МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпека

 Сергій ЄВСЕЄВ
«____» _____ 2024 р.

ІНСТРУКЦІЯ
КІБЕРПОЛІГОН

2024

RDP (Remote Desktop Protocol) дозволяє підключитися до віддаленого комп'ютера та керувати ним, як ніби ви знаходитесь безпосередньо перед ним. В операційних системах Windows RDP вбудований, тому налаштування і використання є досить простими.

1. ПІДКЛЮЧЕННЯ ДО ВІДДАЛЕНОГО КОМП'ЮТЕРА З WINDOWS

1.1 Відкрийте "Підключення до віддаленого робочого столу":

- Натисніть Win + R і введіть mstsc, потім натисніть "Enter".
- Введіть ім'я комп'ютера або IP-адресу віддаленого комп'ютера.
- Натисніть "Підключити".

2.1 Введіть облікові дані:

- Введіть ім'я користувача та пароль для віддаленого комп'ютера.
- Натисніть "ОК" для завершення підключення.

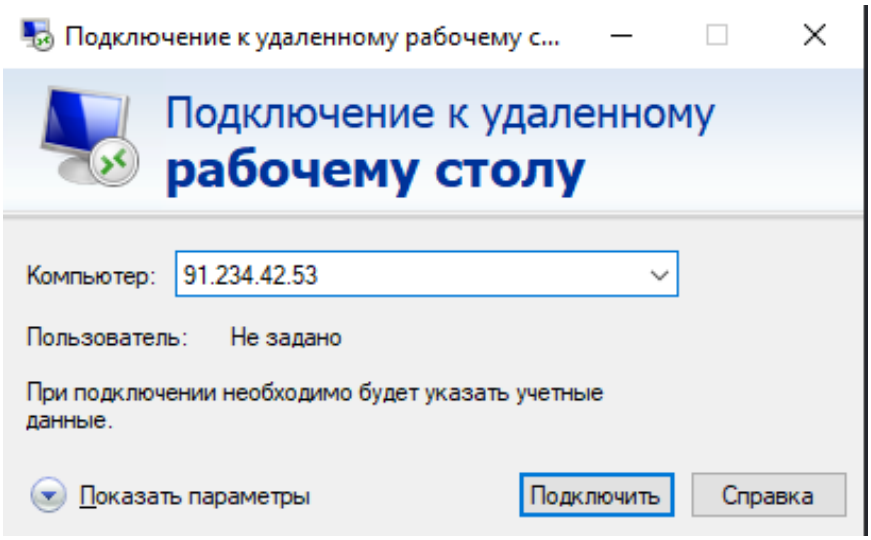

Рис. 1. Підключення до WINDOWS

2. ПІДКЛЮЧЕННЯ ДО ВІДДАЛЕНОГО КОМП'ЮТЕРА З LINUX

1. Встановіть Remmina або rdesktop:

Remmina:

sudo apt update

sudo apt install remmina remmina-plugin-rdp

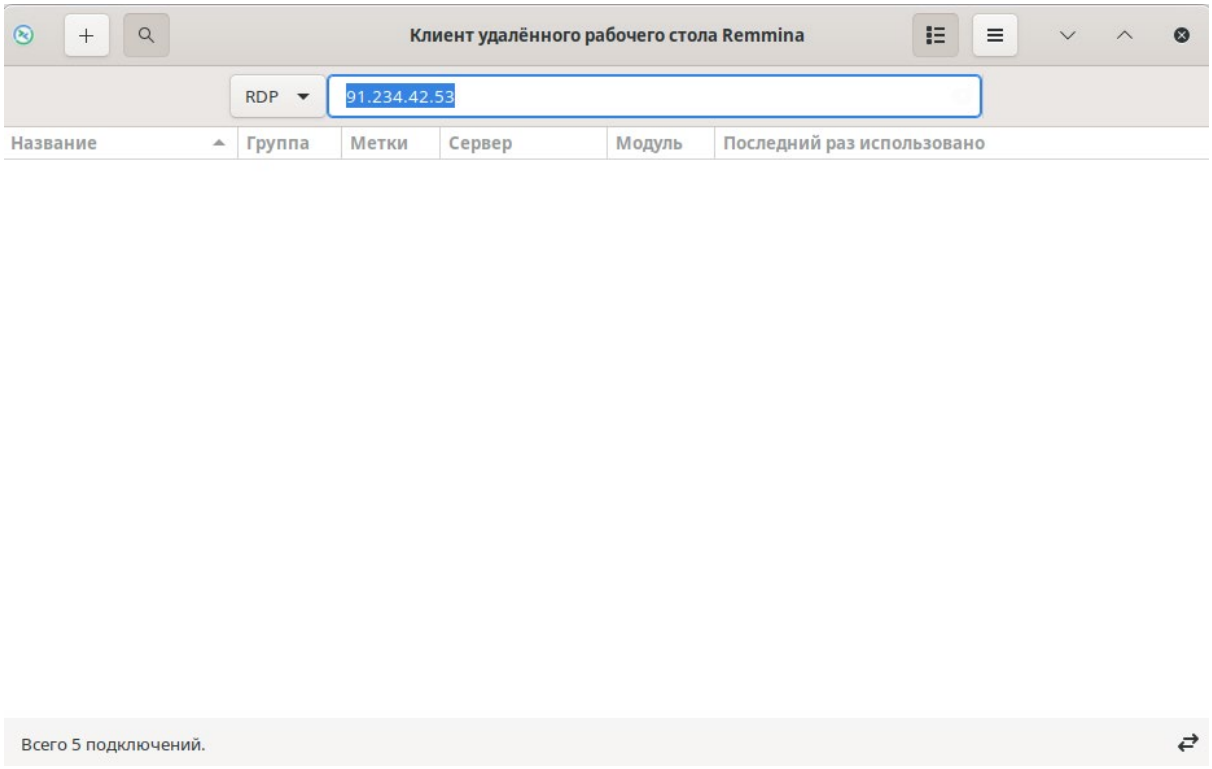

Рис. 2. Підключення до LINUX

2. **Натискаємо enter.**

Далі в обох випадках з’явиться вікно авторизації в систему Kali Linux, де потрібно будет ввести дані користувача.

Рис. 3. Вікно авторизації

Якщо з’єднання досить повільне - переконайтесь, що VPN\PROXY чи інші підключення вимкнені.

Kali Linux – це спеціалізований дистрибутив операційної системи Linux, який призначений для тестування на проникнення, аналізу безпеки та цифрової криміналістики. Він розроблений компанією Offensive Security і базується на дистрибутиві Debian. Kali Linux популярний серед хакерів, системних адміністраторів та фахівців з кібербезпеки завдяки своїм вбудованим інструментам, які полегшують проведення аудиту безпеки систем.

Основні характеристики Kali Linux:

1. **Багато інструментів**: Kali Linux містить сотні інструментів для тестування на проникнення та аналізу безпеки, що охоплюють різні аспекти кібербезпеки – від сканування мереж і аналізу трафіку до експлуатації вразливостей і оцінки захищеності веб-додатків.
2. **Підтримка широкого спектра платформ**: Kali Linux підтримує різні архітектури, включаючи x86, x64, ARM та інші, що дозволяє встановлювати його на різні пристрої, включаючи Raspberry Pi, хмарні сервери та мобільні пристрої.
3. **Висока гнучкість**: Kali Linux дозволяє створювати власні збірки системи та налаштовувати її відповідно до потреб користувача. Крім того, є можливість використовувати Kali Linux як "Live" систему, що не вимагає інсталяції на жорсткий диск.

4. **Розширена документація**: Офіційний сайт Kali Linux містить детальні посібники та документацію, які допомагають новачкам освоїти систему та її інструменти.

Найпопулярніші програми в Kali Linux:

1. **Nmap**: Інструмент для сканування мереж і пошуку відкритих портів, який широко використовується для виявлення активних хостів і служб у мережі.
2. **Metasploit Framework**: Платформа для розробки, тестування та експлуатації вразливостей. Metasploit дозволяє створювати власні експлойти та автоматизувати процес проникнення в систему.
3. **Wireshark**: Аналізатор мережевого трафіку, який дозволяє перехоплювати і детально досліджувати пакети даних, що передаються по мережі.
4. **Burp Suite**: Набір інструментів для тестування безпеки веб-додатків, який включає сканер вразливостей, інтерцептор HTTP-запитів та інші засоби для аналізу веб-приложень.
5. **John the Ripper**: Інструмент для злому паролів, який підтримує різні типи шифрування і широко використовується для перевірки надійності паролів.
6. **Hydra**: Інструмент для проведення атак грубої сили на різні протоколи аутентифікації, включаючи SSH, FTP, HTTP та інші.
7. **Aircrack-ng**: Набір інструментів для аналізу та зламу Wi-Fi мереж, який включає можливості для перехоплення та дешифрування даних, атак на WPA/WPA2.
8. **SQLmap**: Інструмент для автоматизації процесу виявлення та експлуатації SQL-ін'єкцій у веб-додатках.

Metasploit framework

Інструмент для створення, тестування та використання експлойтів. Дозволяє конструювати експлойти з необхідним у конкретному випадку "корисним навантаженням" (payloads), що виконується в разі вдалої атаки, наприклад, встановлення shell або VNCсервера. Також фреймворк дає змогу шифрувати шеллкод, що може приховати факт атаки від IDS або IPS.

Рис. 4. Metasploit

Nmap (Network Mapper)

Це вільна утиліта, призначена для сканування IP-мереж з будь-якою кількістю об'єктів, визначення стану об'єктів сканованої мережі (портів і відповідних їм служб). Nmap зазвичай використовують для аудиту безпеки, багато системних і мережевих адміністраторів знаходять це корисним для повсякденної роботи: такі завдання, як інвентаризація мережі, керування оновленням послуг розкладу та моніторинг працездатності хоста або служби.

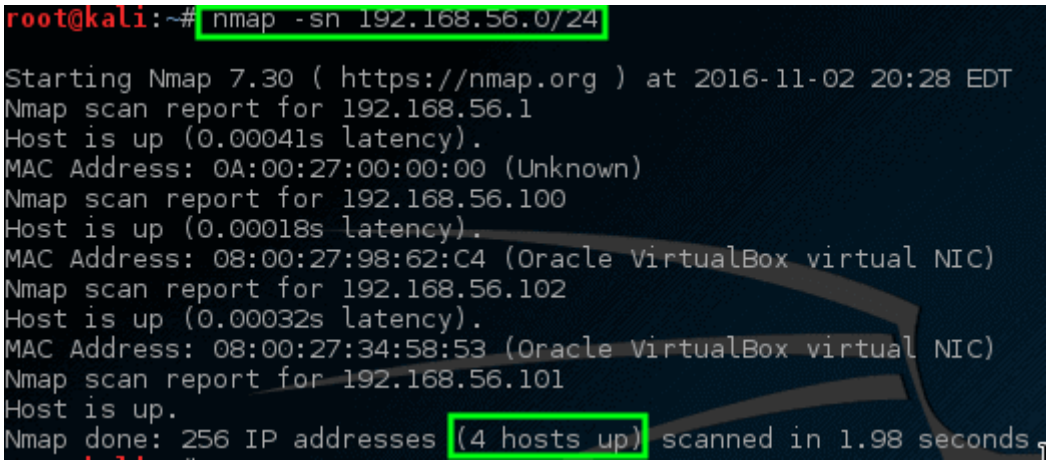

Рис. 5. Nmap

Wifite

Це автоматизований інструмент для атак на бездротову мережу. Працює з прив’язкою wifi адаптер. Не всі підтримує адаптери до kali, потрібно вибрати з розумом. Ось найпопулярніші адаптери:

- Alfa AWUS036NHA
- Alfa AWUS036ACH
- Alfa AWUS1900 / AC1900
- Panda Wireless PAU09
- Panda Wireless PAU06

Рис. 6. Wifite

Sqlmap

Sqlmap - це інструмент тестування на проникнення з відкритим вихідним кодом, який автоматизує процес виявлення і використання помилок SQL-ін'єкцій і захоплення серверів баз даних. Він поставляється з потужним механізмом виявлення, безліччю спеціалізованих функцій для ідеального тестера на проникнення і широким набором перемикачів, починаючи від зняття відбитків пальців з базою даних, вибірки даних з бази даних і закінчуючи доступом до базової файлової системи і виконання команд в операційній системі через зовнішній інтерфейс. позасмугові з'єднання.

Рис. 7. Sqlmap

John The Ripper

John The Ripper - це інструмент з відкритим вихідним кодом для злому паролів методом перебору. Спочатку він був розроблений для Unix, але зараз доступний на всіх Unix-подібних платформах, зокрема й Linux. Програма також відома як JTR або John. Вона найчастіше використовується для перебору паролів за словником.

Програма бере текстовий рядок із файлу, шифрує його так само, як був зашифрований пароль, а потім порівнює зашифрований пароль і отриманий рядок. Якщо рядки збігаються, ви отримуєте пароль, якщо ні, програма бере інший рядок із текстового файлу (словника). Саме за допомогою цього інструменту можна перевірити наскільки надійні паролі у вашій системі.

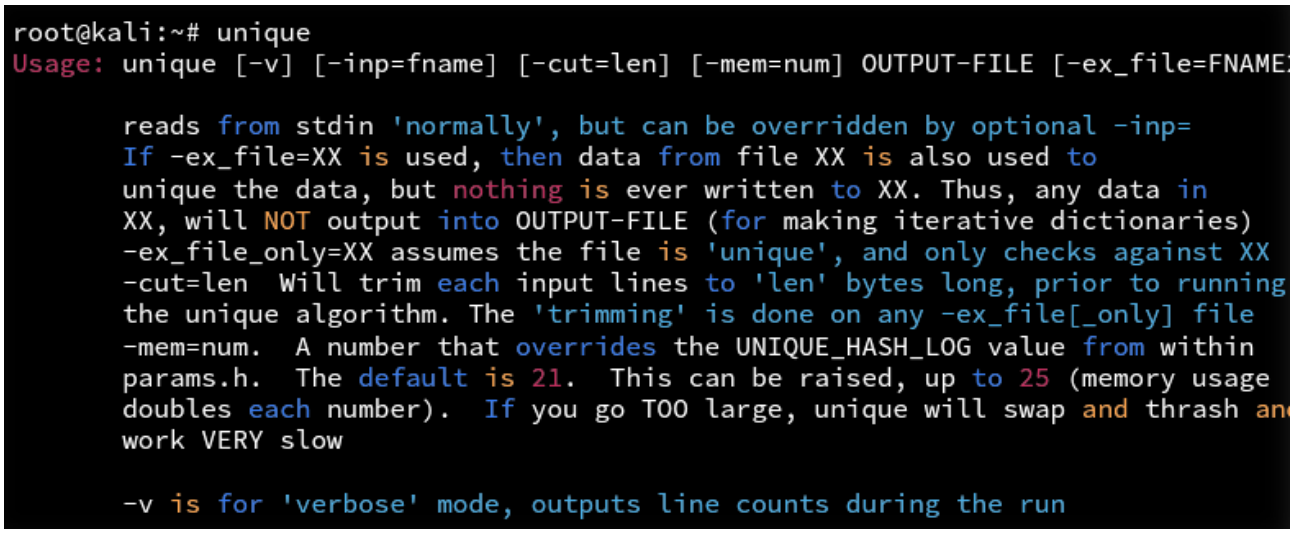

Рис. 8. John The Ripper

Burp Suite

Burp Suite - це інструмент для пошуку вразливостей на сайтах інтернету та у веб-додатках, який може працювати як за HTTP, так і за HTTPS. Він використовується багатьма фахівцями для пошуку помилок і тестування веб-додатків на проникнення. Програма дає змогу об'єднати ручні методи зі своїми засобами автоматизації, щоб виконати тестування якомога ефективніше. Burp Suite написана на Java і поширюється у форматі Jar.

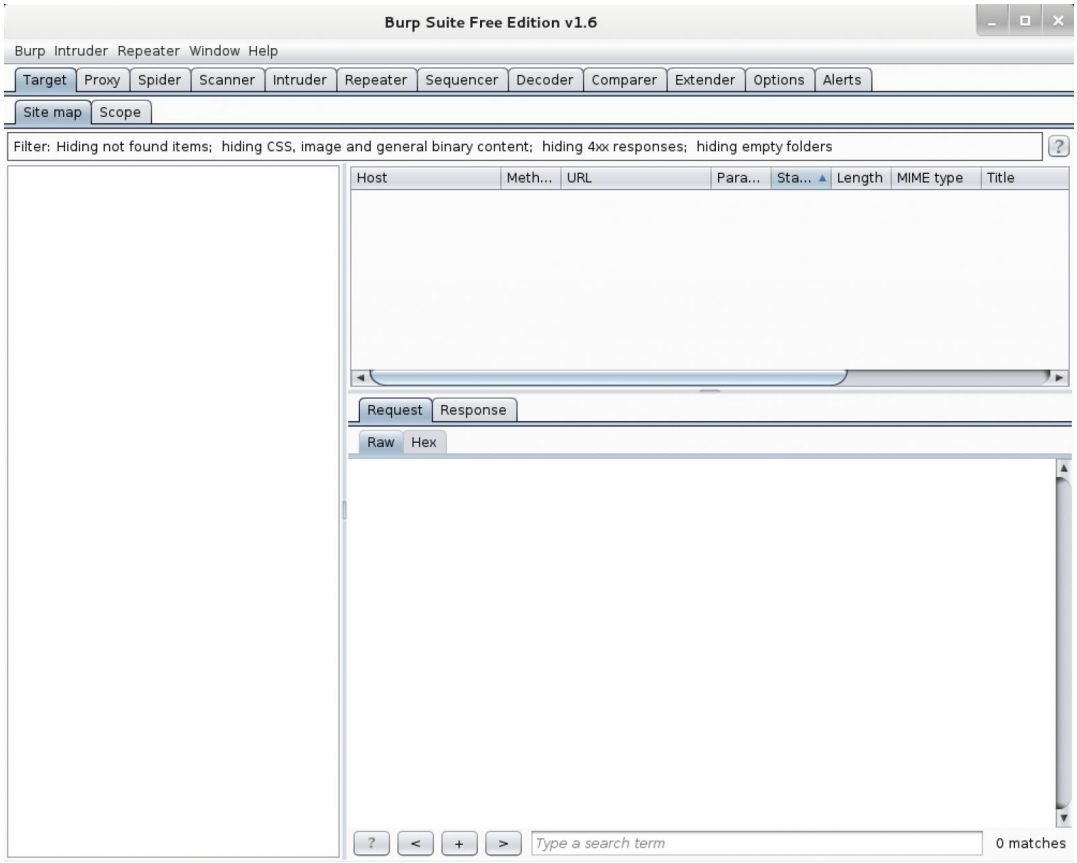

Рис. 9. Burp Suite

Nikto

Nikto - це під'єднуваний веб-сервер і сканер CGI, написаний на Perl з використанням LibWhisker RFP для виконання швидких перевірок безпеки або інформації.

Функції:

- Легко оновлювана база даних чеків у форматі CSV.
- Виведення звітів у вигляді звичайного тексту або HTML
- Доступні версії HTTP з автоматичним перемиканням
- Загальні та спеціальні перевірки серверного програмного забезпечення
- Підтримка SSL (через libnet-ssleay-perl)
- Підтримка проксі (з аутентифікацією)
- Підтримка файлів cookie

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.102
+ Target Hostname:    192.168.0.102
+ Target Port:        80
+ Start Time:         2018-03-23 10:49:04 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 287, size: 1183
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user ag
+ The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to ea
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apach
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 371 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2018-03-23 10:50:44 (GMT0) (100 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
root@kali:~# firefox report.html
```

Рис. 10. Nikto

Начальник навчальної лабораторії Ірина СЕВРЮКОВА