МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Безпека комп'ютерних мереж

Лабораторна робота "Мережне сканування"

Перевірив:
_____

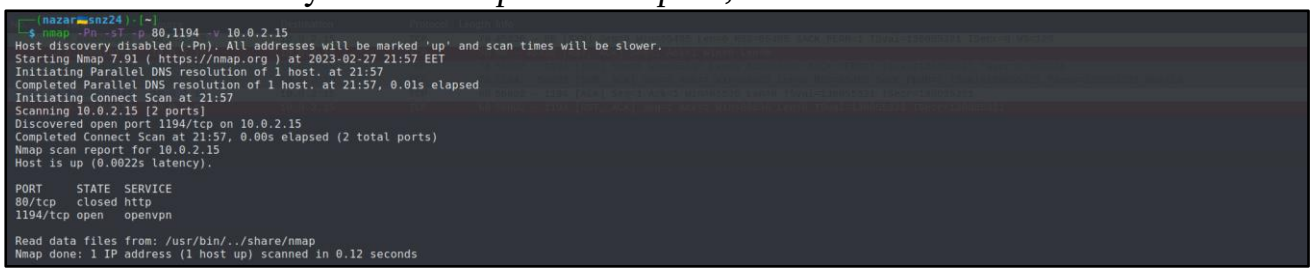
Виконав:
студент III курсу
групи ФБ-01
Сахній Н.Р.

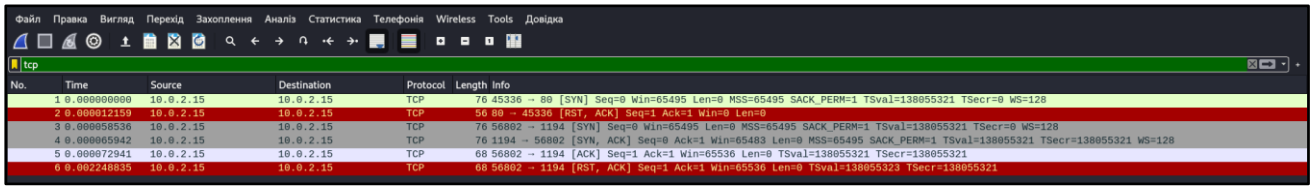
Київ 2022

Завдання 1:

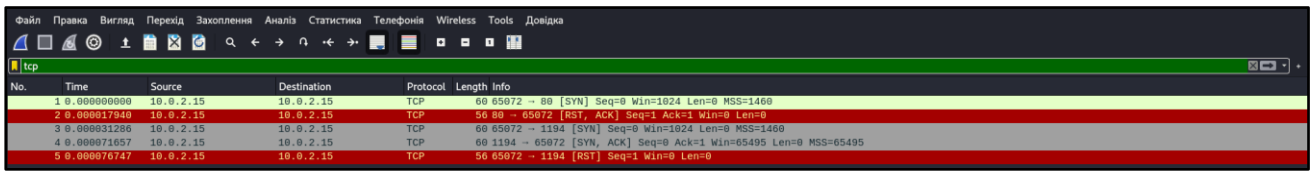
Ознайомлення з роботою NMAP та особливостями різних видів сканування.

- Connect сканування: *nmap -Pn -sT -p 80,1194 -v 10.0.2.15*

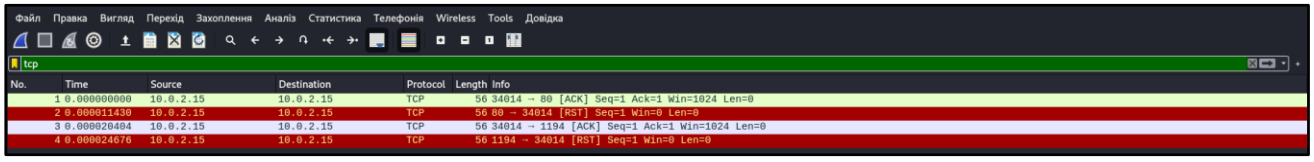




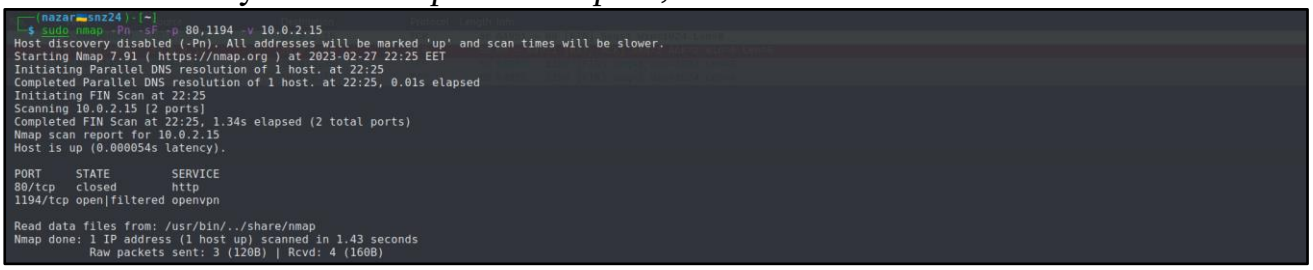
- SYN сканування: *nmap -Pn -sS -p 80,1194 -v 10.0.2.15*

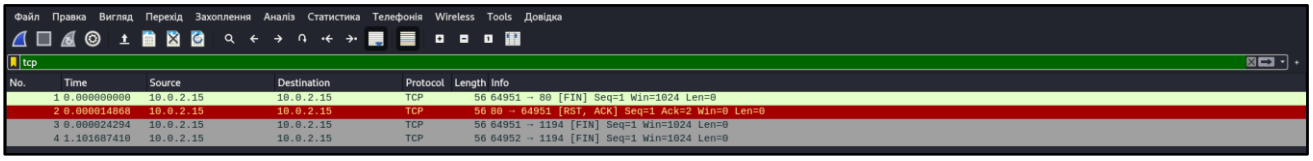


- ACK сканування: *nmap -Pn -sA -p 80,1194 -v 10.0.2.15*

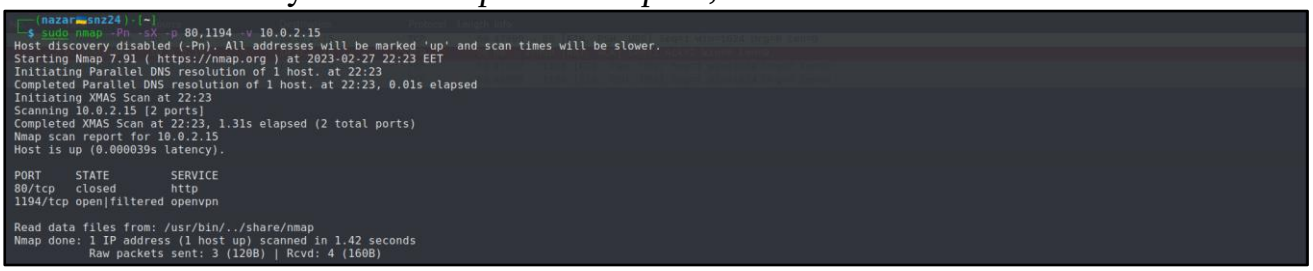


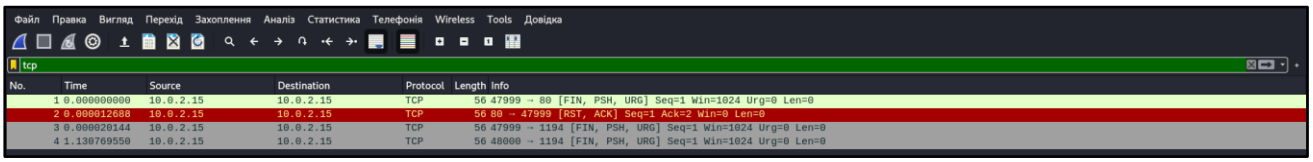
- FIN сканування: *nmap -Pn -sF -p 80,1194 -v 10.0.2.15*



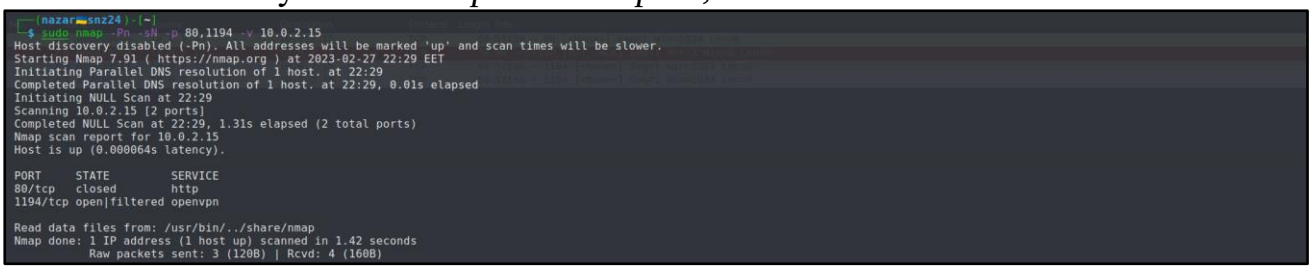


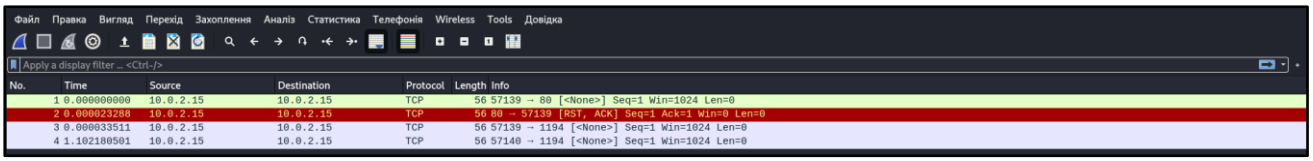
- XMAS сканування: *nmap -Pn -sX -p 80,1194 -v 10.0.2.15*





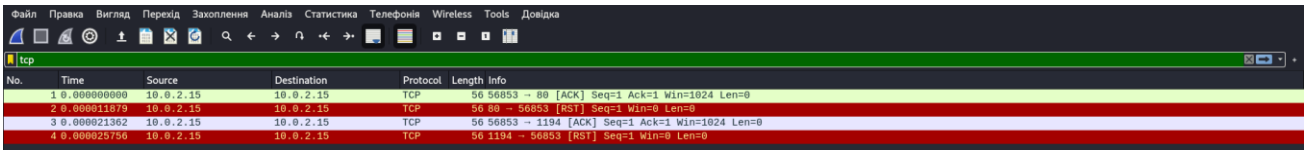
- NULL сканування: *nmap -Pn -sN -p 80,1194 -v 10.0.2.15*





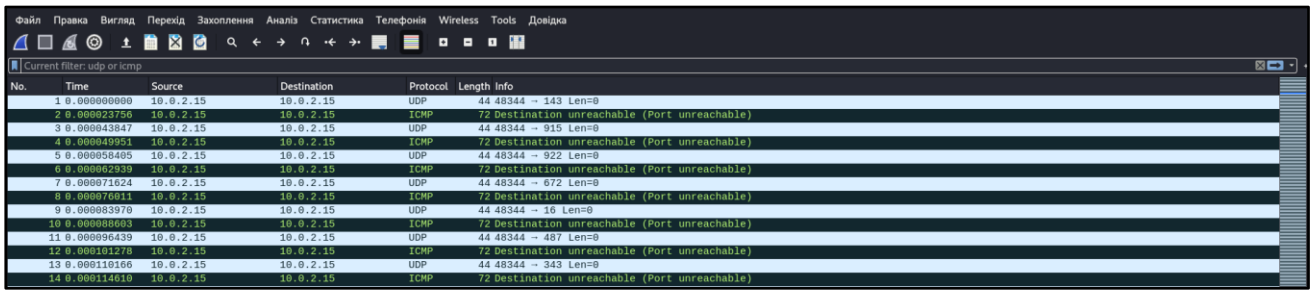
- WIN сканування: *nmap -Pn -sW -p 80,1194 -v 10.0.2.15*

```
┌──(nazar㉿snz24)-[~]
└─$ sudo nmap -Pn -sW -p 80,1194 -v 10.0.2.15
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:31 EET
Initiating Parallel DNS resolution of 1 host. at 22:31
Completed Parallel DNS resolution of 1 host. at 22:31, 0.01s elapsed
Initiating Window Scan at 22:31
Scanning 10.0.2.15 [2 ports]
Completed Window Scan at 22:31, 0.07s elapsed (2 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.000042s latency).

PORT     STATE  SERVICE
80/tcp   closed http
1194/tcp closed openvpn

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
           Raw packets sent: 2 (80B) | Rcvd: 4 (160B)
```



- UDP сканування*: nmap -sU -p 1-1024 -v 10.0.2.15*

```
┌──(nazar㉿snz24)-[~]
└─$ sudo nmap -sU -p 1-1024 -v 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 22:51 EET
Initiating Parallel DNS resolution of 1 host. at 22:51
Completed Parallel DNS resolution of 1 host. at 22:51, 0.01s elapsed
Initiating UDP Scan at 22:51
Scanning 10.0.2.15 [1024 ports]
Completed UDP Scan at 22:51, 0.06s elapsed (1024 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.0000090s latency).
All 1024 scanned ports on 10.0.2.15 are closed

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
           Raw packets sent: 1024 (29.799KB) | Rcvd: 2048 (88.176KB)
```



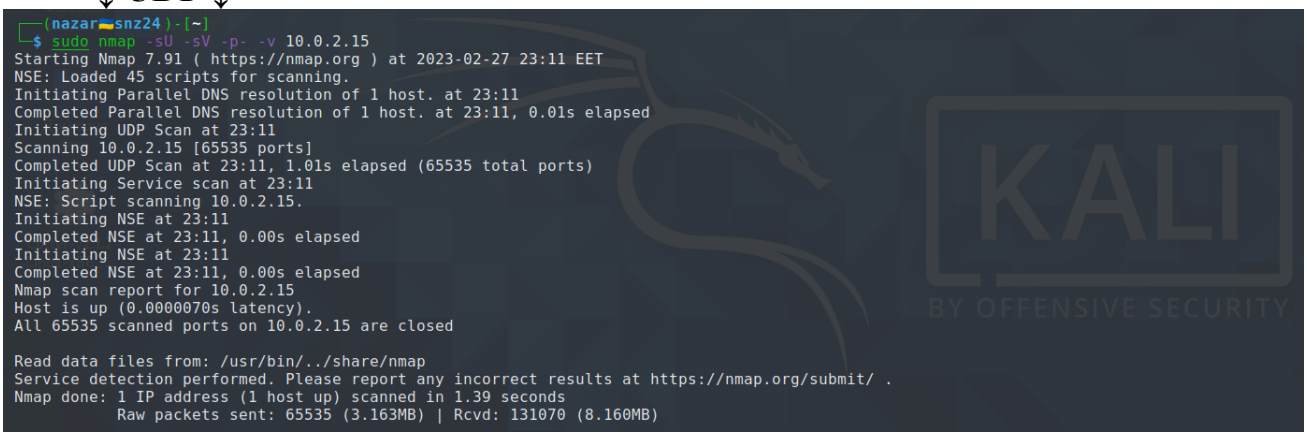
Початкове сканування деякої мережі на наявність активних хостів.

```
┌──(nazar㉿snz24)-[~]
└─$ nmap -sn 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-27 23:10 EET
Nmap scan report for 10.0.2.15
Host is up (0.00075s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.26 seconds
```

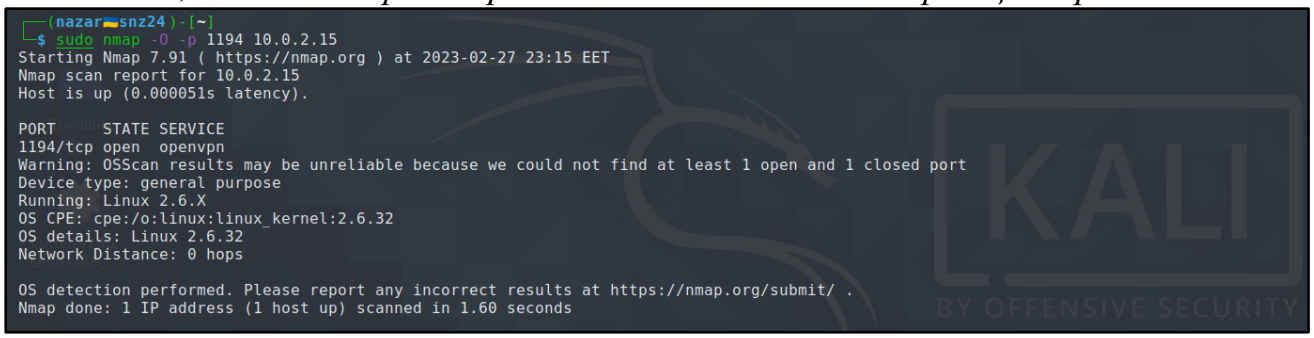
Сканування обраного хоста різними способами на наявність відкритих TCP та UDP портів і аналіз отриманих різними способами результатів.

↓ TCP ↓

↓ UDP ↓



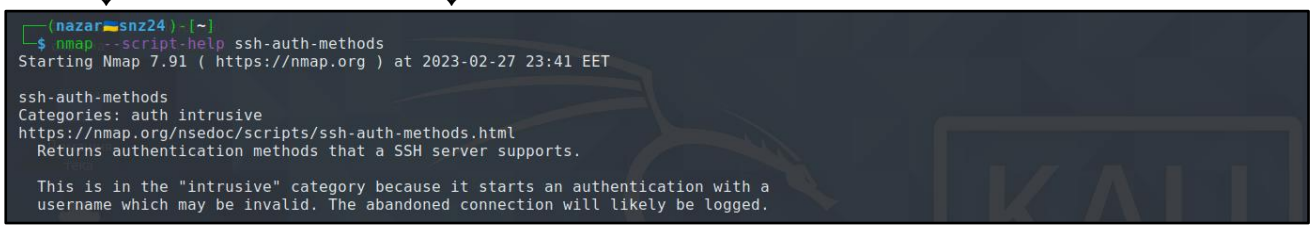
Ідентифікація засобами NMAP версії ОС, що використовується на даному хості. Відповісти, за якими параметрами здійснюється ідентифікація версії ОС?



Утиліта **nmap** з параметром "**-O**" використовує різні ознаки для ідентифікації версії операційної системи, такі як відповіді на ICMP та TCP пакети, MTU, TTL, TCP прапорці, параметри та наявність опцій, розмір вікна TCP, затримка між пакетами та тип (версія) програмного забезпечення.

Ознайомлення з наявними у NMAP скриптами та синтаксисом їх застосування. Спроба застосувати до системи, яка сканується, якомога більше NSE-модулів.

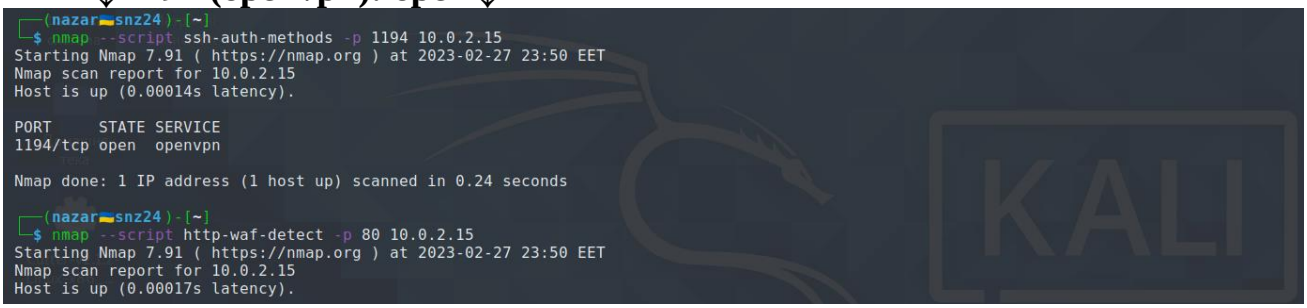
↓ ssh-auth-methods ↓



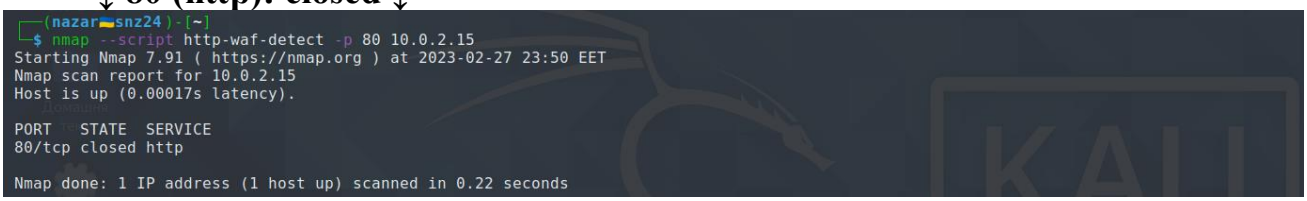
↓ http-waf-detect ↓

Після того, як NMAP виявив відкриті порти (активні мережні служби) – запустити на них відповідні NSE скрипти, щоб добути більше інформації.

↓ 1194 (openvpn): open ↓



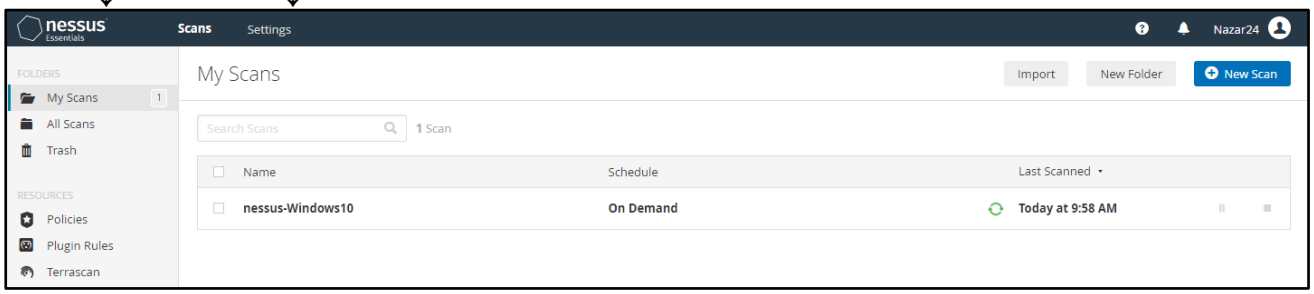
↓ 80 (http): closed ↓



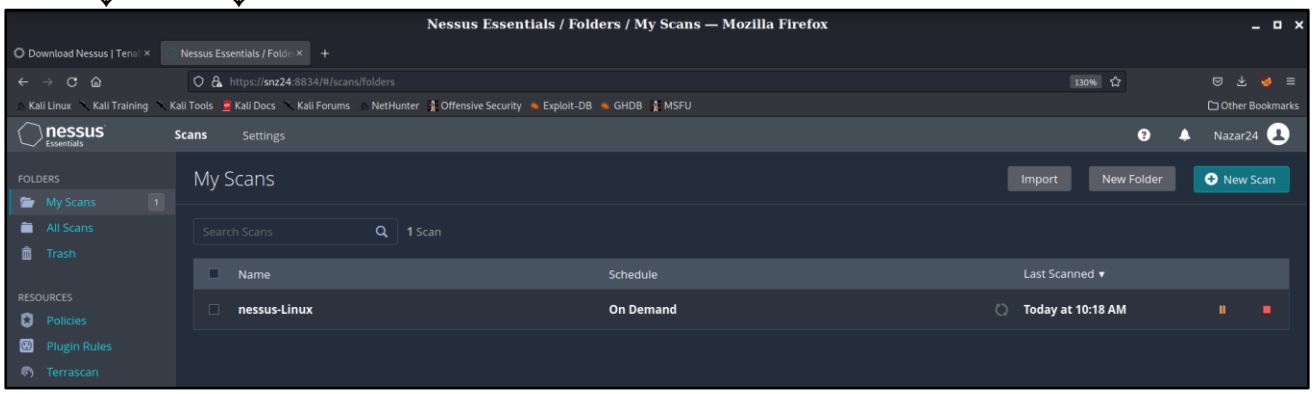
Завдання 2:

Сканування однієї Windows та однієї Linux системи на предмет наявності вразливостей сканером Nessus.

↓ Windows ↓

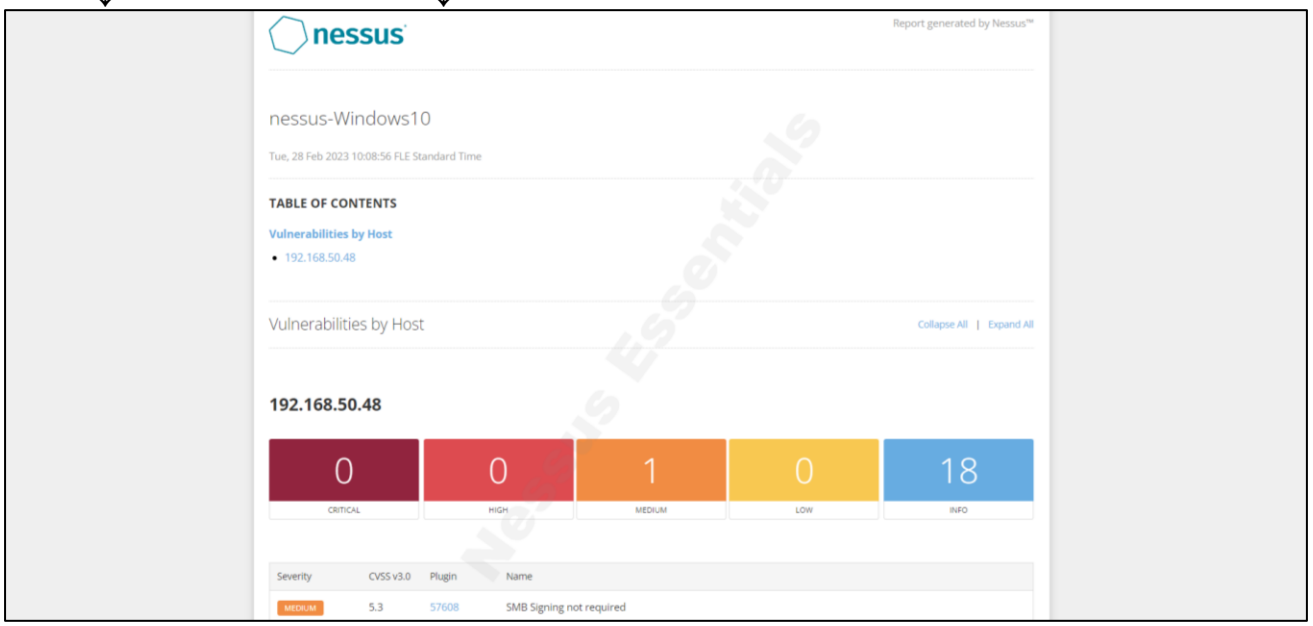


↓ Linux ↓

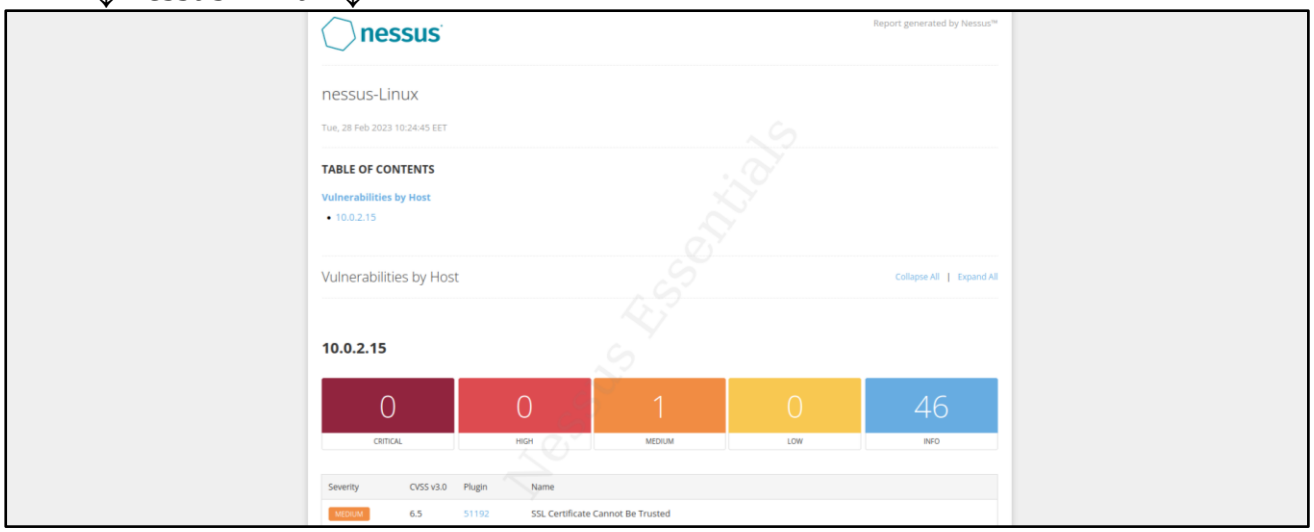


За наявними базами даних вразливостей отримайте інформацію про знайдені вразливості, ступінь їх значущості, наявність експлойтів, версії ПЗ, до яких вони застосовні, та хронологію вразливості (час публікації інформації, час появи оновлення безпеки або оновленої версії ПЗ в яких вразливість усунуто).

↓ nessus-Windows10 ↓

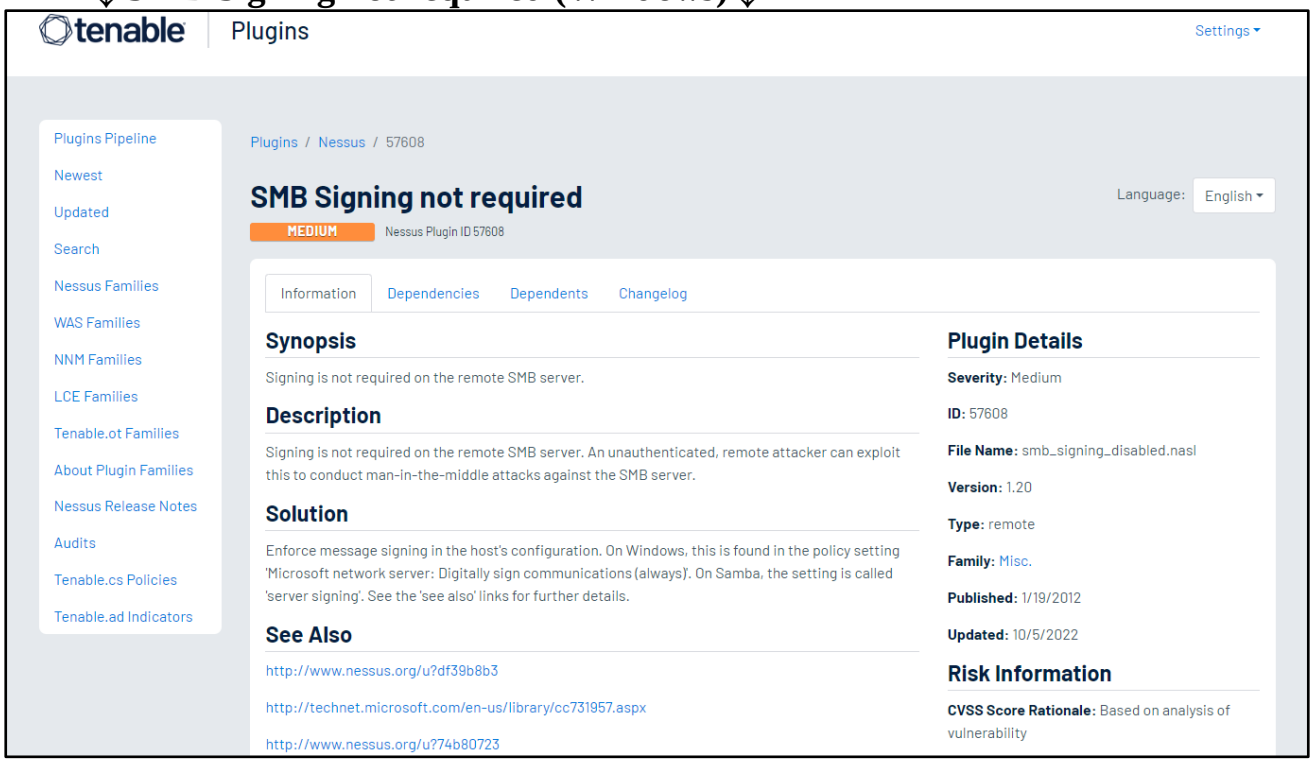


↓ nessus-Linux ↓

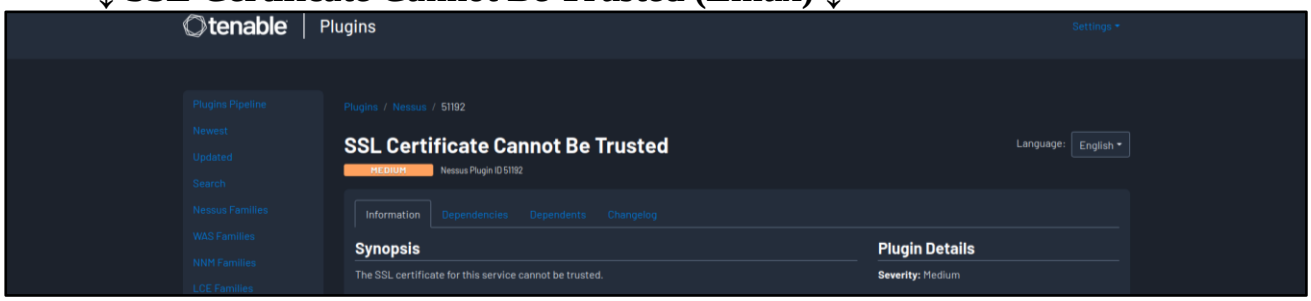


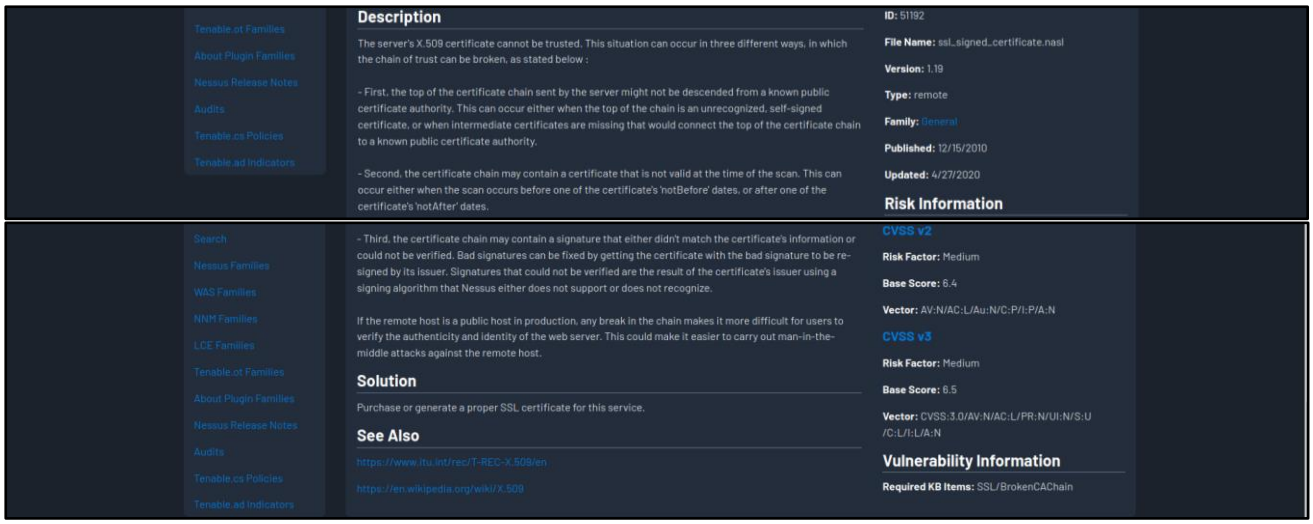
Чи зможе зловмисник використати знайдені у вашій системі вразливості?

↓ SMB Signing not required (Windows) ↓



↓ SSL Certificate Cannot Be Trusted (Linux) ↓





Висновки:

Під час виконання лабораторної роботи було використано функціонал утиліти *nmap* та сканера *Nessus*. Завдяки цим інструментам було можливо дослідити мережу та виявити потенційні вразливості та проблеми з безпекою. Їхнє використання є важливим для забезпечення безпеки мережі та даних, а також для виявлення потенційних загроз та протидії їм.

Отже, використання утиліти nmap та програми *Nessus* є необхідним кроком для забезпечення безпеки мережі та сервісів, які у ній знаходяться.