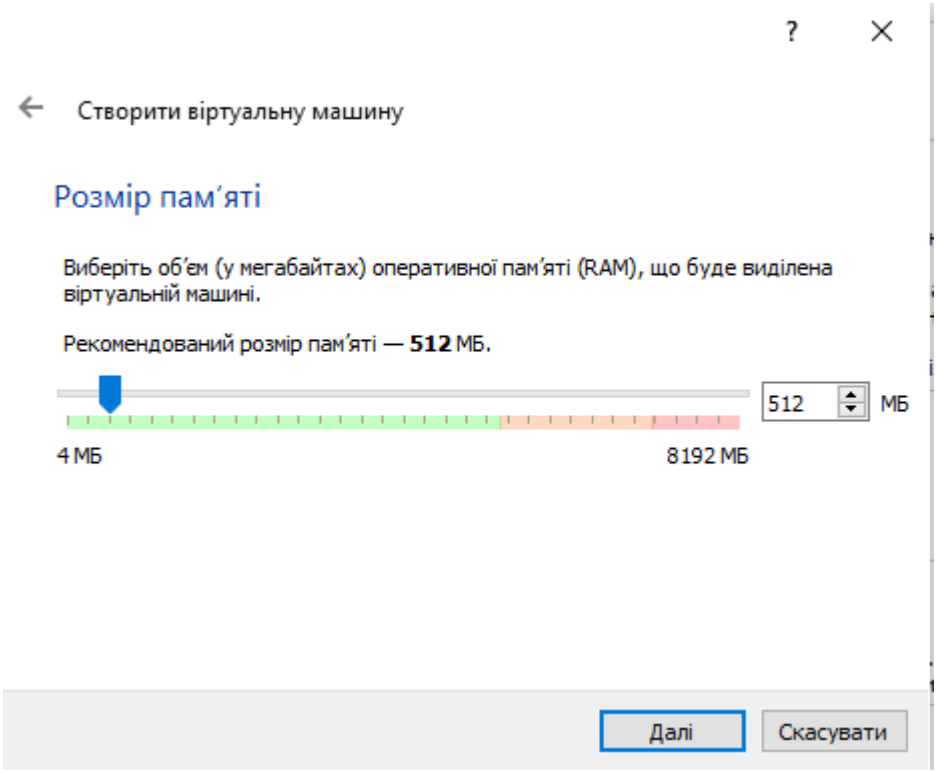
Для встановлення системи у віртуальному середовищі необхідно, для початку створити нову віртуальну машину. Для цього запустіть VirtualBox або інше відповідне ПЗ і створіть машину. Нижче на скріншотах показана послідовність створення віртуальної машини для ПЗ VirtualBox:



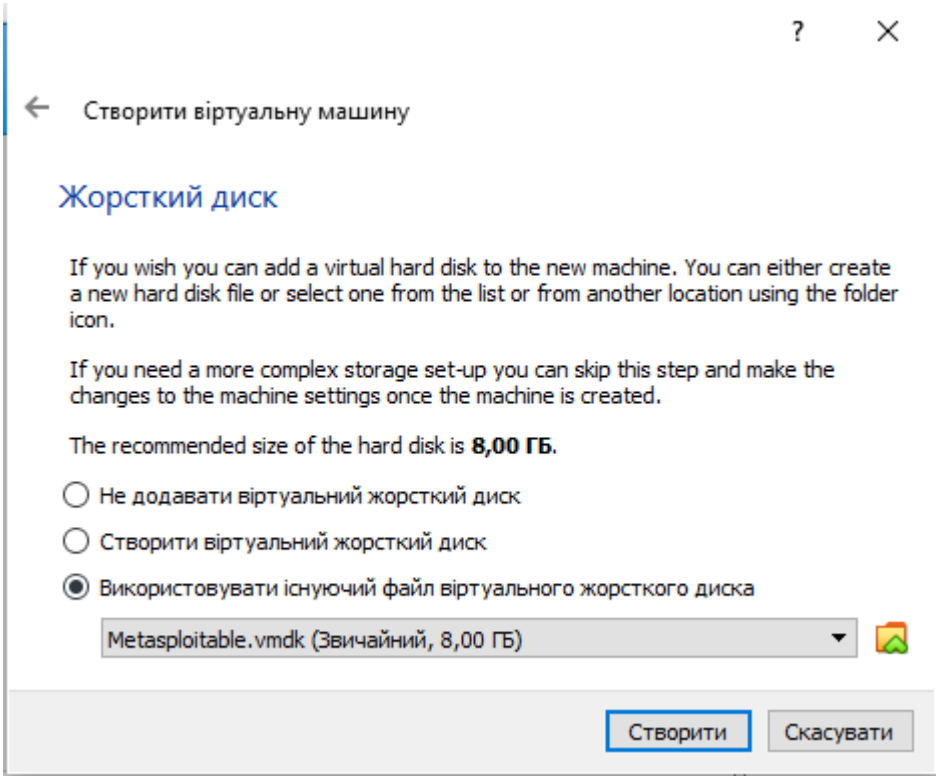
Встановіть ім'я вашої віртуальної машини, виберіть Other Linux 32 і натисніть Next (Далі):



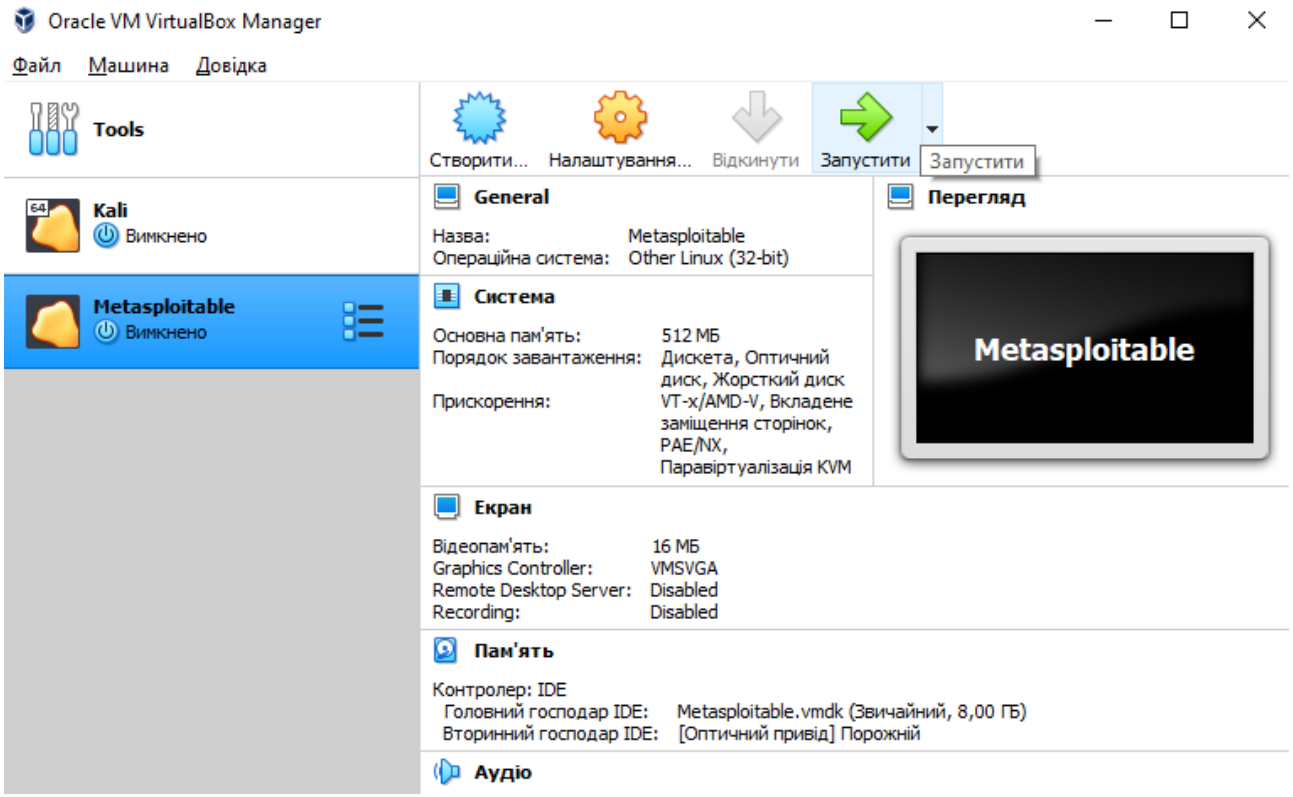
Metasploitable не потребує занадто багато пам'яті, тут ви призначаєте пам'ять для вашого віртуального пристрою і натискаєте Next (Далі).

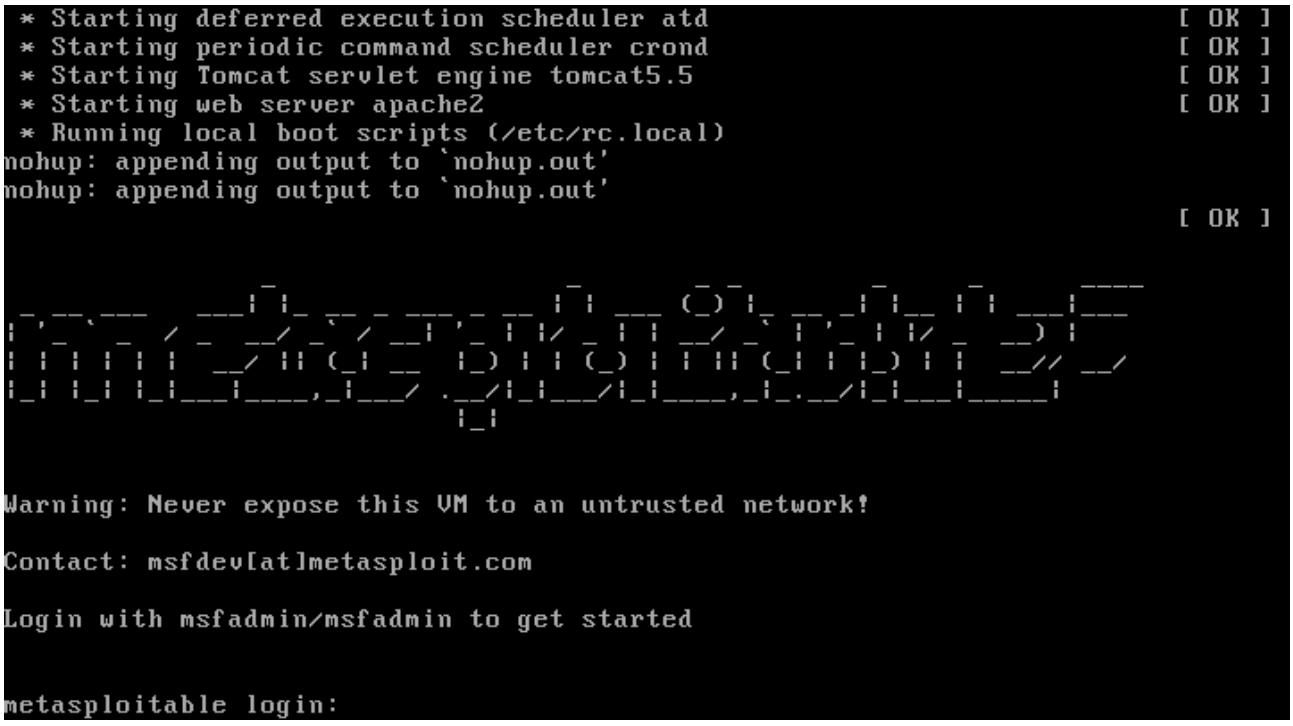


Тепер виберіть «Use an existing virtual hard drive», виберіть образ Metasploit.vmdk, який ви раніше розпакували, і натисніть «Create».



Потім запустіть вашу систему Metasploit 2 VM, вона повинна завантажитися без проблем.





Логін і пароль за замовчуванням – **msfadmin** : **msfadmin**.

Можна використовувати систему, переключаючись між віртуальною машиною та робочим столом Windows.

3) Атакуючої машиною обираємо **Kali Linux**.

Kali Linux – це дистрибутив Debian-похідних Linux, призначений для цифрової криміналістики і тестування на проникнення. Він підтримується і фінансується компанією Offensive Security Ltd. Також існує варіант для мобільних пристроїв Kali Linux NetHunter.

Kali Linux має понад 600 встановлених програм для тестування на проникнення, у тому числі Armitage (графічний інструмент управління кібератаками), Nmap (сканер портів), Wireshark (аналізатор трафіку), John the Ripper (зломщик паролів), Aircrack-ng (набір програмного забезпечення для проникнення у бездротові локальні мережі), Burp suite і OWASP ZAP (сканер безпеки веб-додатків).

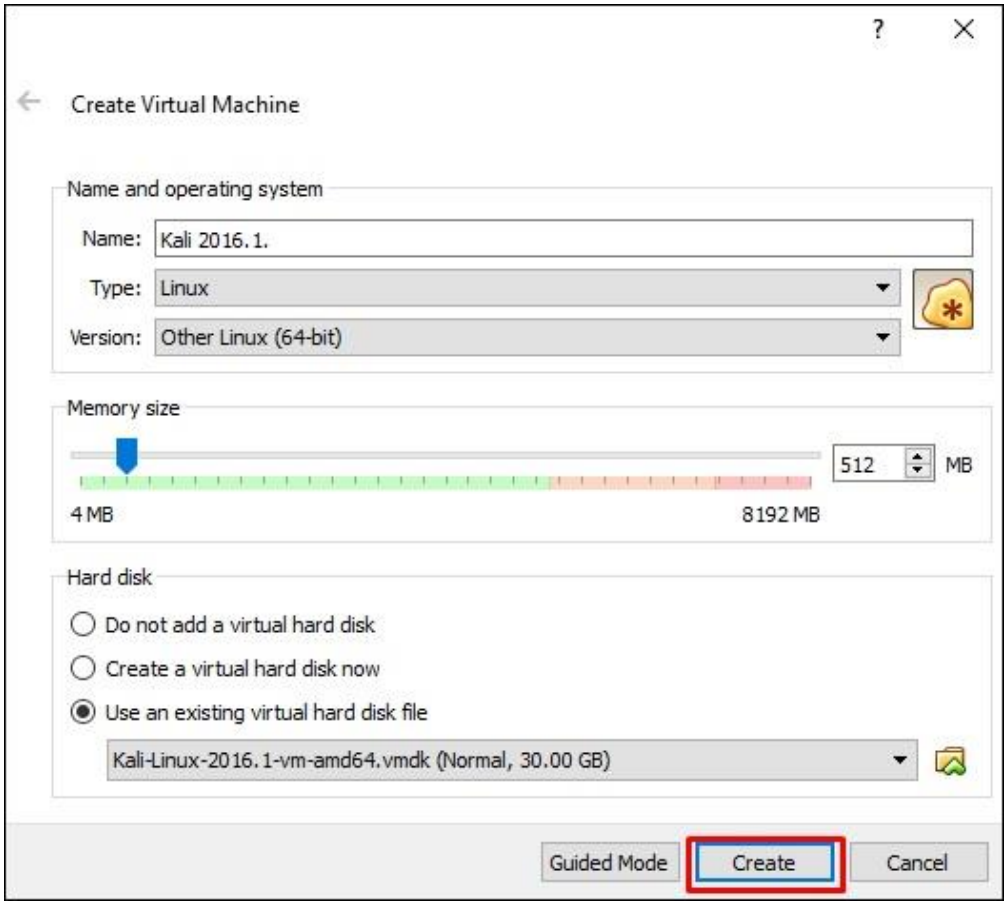
Kali Linux може працювати при установці на жорсткий диск комп'ютера, або завантажившись з Live CD або з USB-носія, також він може працювати у віртуальній машині. Це підтримувана платформа Metasploit Project з проекту Metasploit Framework, інструмент для розробки і виконання експлойтів.

Експло́йт (від англ. exploit – експлуатувати) — це комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака).

Завантажимо готовий образ віртуальної машини Kali Linux для VirtualBox з сайту https://www.osboxes.org/kali-linux/

Для економії місця на диску вибираємо найменший доступний дистрибутив **Kali Linux 2017.3** (VirtualBox (VDI) 64bit Size: 2.08GB). Після розархівації завантаженого файлу 7.0364.7z отримуємо файл Kali Linux 2017.03 (64bit).vdi розміром більше 10 Гбайт.

Створюємо нову віртуальну машину у VirtualBox аналогічно як на попередньому кроці.



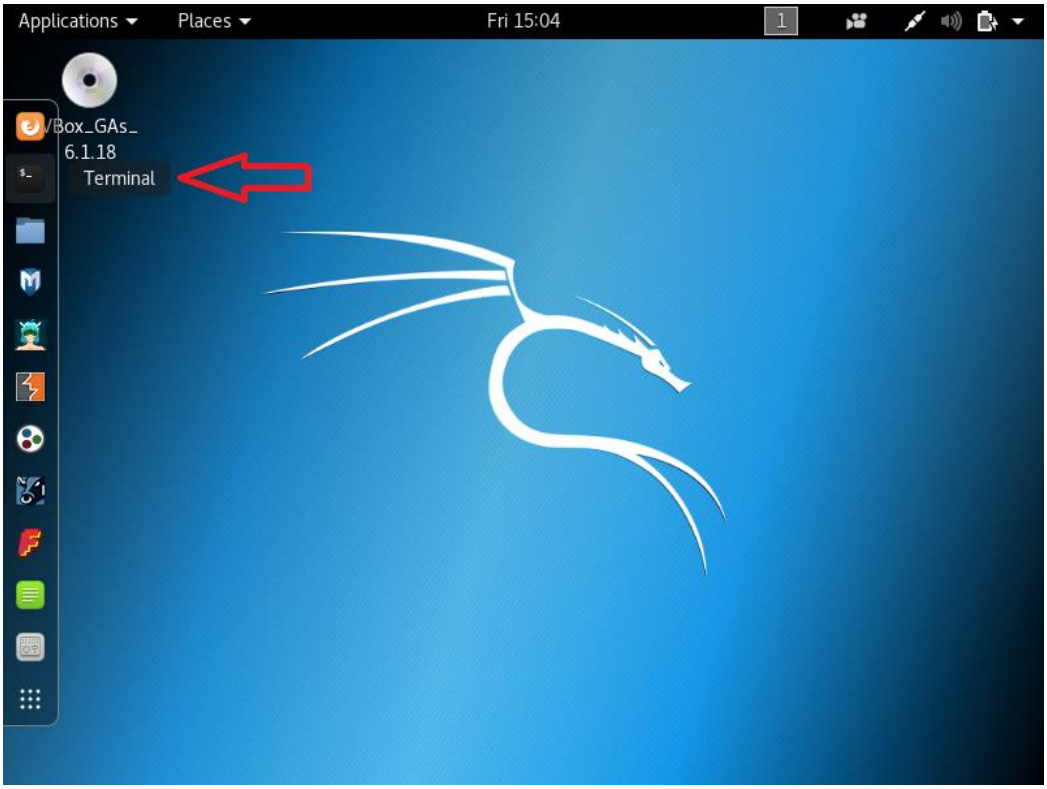
Запустіть Kali OS. Ім'я користувача за замовчуванням - root, а пароль - toor.

Проте, у нашій версії з сайту https://www.osboxes.org/kali-linux/ ім'я користувача – **root**, а пароль – **osboxes.org.**

Як збільшити роздільну здатність екрану Virtualbox

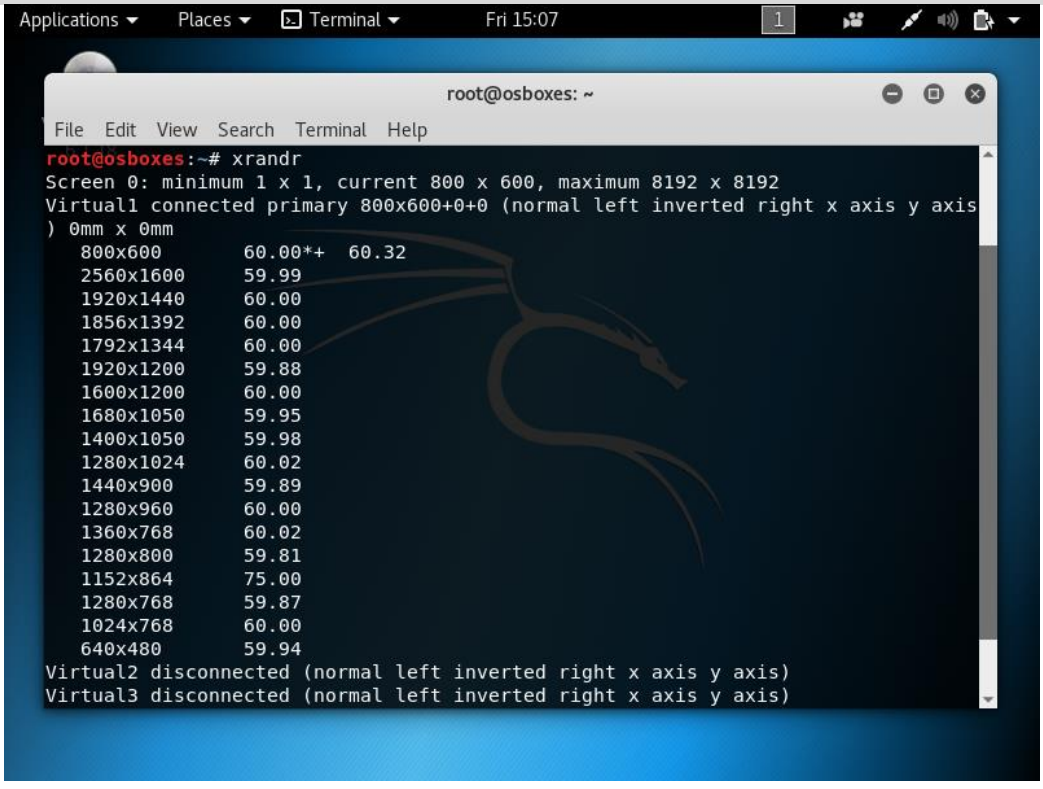
Один зі способів – за допомогою утиліти **xrandr**. Вона дозволяє змінювати налаштування екрану, і в тому числі роздільну здатність.

Запускаємо термінал:



Спочатку дивимося доступні варіанти роздільної здатності екрану:

```
xrandr
```



Далі щоб змінити розмір екрану Virtualbox достатньо виконати:

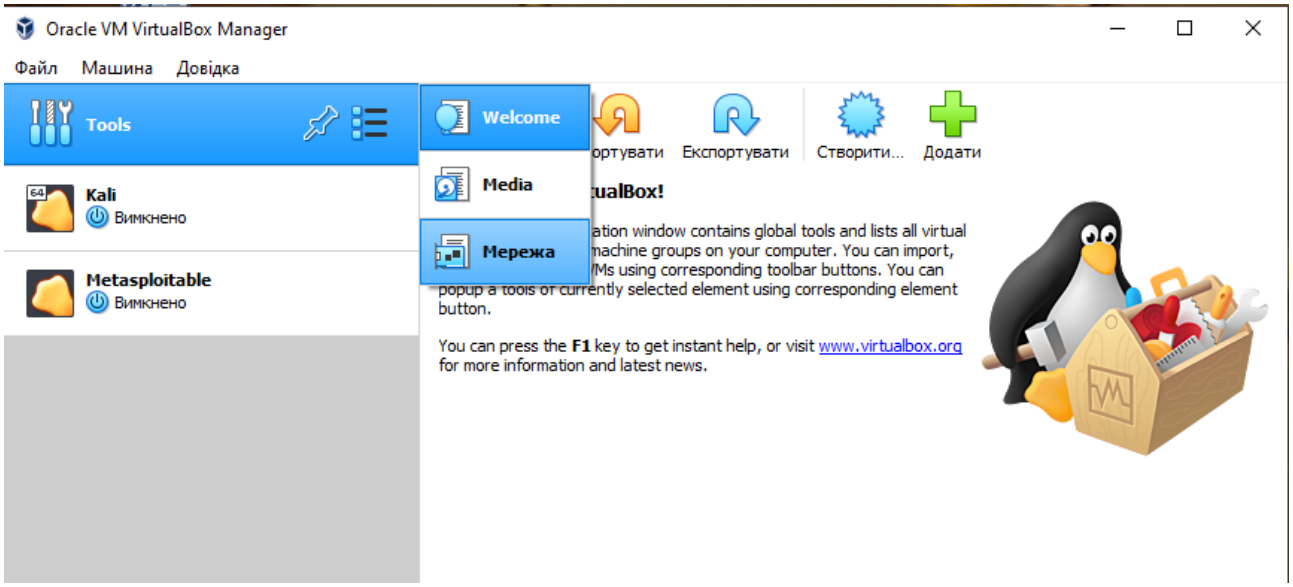
```
xrandr -s 1280x800
```

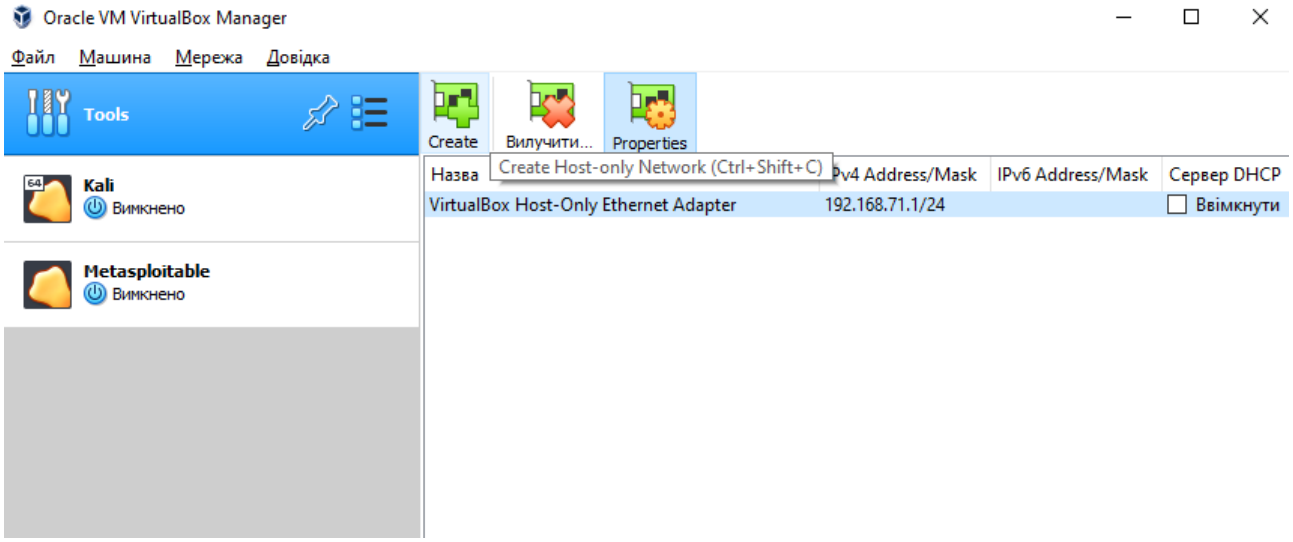
Для того, щоб ***оновити Kali Linux***:

виконати від користувача root наступні команди (це може зайняти деякий тривалий час, оскільки потребує завантаження файлів):

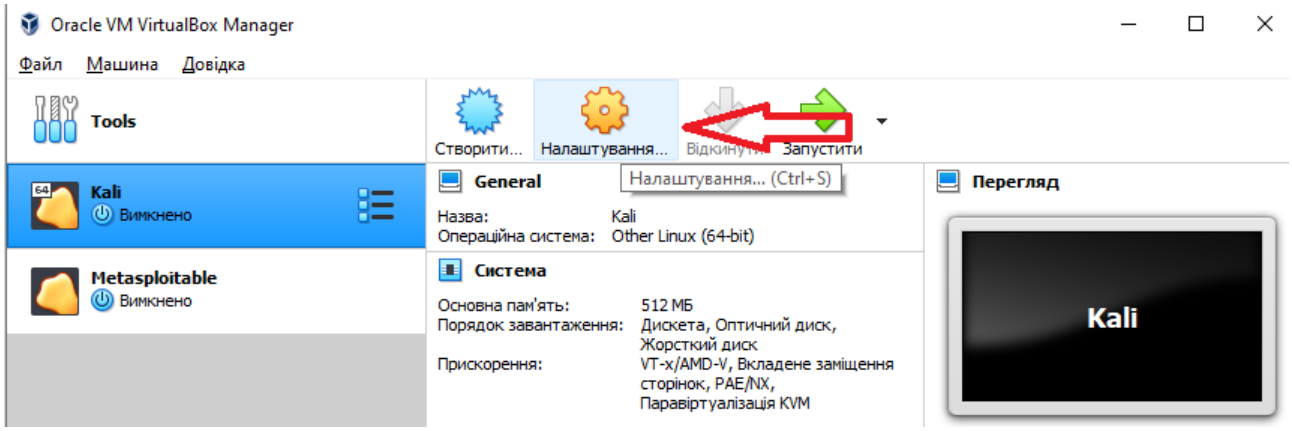
```
apt-get update
apt-get dist-upgrade
```

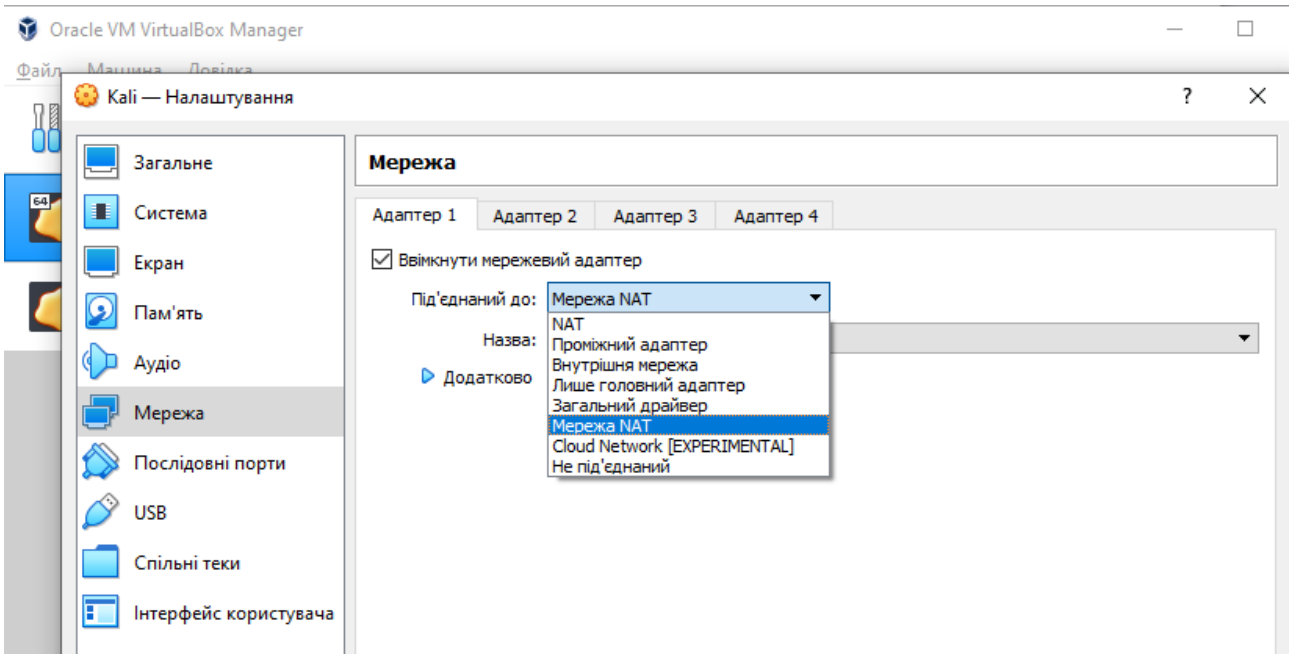
4) Для завершення налаштування інфраструктури необхідно **конфігурувати мережу** таким чином, щоб віртуальні машини бачили одна одну. Для цього у вкладці «Мережа» налаштувань Virtualbox натиснути зелений + і створити NAT мережу (Network Adress Translation – механізм в мережах, побудованих з використанням TCP / IP протоколу, що перетворює IP-адреси транзитних пакетів):





Далі для кожної віртуальної машини необхідно вибрати тип підключення «NAT».



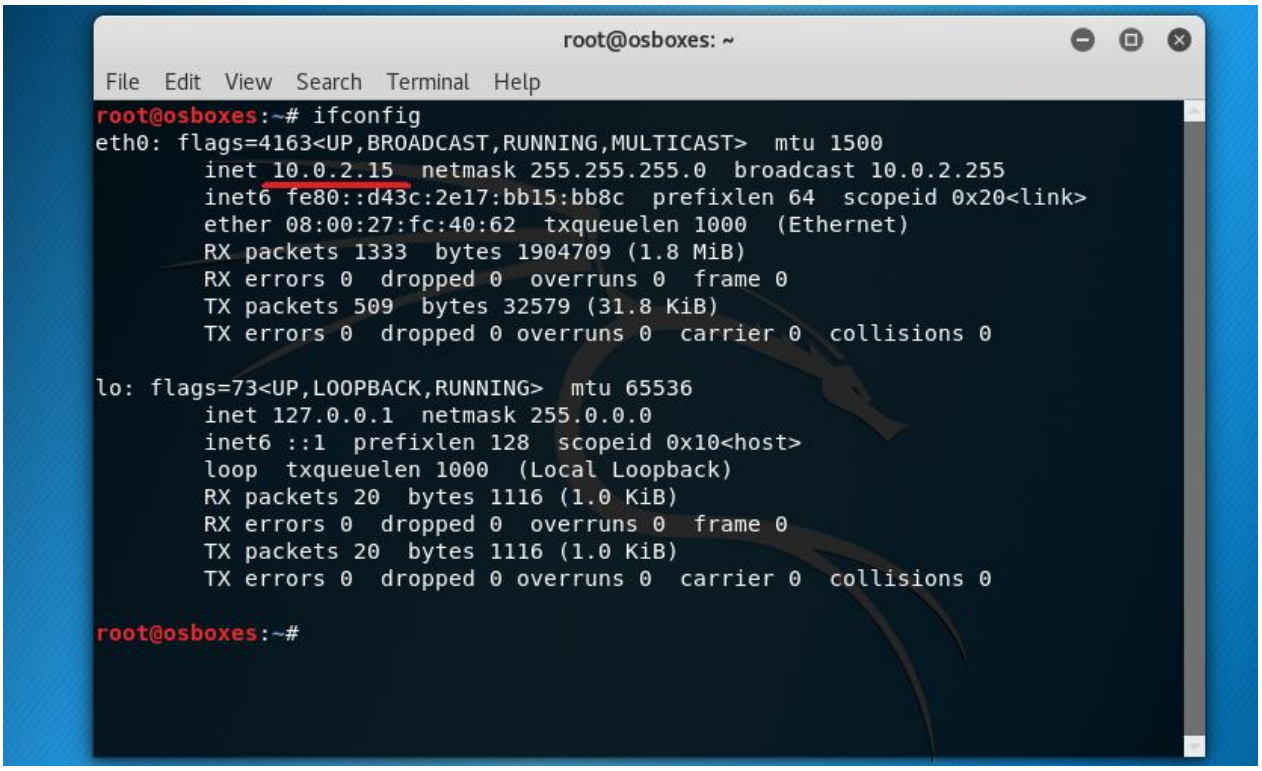


Виконавши команду **ifconfig** отримаємо дані про ip-адресу кожної віртуальної машини у нашій мережі:

- для Metasploit2: 10.0.2.4 (*у Вас адреса напевно буде іншою*)

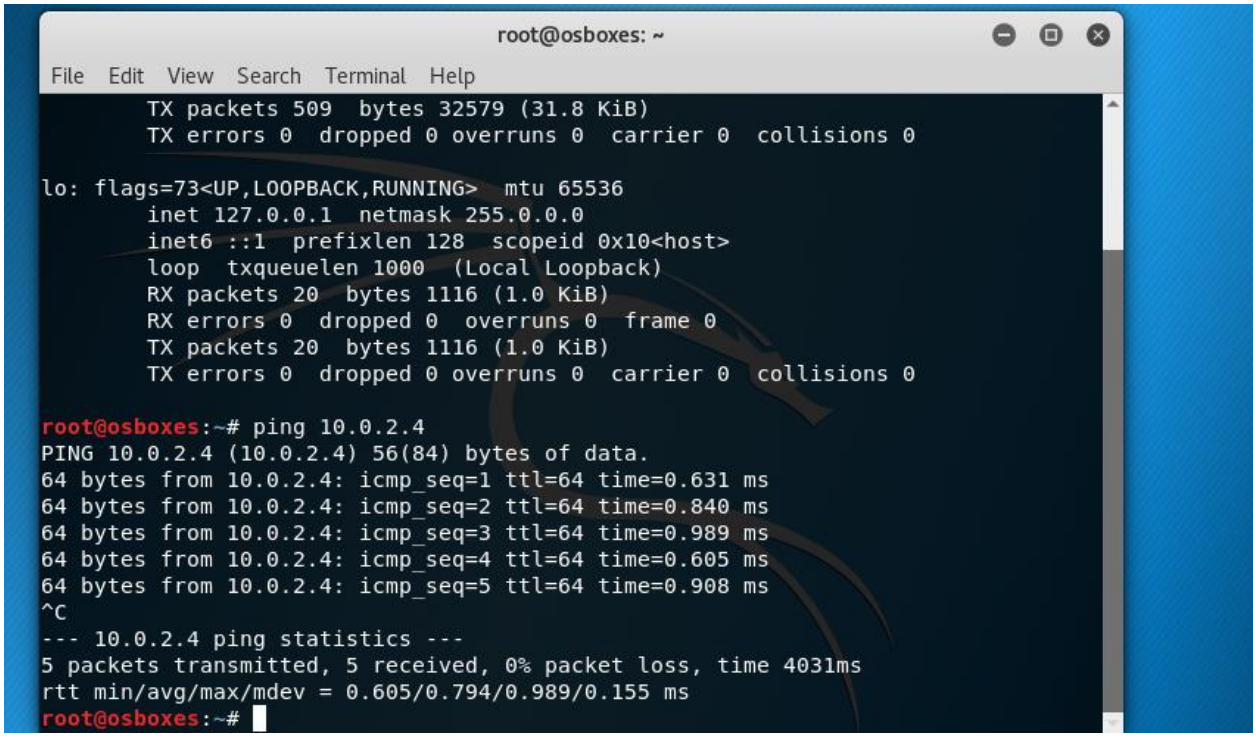
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d9:86:5e
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed9:865e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4092 (3.9 KB)  TX bytes:6076 (5.9 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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

- для Kali Linux: 10.0.2.15 (*у Вас адреса напевно буде іншою*)



Перевіримо доступ з машини Kali Linux до машини «жертви» (використаємо ip-адресу Metasploitable отриману на попередньому кроці):

виконаємо команду **ping 10.0.2.4**



Щоб зупинити **ping** натисніть клавіші **Ctrl + C**.

2. Мережеві перерахування

Перерахування мережі – це процес, який включає збір інформації про таку мережу, як хости, підключені пристрої, а також імена користувачів, групову інформацію та супутні дані. Використовуючи протоколи, такі як ICMP та SNMP, перерахування мережі забезпечує кращий огляд мережі для цілей захисту або злому.

Інструменти мережевого перерахування сканують порти для збору інформації. Вони також можуть брати відбитки пальців операційної системи. Все це робиться для того, щоб більш уважно ознайомитися з тим, як налаштована мережа та як обробляється трафік даних.

Деякі IT-спеціалісти називають перерахування мережі частиною "етичного злому" для роботи з безпеки. Деякі сканери вразливості можуть здійснити перерахування мережі, щоб спробувати захистити комп'ютерну систему. Ідея полягає в тому, що при перерахуванні мережі можна виявити вразливості, які потім можуть бути використані адміністраторами мережі / системи для виправлення системи або хакерами для атаки на ту саму.

Існує велика кількість різноманітних засобів та методів збору технічної інформації, однак, найбільш поширеним з них є **nmap**. Для nmap було розроблено графічний інтерфейс – **zenmap**.

Nmap ("Network Mapper") це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча прекрасно справляється і з одиничними цілями. Nmap використовує IP-пакети з вкладеними заголовками TCP-сегментів оригінальними способами, щоб визначити, які хости доступні в мережі, які служби (назва програми та версіz) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів / брандмауерів використовуються і ще десятки інших характеристик. У той час як Nmap зазвичай використовується для перевірки безпеки, багато системних адміністраторів вважають її корисною для звичайних завдань, таких як контролювання структури мережі, управління розкладами запуску служб і облік часу роботи хоста або служби.

Синтаксис запуску програми наступний:

```
Nmap [Scan type(s)] [options] {target specification}

nmap [<тип сканування>] [<Опції>] {<ціль сканування>}
```

де замість [Scan type (s)] вказується тип сканування (за замовчуванням, якщо це місце залишити порожнім, Nmap буде відкрито сканувати доступні порти). Як [options] вводяться різноманітні ключі і параметри сканування, а замість {target specification} - або IP-адреса комп'ютера, або діапазон IP-адрес (який визначається маскою підмережі), або назву хоста.

Описи типів сканування

-sT – сканування TCP портів в звичайному режимі. Якщо з'єднання з віддаленим портом встановлено, то даний порт відкритий, інакше порт закритий або фільтрується.

-sS – використання методу TCP SYN. Це так зване стелс сканування. Nmap відправляє на віддалений порт SYN-пакет і чекає на відповідь. Залежно від відповіді визначається стан порту. При цьому повноцінне з'єднання не встановлюється. Завдяки цьому визначити факт сканування дуже складно. Для запуску цього методу потрібні привілеї адміністратора на Вашому комп'ютері.

-sF, -sX, -sN (scan FIN, scan Xmas, scan NULL) – ці спільні методи використовують, наприклад, якщо не допомогло -sS або -sT сканування.

-sU – сканування UDP портів. На віддалений порт відправляється UDP-пакет і очікується відповідь. Якщо відповідь містить ICMP-повідомлення «порт недоступний» означає порт закритий або захищений файрволом, інакше порт відкритий.

-sR – використання RPC-сканування (RPC - віддалений виклик процедури). Цей метод дозволяє визначити програму, яка обслуговує RCP-порт і її версію. При цьому, якщо на віддаленому сервері встановлений файрвол, Nmap може його «пробити», не залишаючи логів.

-sP – ping-сканування. Даний метод дозволяє дізнатися всі адреси активних хостів в мережі. Якщо Ви пінгуєте мережі краще не вказувати більше ніяких методів сканування.

Описи деяких опцій

Опції служать для тонкого налаштування сканування та завдання додаткових функцій. Опції не обов'язкові, робота сканера буде нормальною і без них.

-O – режим «зняття відбитків» TCP / IP для визначення віддаленої ОС (OS fingerprints). Працює це таким чином: Nmap відправляє віддаленій системі запити і в залежності від відповідей («відбитків» стека) визначається ОС і її версія.

-p [діапазон] – сканування певного діапазону портів.

-F – сканування стандартних портів (1-1024) записаних в файл services. Це, так зване, швидке сканування.

-P0 – скасування ping-опитувань перед скануванням портів хоста. Корисна в тих випадках, якщо Ви бажаєте сканувати мережі типу microsoft.com, так як в них ICMP-запит заборонений файрволом.

-6 – сканування через протокол IPv6. працює значно швидше ніж через IPv4.

-T «Paranoid | Sneaky | Polite | Normal | Aggressive | Insane» – настройка часових режимів. При «Paranoid» сканування триватиме дуже довго, але тоді у Вас більше шансів залишитися не виявленими скан-детекторами. І, навпаки, «Insane» використовується при скануванні швидких або слабо захищених мереж.

-D «host_1, host_2, ..., host_n» – це дуже корисна функція. Вона дозволяє заплутати віддалену систему і створити видимість що її сканують з декількох хостів («host_1, host_2, ..., host_n»), тим самим намагаючись приховати Вашу реальну адресу.

Варто зауважити що інструмент nmap настільки потужний що має свою скрипкову мову – NSE, яка дозволяє організовувати дуже складні механізми збору інформації.

Стани портів які розпізнаються Nmap

Відкритий (open)

Додаток приймає запити на TCP з'єднання або UDP пакети на цей порт. Виявлення цього стану зазвичай є основною метою сканування. Люди, котрі розуміються на безпеці, знають, що кожний відкритий порт це прямий шлях до здійснення атаки. Атакуючі хочуть використовувати відкриті порти, а адміністратори намагаються закрити їх або захистити за допомогою брандмауерів так, щоб не заважати роботі звичайних користувачів. Відкриті порти також цікаві з точки зору сканування, не пов'язаного з безпекою, тому що вони дозволяють визначити служби доступні в мережі.

Закритий (closed)

Закритий порт доступний (він приймає і відповідає на запити Nmap), але не використовується якимось додатком. Вони можуть бути корисні для встановлення, що по заданій IP адресі є працюючий хост, або для визначення ОС. Оскільки ці порти досяжні, може бути корисним провести сканування пізніше, тому що деякі з них можуть відкритися.

Фільтрується (filtered)

Nmap не може визначити, чи порт відкритий, тому що фільтрація пакетів не дозволяє досягти запитам Nmap цього порту. Фільтрація може здійснюватися виділеним брандмауером, правилами роутера або брандмауером на цільовій машині. Ці порти не приносять користі для атакуючих, тому що надають дуже мало інформації.

Не фільтрується (unfiltered)

Цей стан означає, що порт доступний, але Nmap не може визначити, відкритий він чи закритий.

Відкритий | Фільтрується (open | filtered)

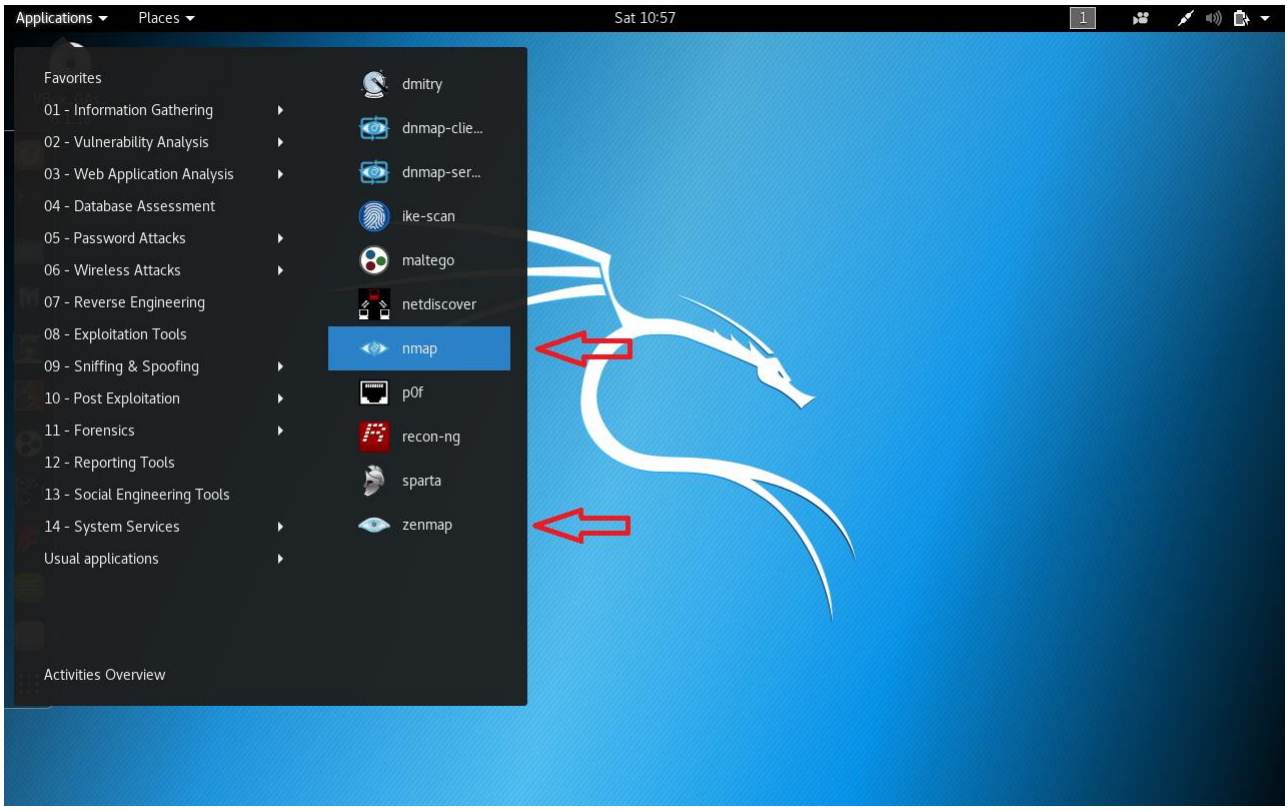
Nmap характеризує порт таким станом, коли не може визначити чи відкритий порт чи фільтрується.

Закритий | Фільтрується (closed | filtered)

Це стан використовується, коли Nmap не може визначити, чи закритий порт чи фільтрується.

Тепер давайте підемо крок за кроком і дізнаємося, як використовувати **NMAP** і **ZenMAP**.

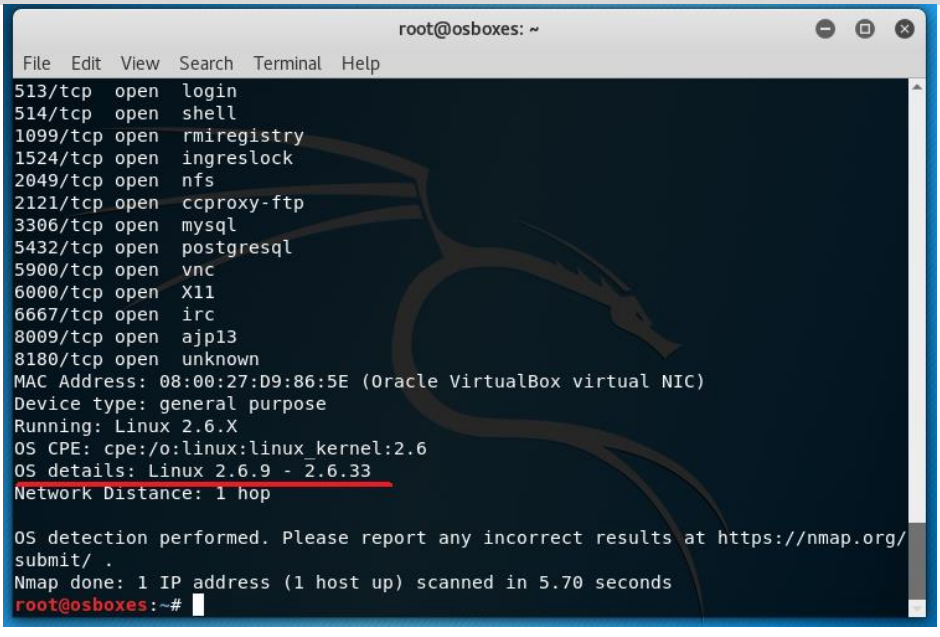
Крок 1 – Щоб відкрити, перейдіть в Програми → 01-Збір інформації → nmap або zenmap.



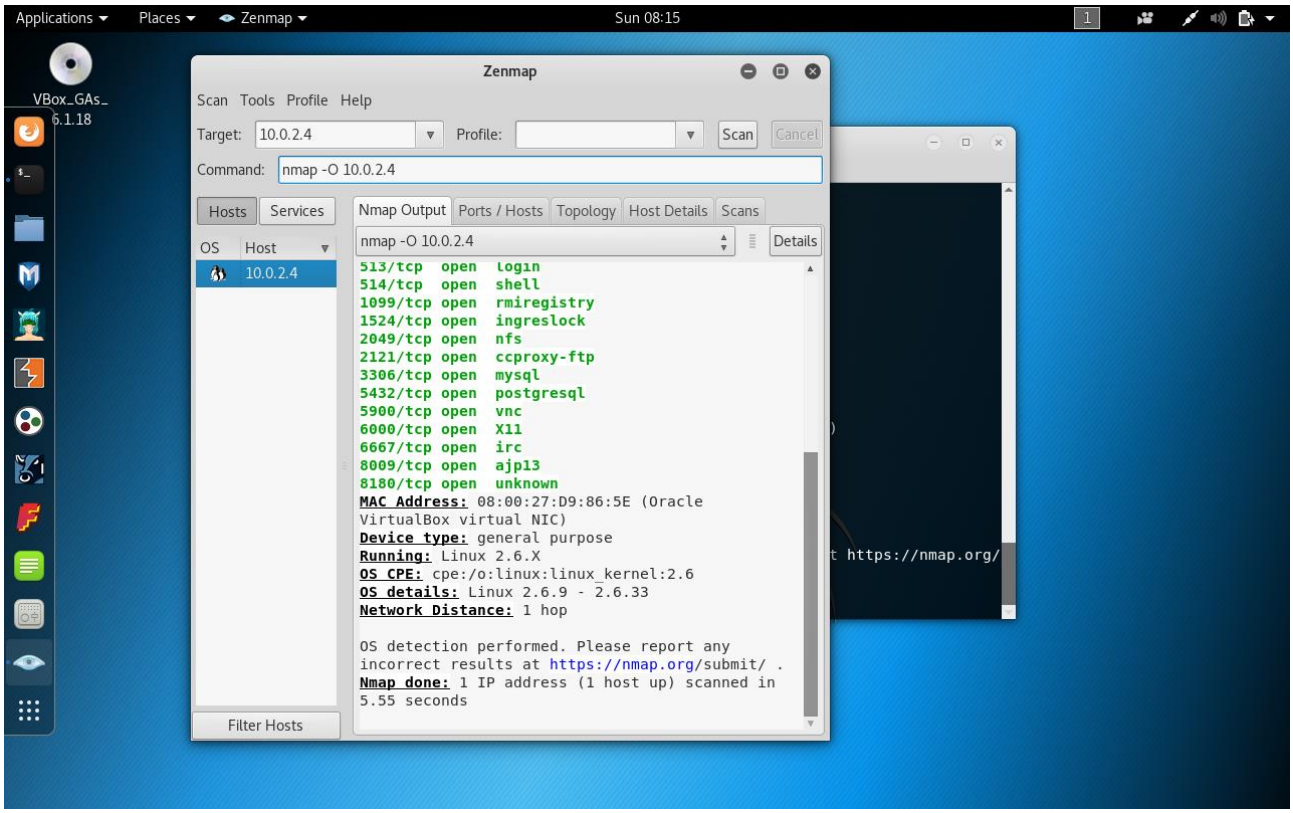
Крок 2 - Наступним кроком є визначення типу / версії ОС цільового хоста. Параметр визначення типу / версії ОС є змінною «-O».

Команда, яку ми будемо використовувати,

```
nmap -O 10.0.2.4
```

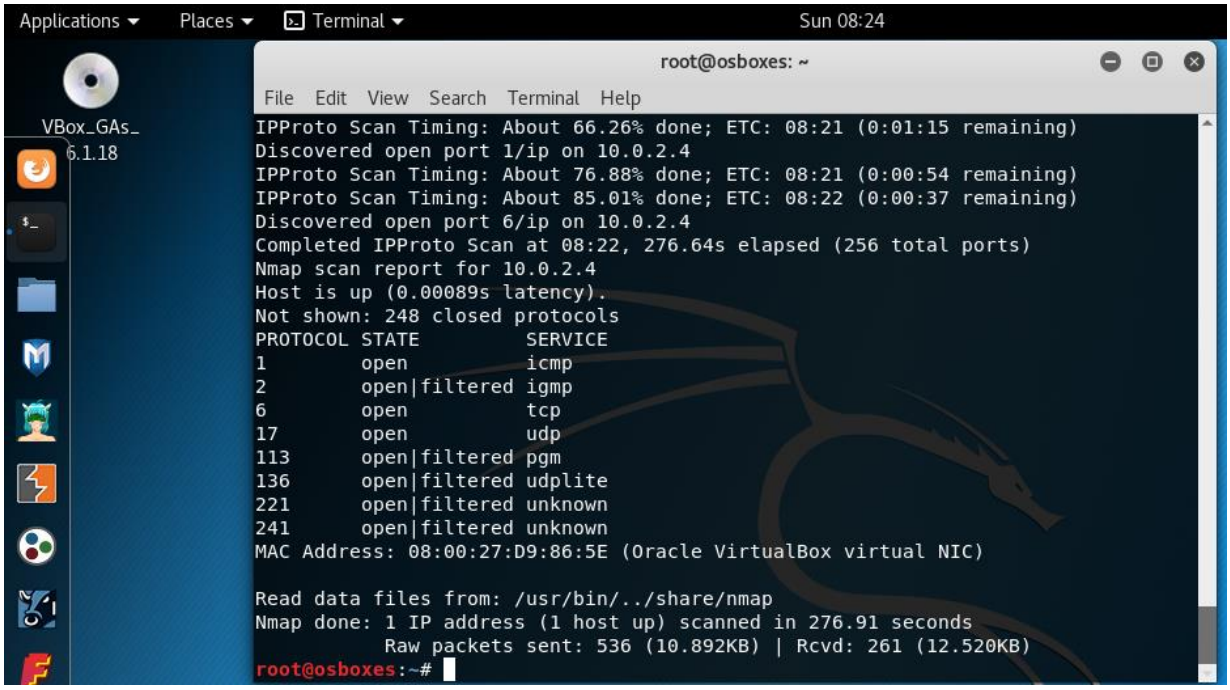


На наступному скріншоті показано, де вам потрібно ввести вищевказану команду у **ZenMAP**, щоб побачити вивід Nmap:



Крок 3. Визначення переліку протоколів, які підтримуються

```
nmap -sO -v -n 10.0.2.4
```

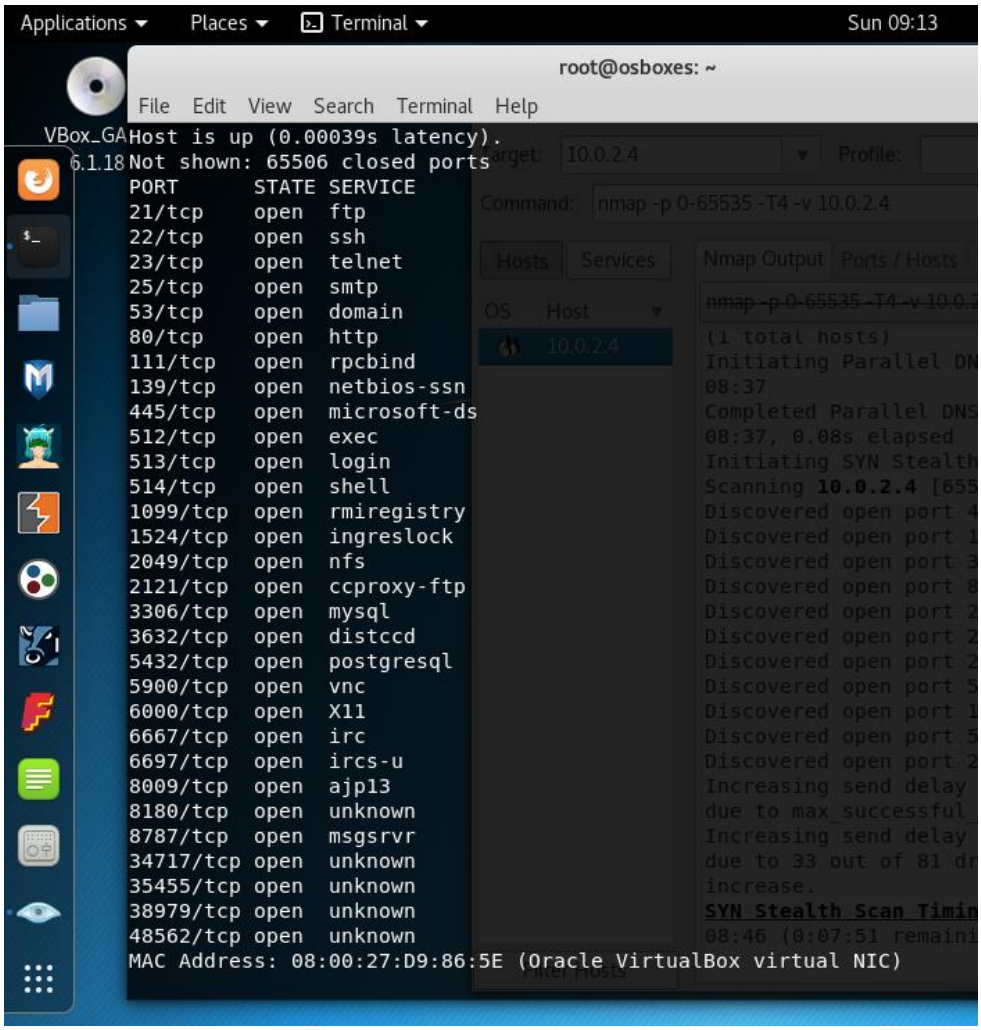


Крок 4. Щоб просканувати всі порти TCP на основі NMAP, використовуйте наступну команду

```
nmap -p 1-65535 -T4 -v 10.0.2.4
```

Де параметр «-p» вказує всі порти TCP, які повинні бути перевірені. В цьому випадку ми скануємо всі порти, і «-T4» - це швидкість сканування, на якій повинен працювати NMAP, «-v» – виводить поточні результати на екран.

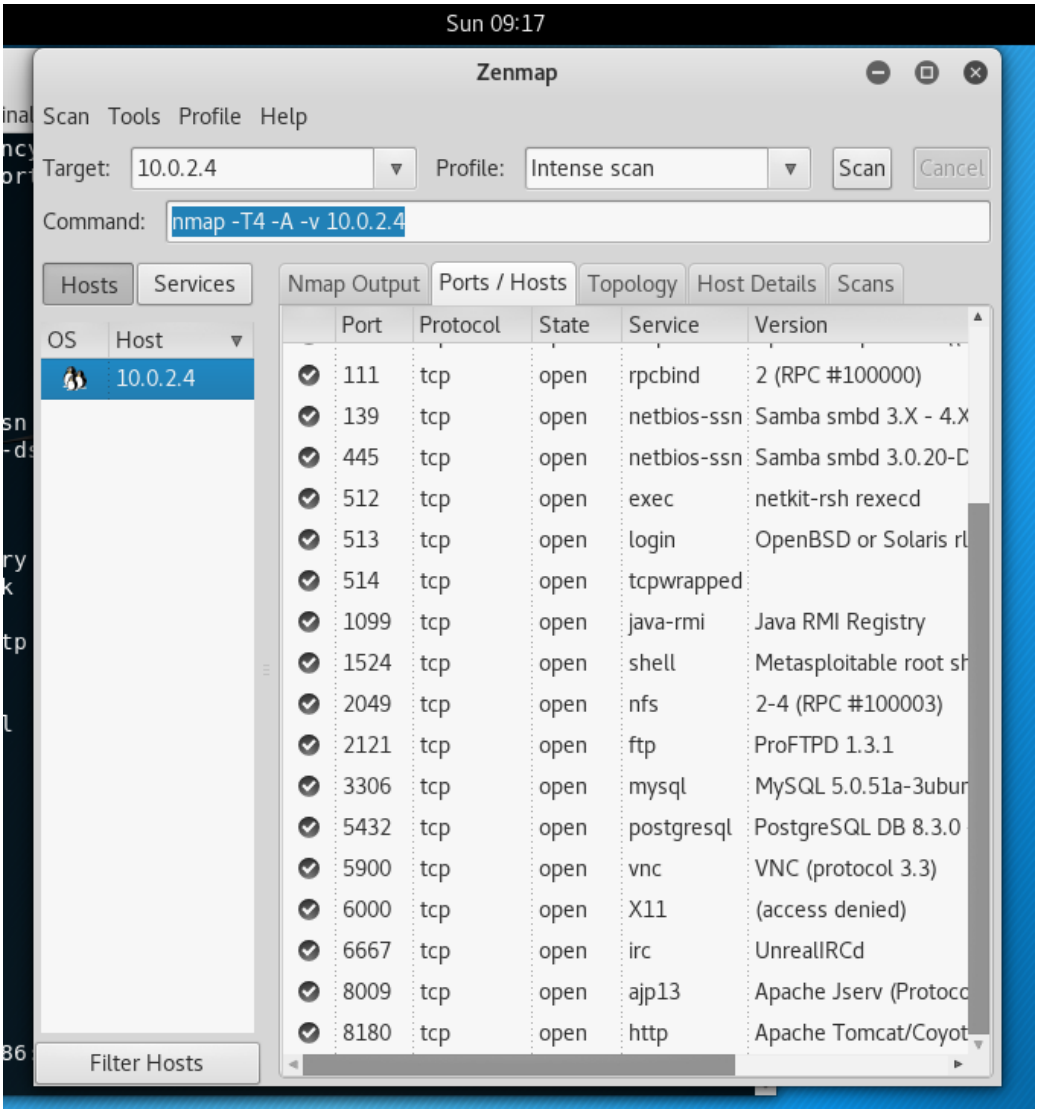
Після завершення сканування утиліта Nmap видає інформацію про стан портів, що дозволяє зробити висновок про те, що в Metasploitable 2 існує велика кількість вразливостей і можливі різні вектори атак. Майже кожен з відкритих портів дозволяє виконати віддалений вхід в систему.



Подібний результат отримаємо запустивши zenmap із командою за замовчуванням

```
nmap -T4 -A -v 10.0.2.4
```

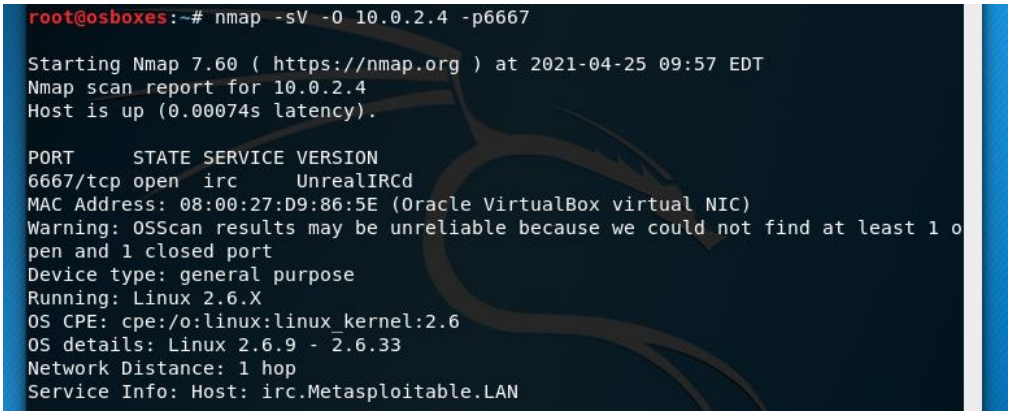
На рисунку нижче демонструється закладка «Порти» утиліти zenmap:



Ми бачимо, що в цільовій системі є багато відкритих портів та служб, включаючи FTP, SSH, HTTP та MySQL. Ці служби можуть містити вразливі місця, якими ви можете скористатися.

Крок 5. Тепер переходимо до детального сканування одного з портів для отримання більш докладної інформації.

Після сканування порту 6667, на якому знаходиться сервіс IRC, можна зробити висновок, що встановленою версією є UnrealIRCD IRC.

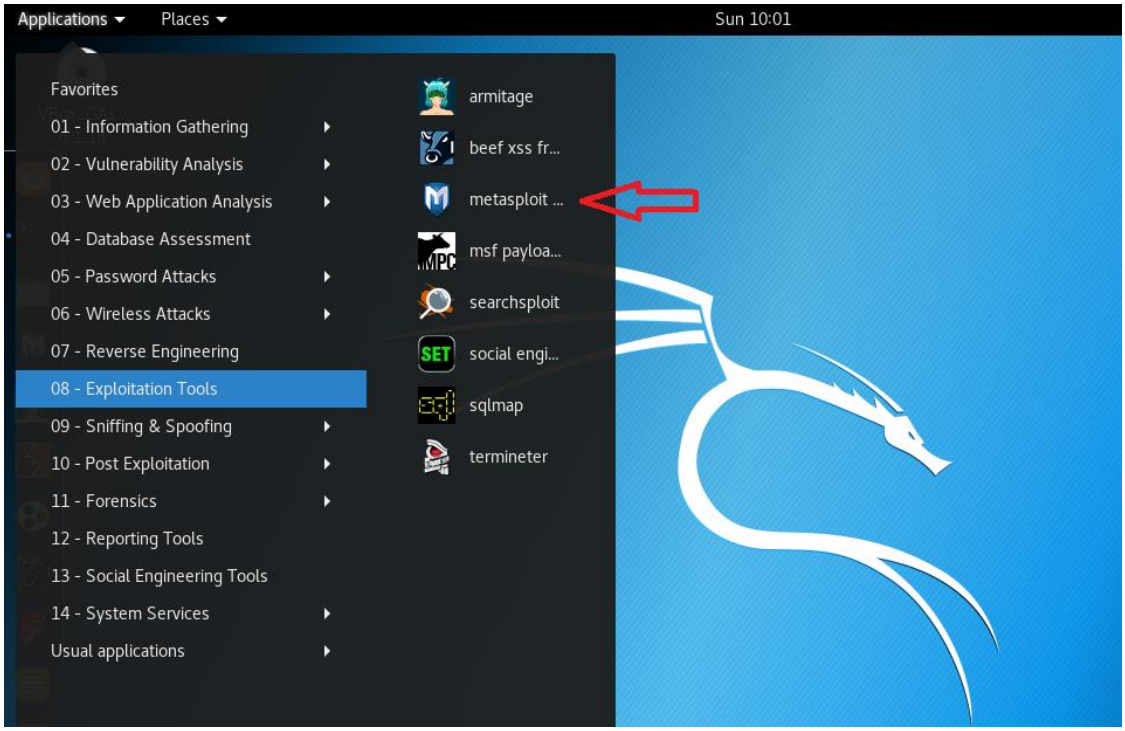


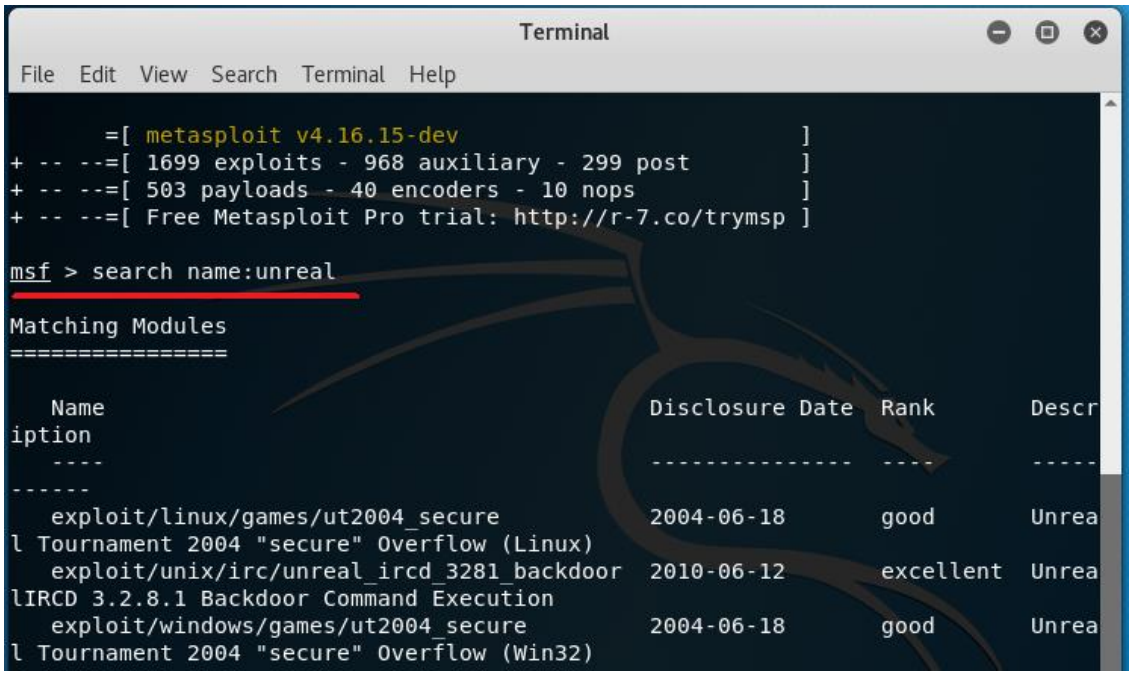
Ця версія містить бекдор, який довгий час залишався непоміченим для фахівців з ІБ. він запускається відправкою букв «AB», які слідують за системної командою на сервер. Даний бекдор можна реалізувати за допомогою **Metasploit framework**.

Metasploit – один з найпотужніших інструментів, які використовуються для тестування на проникнення.

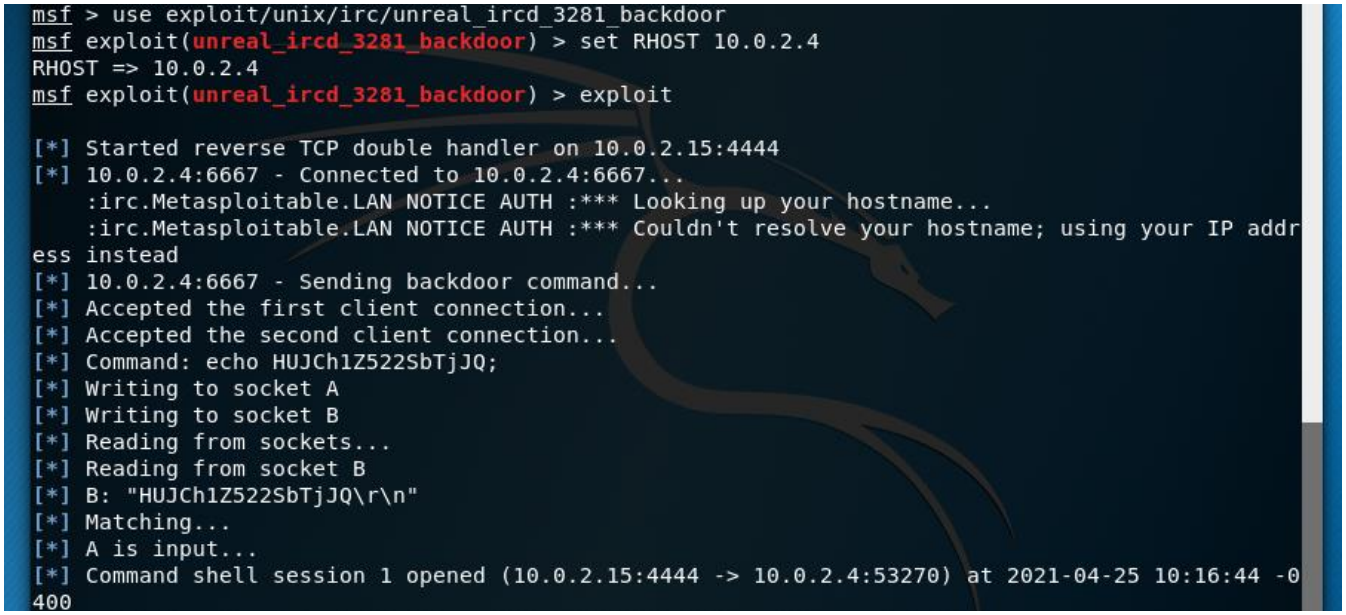
Алгоритм дій містить наступні кроки:

1. Пошук в базі Metasploit framework потрібного експлойта;
2. Вибір і налаштування експлойта;
3. Проведення атаки.

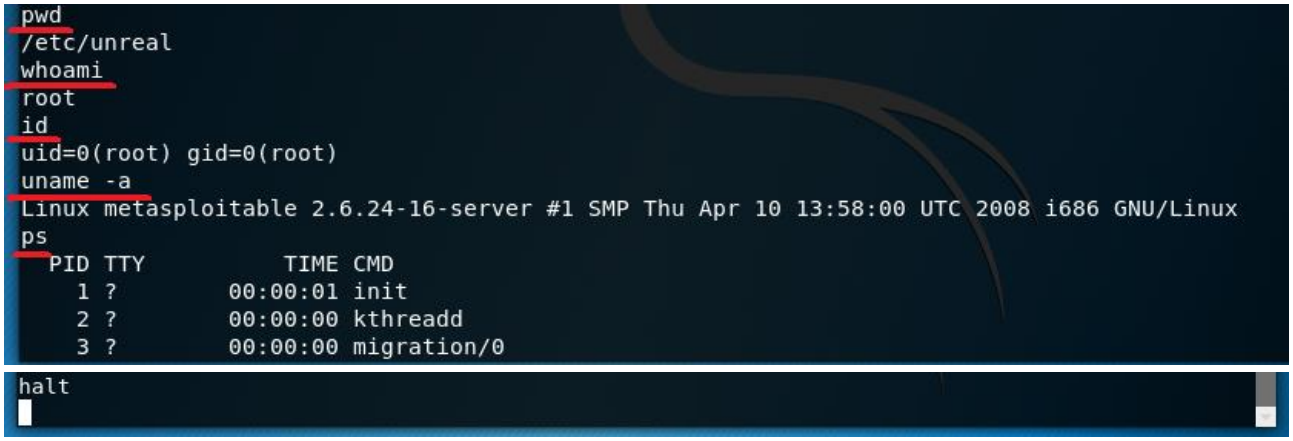




Після запуску експлойта можна спостерігати процес зараження і отримання доступу до атакованого комп'ютера.



Бачимо, що було відкрито сеанс командної стрічки, де ви можете запускати всі unix команди, і застосовувати їх проти цільової машини.



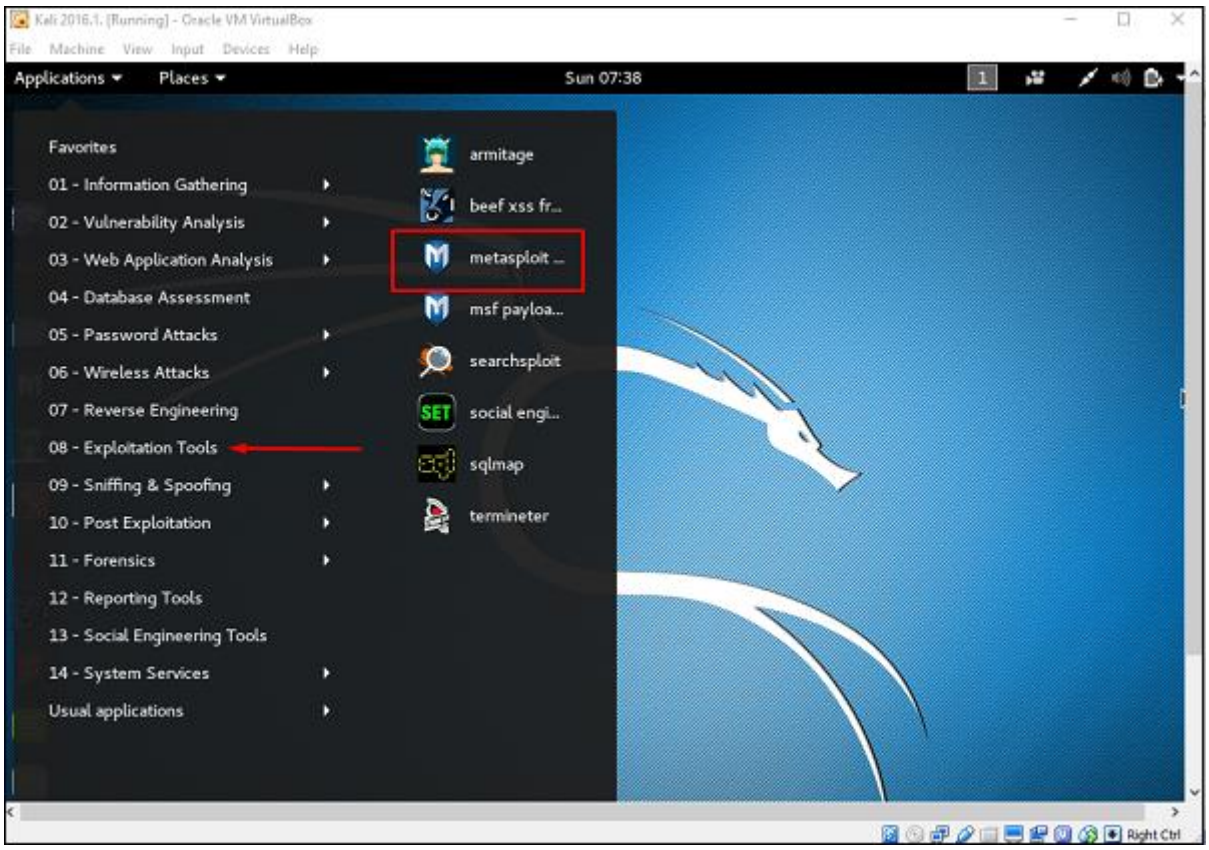
3. Metasploit Framework

Metasploit – один з найпотужніших інструментів, які використовуються для тестування на проникнення. Більшість його ресурсів можна знайти за адресою - www.metasploit.com. Він поставляється в двох версіях: комерційна і безкоштовна.

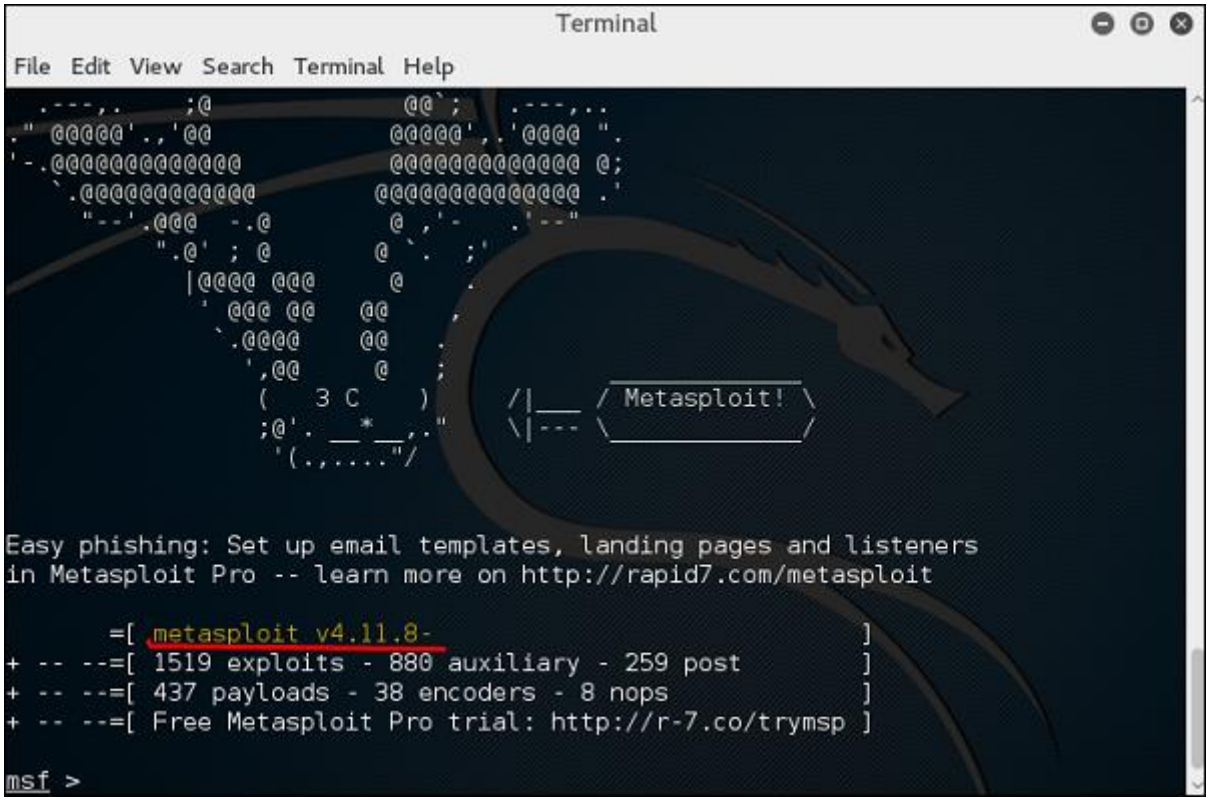
Як етичний хакер, ви будете використовувати «Kali Distribution», в яку вмонтована безкоштовн версія Metasploit разом з іншими інструментами етичного злому. Але якщо ви хочете встановити Metasploit як окремий інструмент, ви можете легко зробити це в системах, що працюють на Linux, Windows або Mac OS X.

У цьому розділі ми обговоримо деякі основні команди, які часто використовуються в Metasploit.

Перш за все, відкрийте консоль Metasploit в Калі. Ви можете зробити це, пройшовши по шляху: Програми → Інструменти експлуатації → Metasploit.

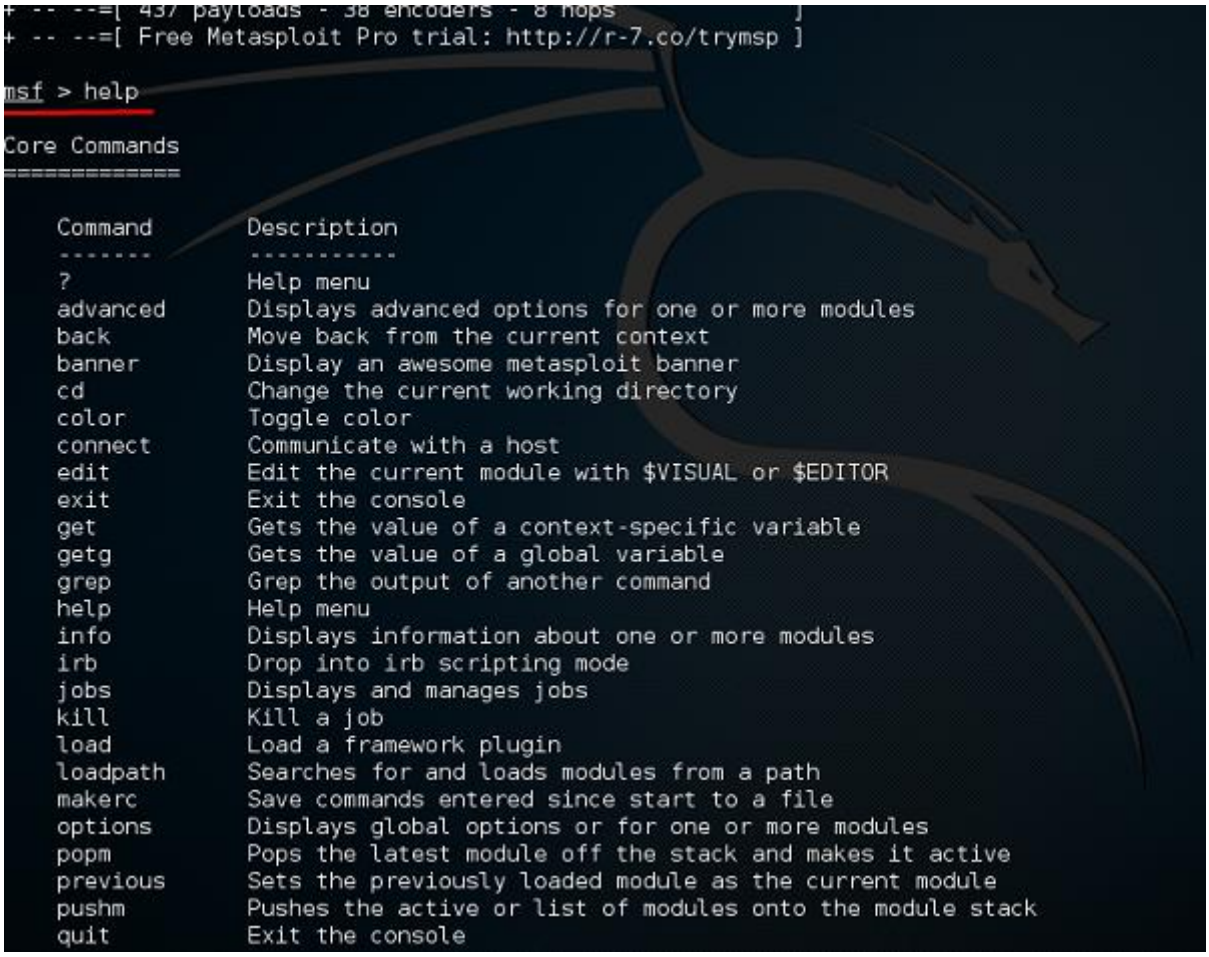


Відкривши консоль Metasploit, ви побачите наступний екран. Підкреслене червоним показує версію Metasploit.



Команда help

Якщо ви введете команду **help** в консолі, вона покаже вам список основних команд в Metasploit разом з їх описом.



Команда msfupdate

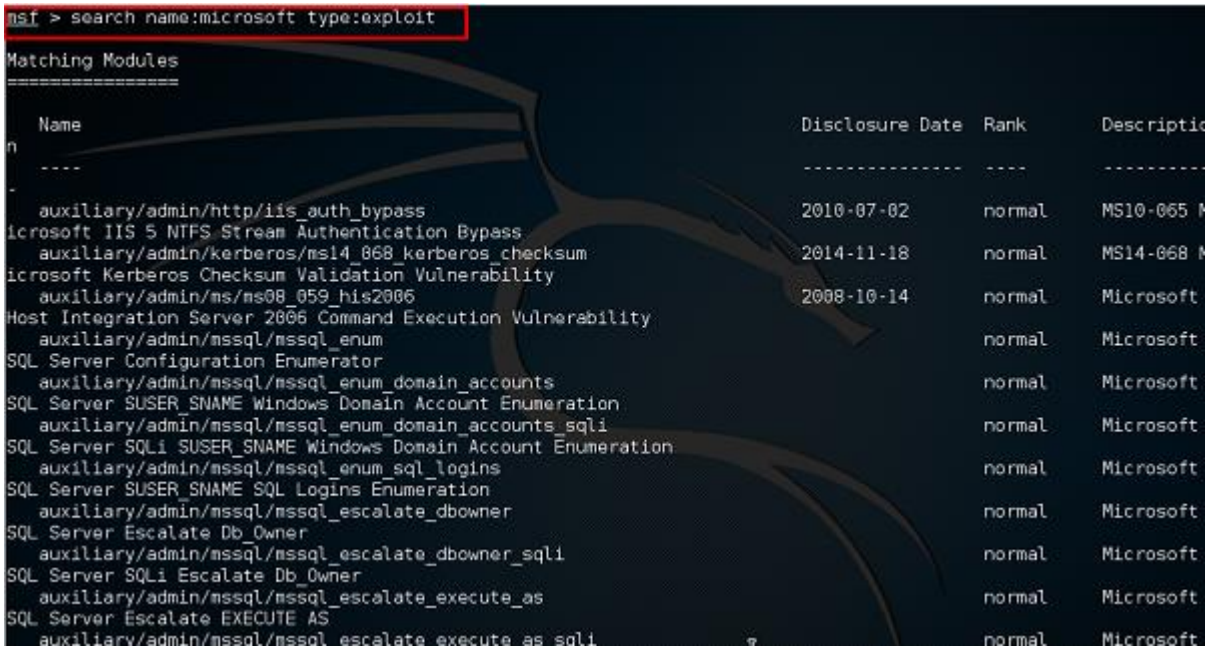
msfupdate – важлива адміністративна команда. Вона використовується для поновлення Metasploit найновішими вразливостями. Після виконання цієї команди вам доведеться почекати кілька хвилин до завершення оновлення.

Команда пошуку

Наприклад, якщо ви хочете знайти експлойти, пов'язані з Microsoft, то команда буде такою:

```
msf >search name:Microsoft type:exploit
```

Тут **search** – це команда, name – це ім'я об'єкта, який ви шукаєте, а type – це тип сценарію, який ви шукаєте.



Команда інформації

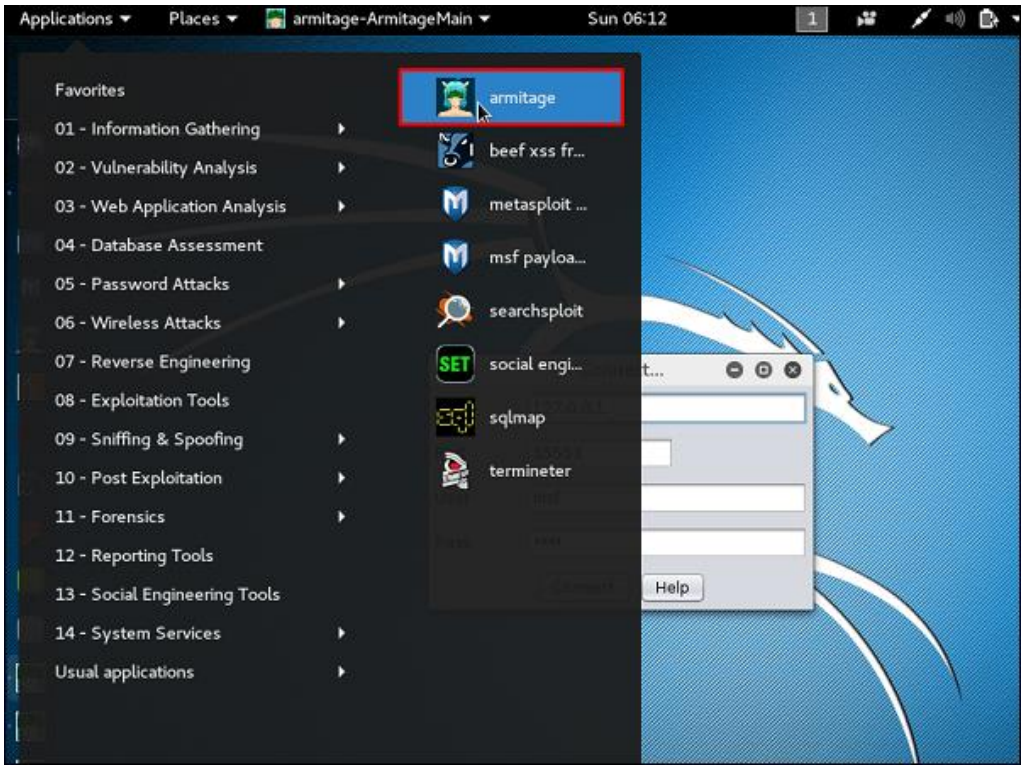
Команда **info** надає інформацію про модуль або платформу, наприклад, про те, де він використовується, хто є автором, посилання на вразливість і обмеження корисного навантаження.

```
f auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass

     Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
   Module: auxiliary/admin/http/iis_auth_bypass
  License: Metasploit Framework License (BSD)
     Rank: Normal
Disclosed: 2010-07-02

ovided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

sic options:
Name       Current Setting  Required  Description
----       ---------------  --------  -----------
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOST                       yes       The target address
RPORT      80               yes       The target port
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /                yes       The URI directory where basic auth is enabled
VHOST                       no        HTTP server virtual host

scription:
This module bypasses basic authentication for Internet Information
Services (IIS). By appending the NTFS stream name to the directory
name in a request, it is possible to bypass authentication.

ferences:
http://cvedetails.com/cve/2010-2731/
http://www.osvdb.org/66160
http://technet.microsoft.com/en-us/security/bulletin/MS10-065
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation
```

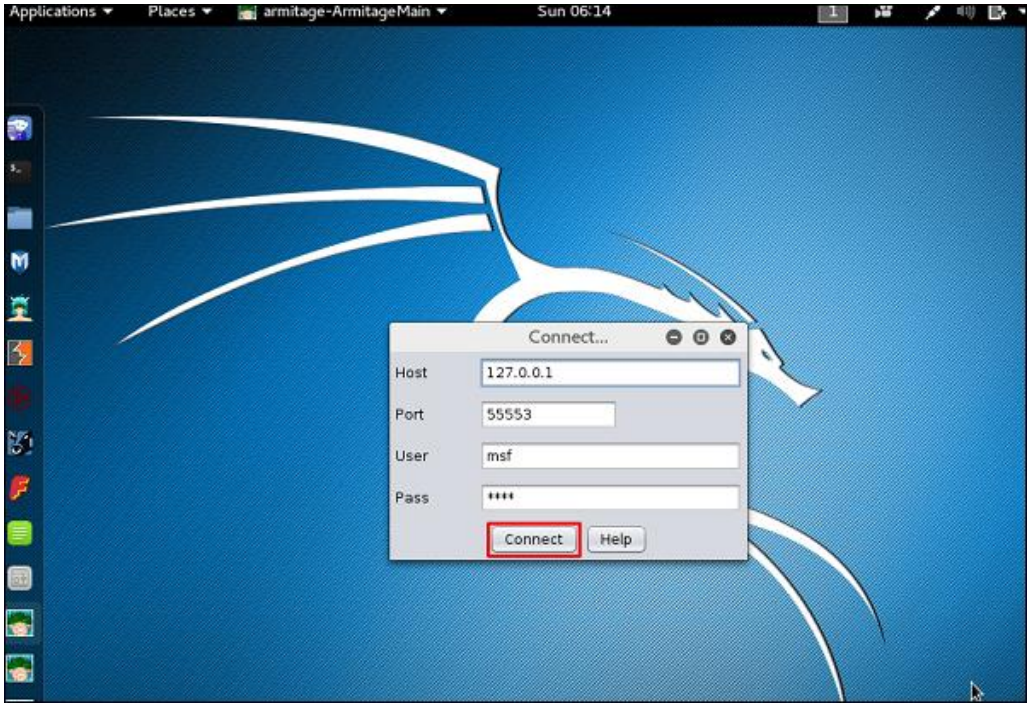
Metasploit – Armitage GUI

У цьому підрозділі ми побачимо, як використовувати графічний інтерфейс Armitage для Metasploit. Armitage - це додатковий інструмент для Metasploit. Він візуалізує цілі, рекомендує експлойти і надає розширені функції після експлуатації. Armitage включений в дистрибутив Kali. Якщо вам необхідно пройти тестування на проникнення, вам доведеться використовувати обидва інструменти разом.

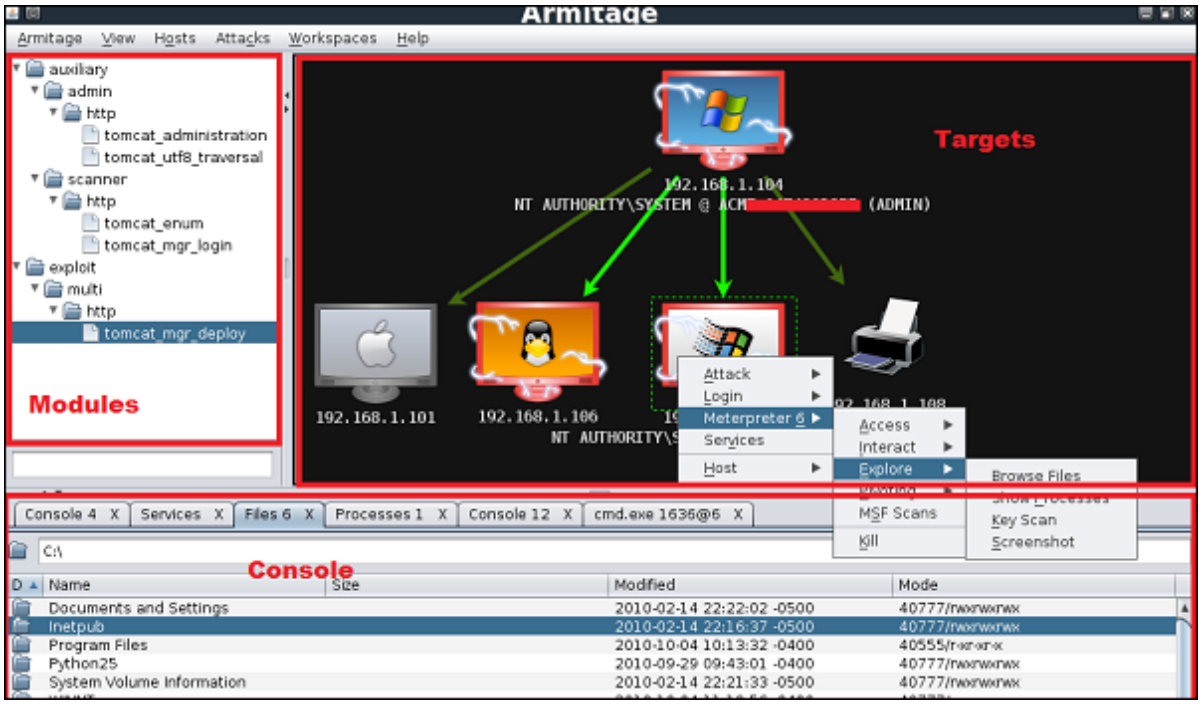
Спочатку відкрийте консоль Metasploit і перейдіть в Програми → Інструменти для експлойтів → Armitage.



Введіть необхідні дані як на наступному екрані і натисніть «Підключитися».



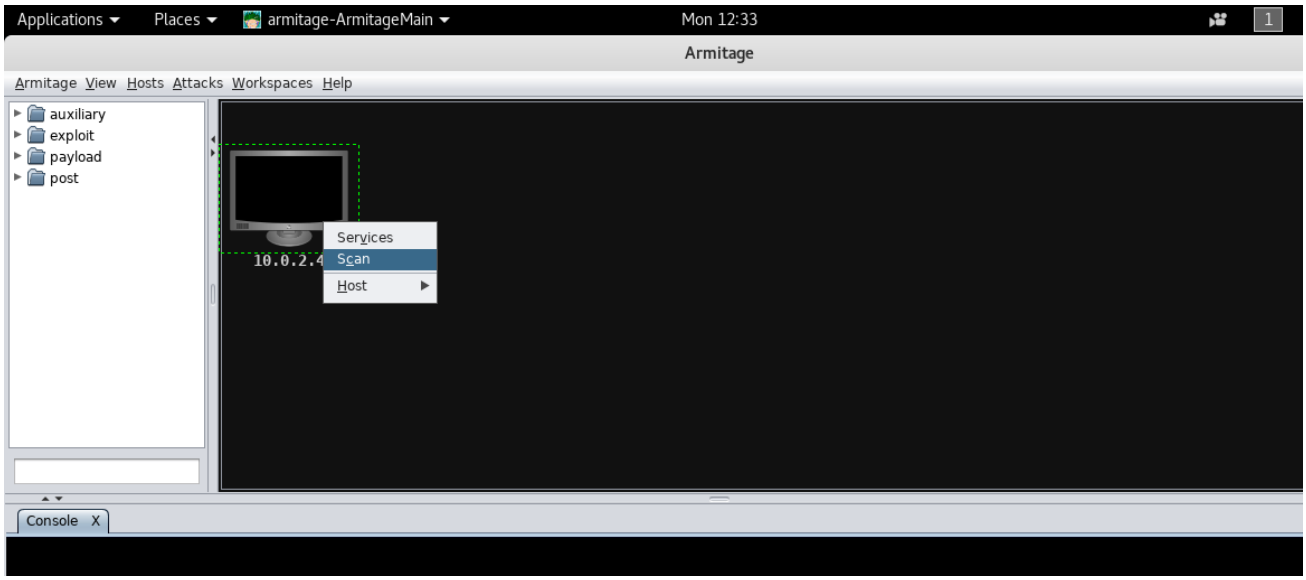
Armitage дуже зручний у використанні. Його графічний інтерфейс має три окремих області: **цілі**, **консоль** і **модулі**.



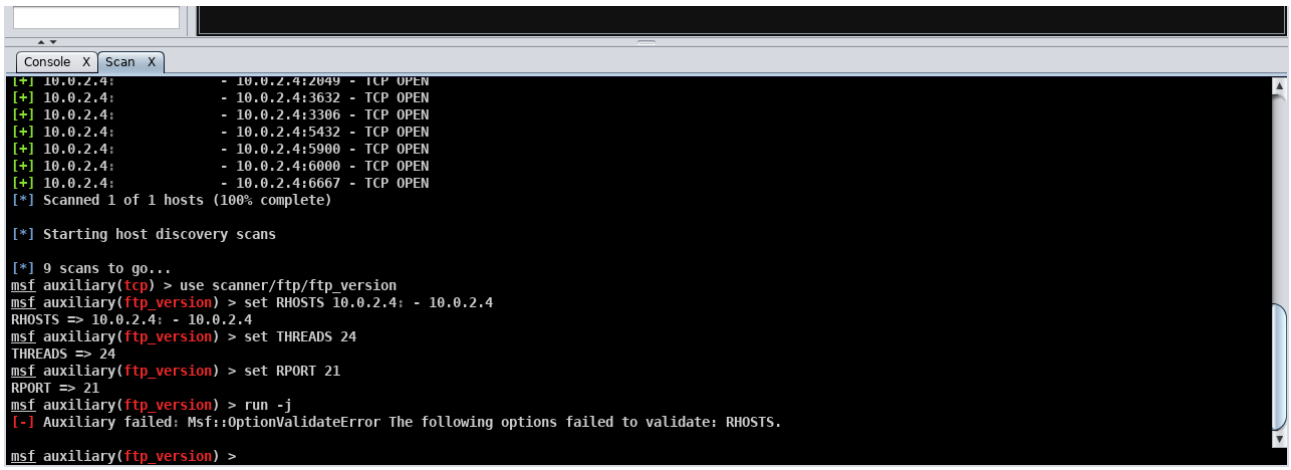
- В області **Targets** перераховані всі машини, які ви виявили, і ті, з якими ви працюєте. Зламані цілі мають червоний колір з грозою. Після того, як ви зламали ціль, ви можете клацнути по ній правою кнопкою миші і продовжити дослідження, наприклад, вивчити (переглянути) папки.
- Область **Консоль** надає доступ для папок. Просто натиснувши на неї, ви можете безпосередньо перейти до папок без використання будь-яких команд Metasploit.
- Область **Модулі** – це розділ, в якому перераховані модулі вразливостей.

У Armitage в меню вибираємо Hosts → Add Hosts .... Вставляємо у віконечко IP нашої цілі: **10.0.2.4**.

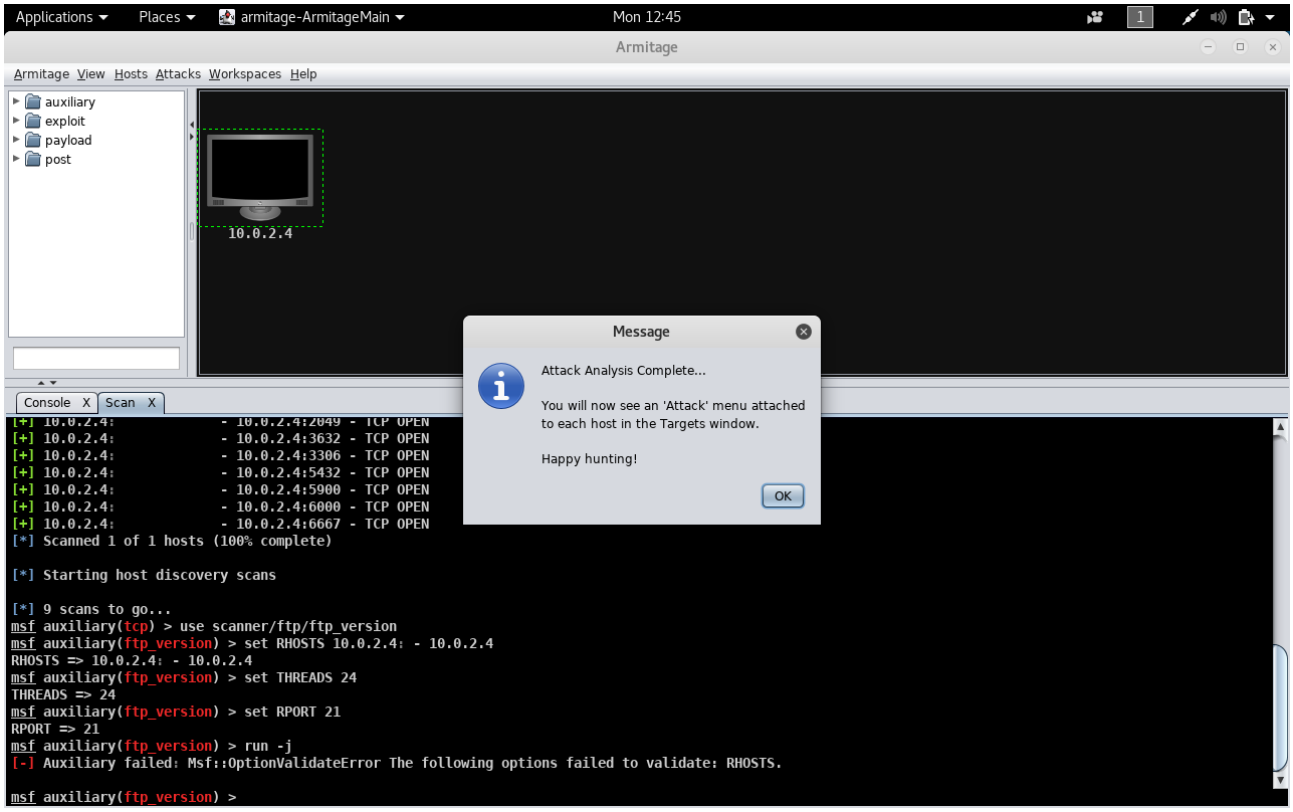
Натискаємо правою кнопкою миші по хосту і вибираємо Scan. Під час сканування визначається версія ОС, запущені процес, відкриті порти. Завдяки цій інформації будуть відібрані можливі експлойти.



Сканування завершено:



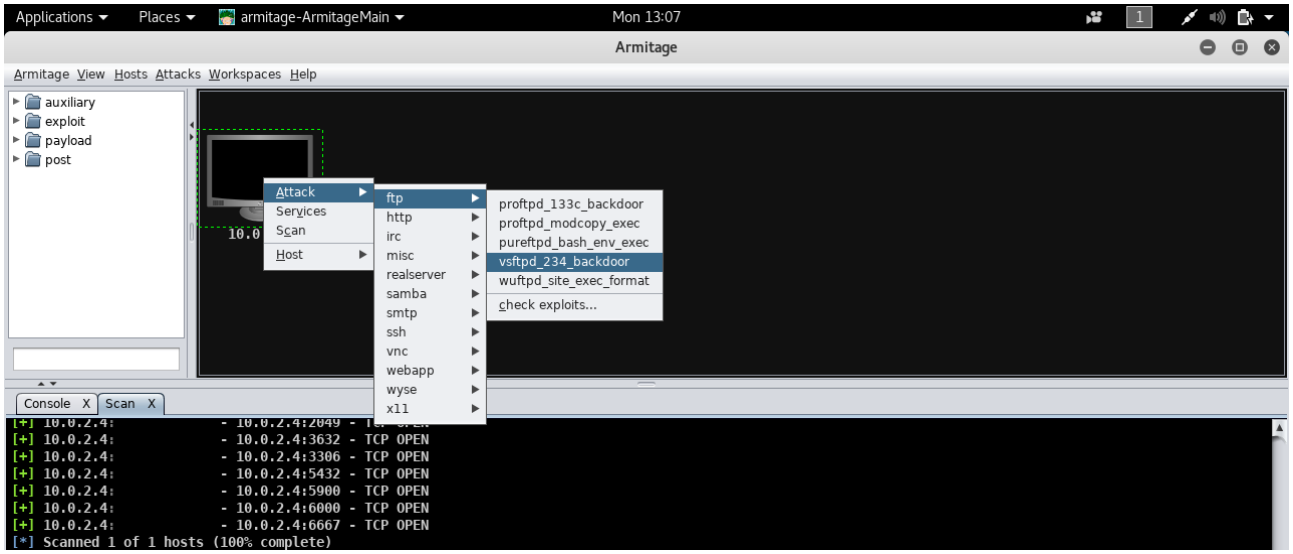
Тепер ми повністю готові для підбору експлойтів. Для цього переходимо в пункт меню Attacks → і вибираємо Find Attacks.



Тепер клікайте правою кнопкою миші по хосту і вибирайте Attack. У меню, атаки згруповані по типу цілі. Можна вже зараз вибрати конкретну атаку або провести перевірку групи атак .. Робиться це вибором опції check exploits.

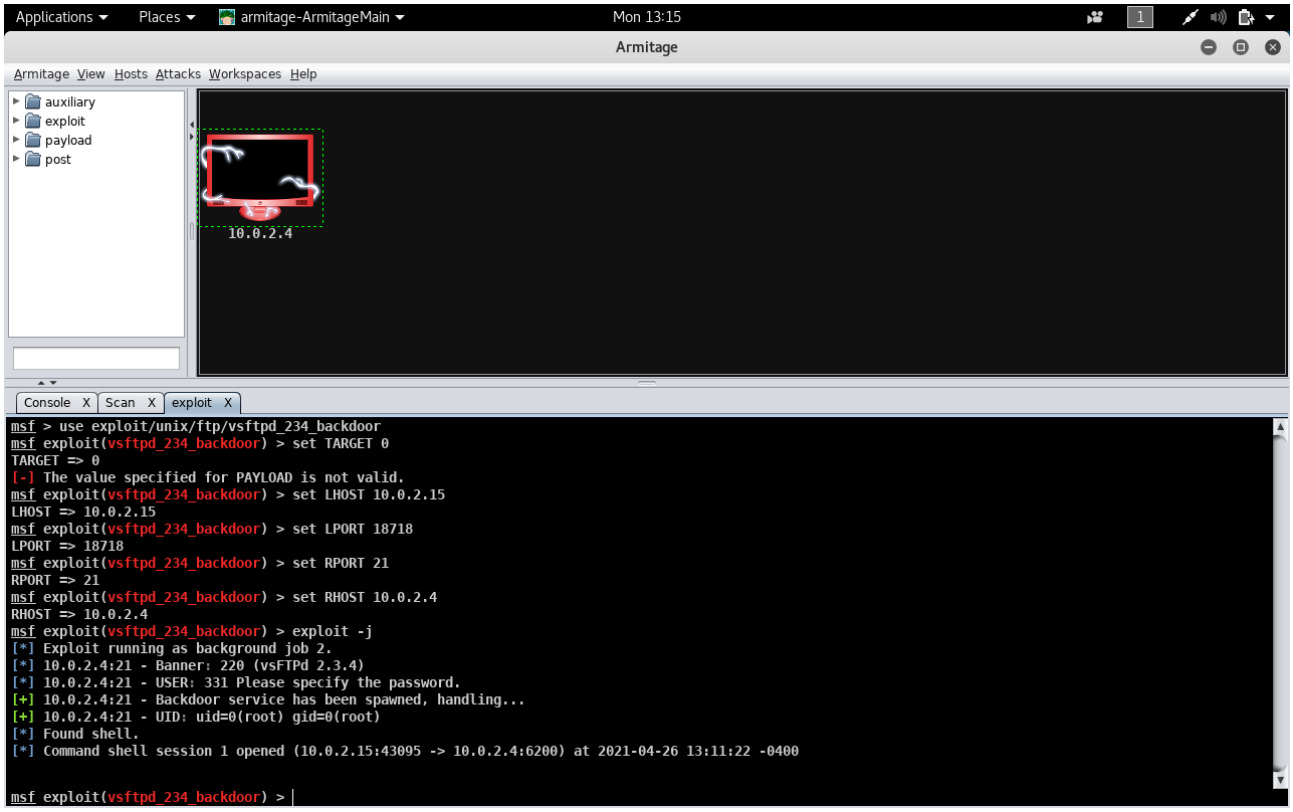
Далі ми використаємо вразливість **Vsftpd backdoor**.

Клацніть правою кнопкою миші на цільовому хості, виберіть “Attack” -> “ftp” -> “vsftpd_234_backdoor”.

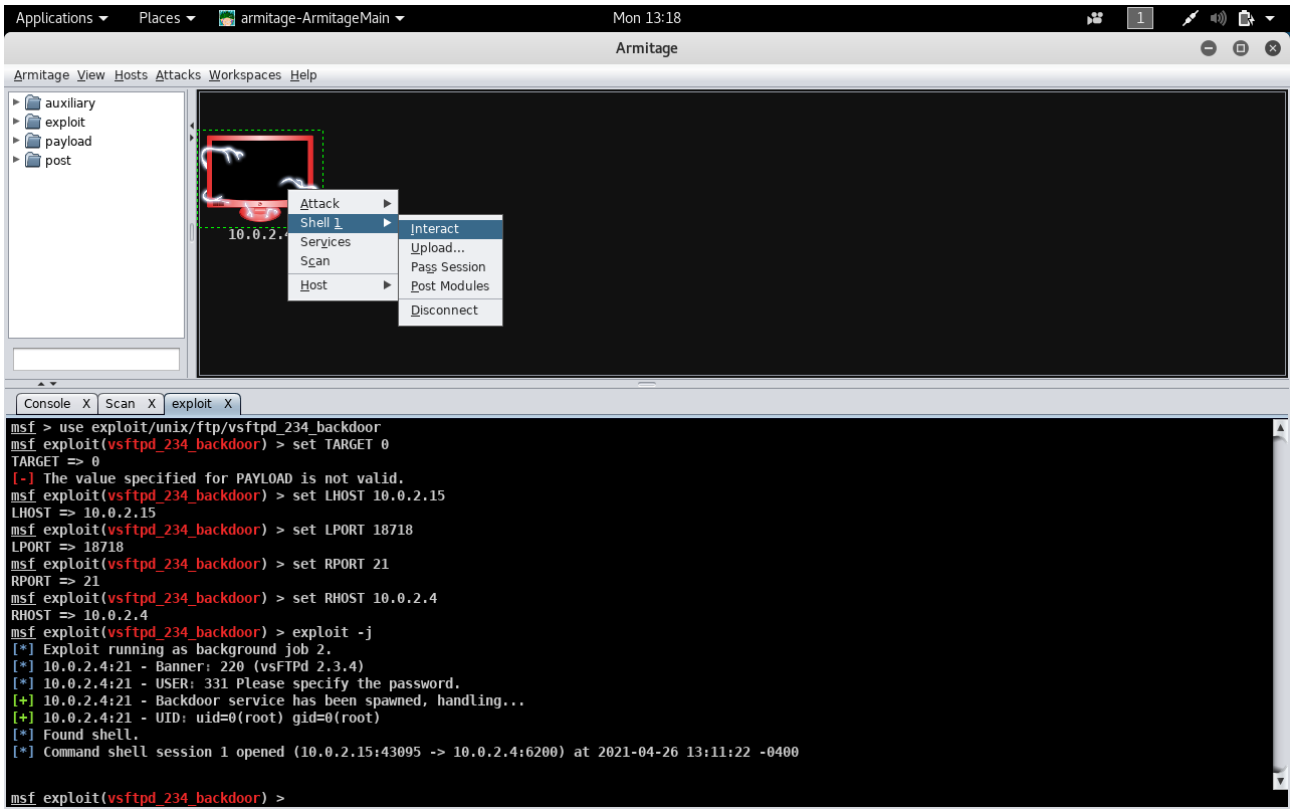


Виберіть “Використовувати зворотне з’єднання (Use a reverse connection)” та натисніть “Запуск”.

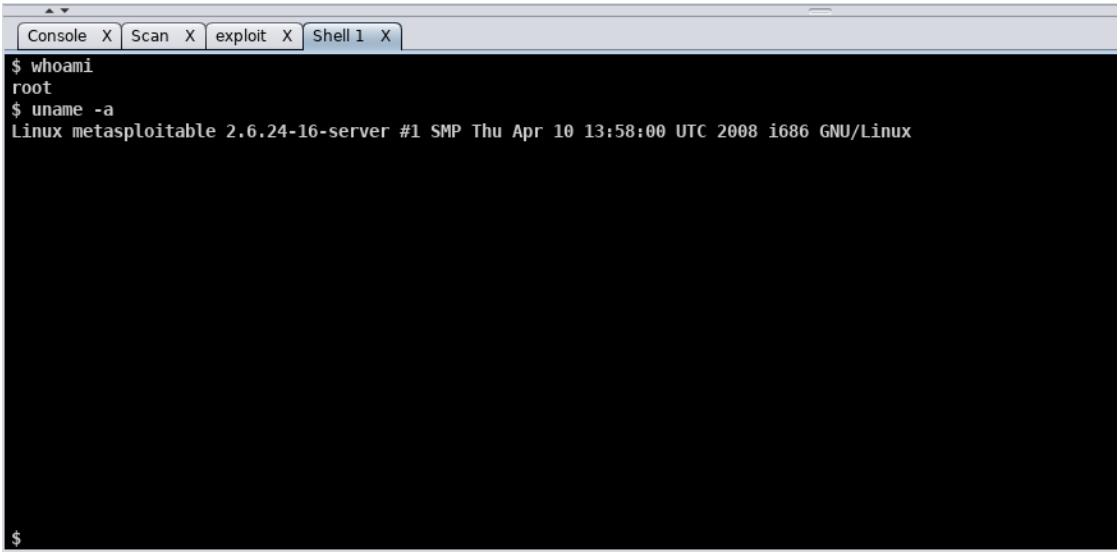
Консоль в Armitage показує, що скрипт успішно запущений.



Клацніть правою кнопкою миші на машині-«жертві» та виберіть «Shell 1» -> «Взаємодіяти (Interact)».



У нижній області відкриється нова вкладка з командною стрічкою. Набрані команди “whoami” та “uname -a”, показують, що ми справді успішно отримали доступ до цілі.



Базові команди Linux

pwd - відображає інформацію про поточне знаходження у файловій системі (шлях директорії (папки) у якій ви знаходитесь);
dir, ls - показує список файлів і папок у поточній директорії;
cd (change directory - змінити поточну директорію) дозволяє перейти у іншу папку;
Наприклад:

cd ../ - перейде у папку на рівень вище;
cd foo - перейде у дочірню папку "foo";
cd /var - перейде папку "var", що знаходиться у **корені** файлової системи;

touch file_name - створення нового файлу з назвою "file_name";
mkdir dir_name - створення нової папки "dir_name" у поточній директорії;
rm file_name (remove - видалити) - видалення файлу "file_name";
rm -r dir_name - видалення папки "dir_name";
cp origin_name new_name (copy - копіювати) - копіювання файлів і папок;
mv old_name new_name - перенесення файлів і папок;
ln -s origin_name link_name - створення символьного посилання;

Завдання до лабораторної роботи

Завдання А. Розгортання віртуальної лабораторії.

1. Встановлення середовища віртуальних машин VirtualBox або VMware Workstation.
   Завантажити програму встановлення для одного із середовищ:
   VirtualBox: https://www.virtualbox.org/wiki/Downloads
   VMware Workstation: http://www.vmware.com/products/player/
   Встановити вибране середовище віртуалізації.
2. Встановлення віртуальної машини для дослідження – Metasploitable2.
   Завантажити образ з сайту https://sourceforge.net/projects/metasploitable/
   та розгорнути віртуальну машину.
3. Встановлення віртуальної машини атакуючого – Kali Linux.
   Завантажити готовий образ віртуальної машини Kali Linux з сайту https://www.osboxes.org/kali-linux/
   Відкрити командний рядок Kali Linux.
   Виконати ping google.com і переконатися у доступності серверів google.com.
   Виконати tracert google.com.
4. Конфігурувати мережу таким чином, щоб віртуальні машини бачили одна одну. Виконавши команду ifconfig отримати дані про ip-адресу кожної віртуальної машини у мережі.
5. Скласти характеристику машини-цілі використовуючи інструменти nmap або zenmap, або інші У характеристиці повинні бути викладені наступні питання:
   – Версія операційної системи
   – Відкриті порти
   – Запущені сервіси (перелічіть принаймні 3 запущені сервіси)
6. Використайте nmap для сканування цілі та пошуку версії ОС та запущених сервісів (перелічіть принаймні 3 запущені сервіси).

Завдання Б. Дослідження можливостей Metasploit Framework.

1. Використайте описані у методичних вказівках вразливості (unreal_ircd та vsftpd_234_backdoor) для отримання доступу до машини-цілі з допомогою msfconsole та Armitage.

2. Використайте іншу вразливість для отримання доступу до машини-цілі з допомогою msfconsole та Armitage.
   Список вразливостей для Metasploitable2 ви можете знайти тут:
   https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
   або
   https://chousensha.github.io/blog/2014/06/03/pentest-lab-metasploitable-2/

3. Покажіть у звіті (у вигляді скріншотів), що Ви створили файл на атакованій віддаленій машині за допомогою команди “touch <yourname>”, де <yourname> слід замінити на ваше прізвище.