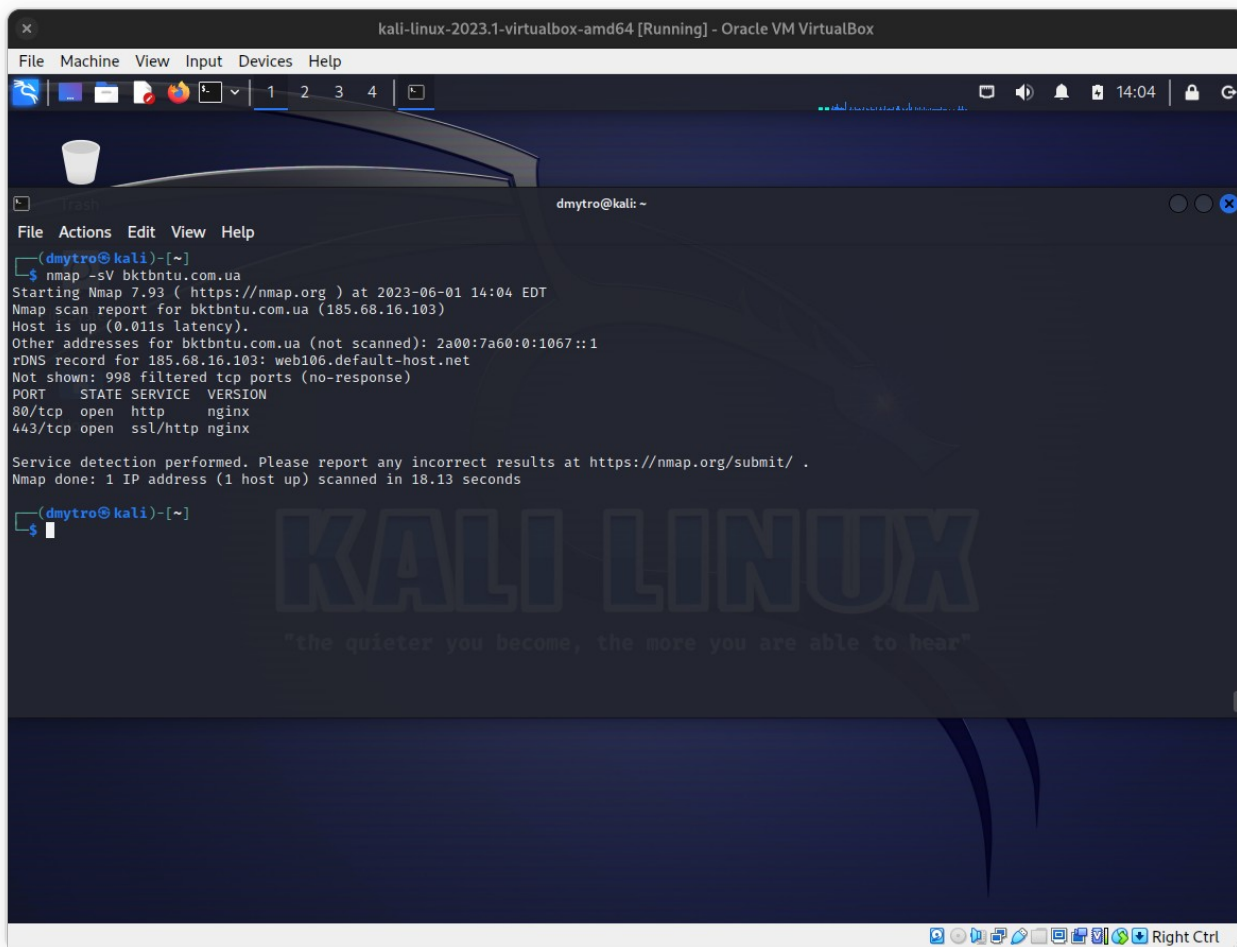


Лабораторна робота № 9-10**«Основи сканування IP-мереж за допомогою утиліти Nmap. Частина 1-2».****Завдання до роботи:****Частина I. Сканування хоста**

Примітка: Для сканування необхідно взяти ресурс, за яким виконувалася лабораторна робота № 3, і один ресурс обрати самостійно.

1. Запустити Nmap.
2. Ввести команду `nmap -sV` для визначення інформації про сервіс та його версії на відкритих портах.



The screenshot shows a Kali Linux terminal window titled "kali-linux-2023.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal displays the output of the command `nmap -sV bktbntu.com.ua`. The output includes the Nmap version (7.93), the scan time (2023-06-01 14:04 EDT), the host IP (185.68.16.103), and the results of the service detection. The detected services are `80/tcp open http nginx` and `443/tcp open ssl/http nginx`. The terminal also shows the Nmap logo and the slogan "the quieter you become, the more you are able to hear".

```
(dmytro@kali)-[~]
$ nmap -sV bktbntu.com.ua
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 14:04 EDT
Nmap scan report for bktbntu.com.ua (185.68.16.103)
Host is up (0.011s latency).
Other addresses for bktbntu.com.ua (not scanned): 2a00:7a60:0:1067::1
rDNS record for 185.68.16.103: web106.default-host.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
443/tcp   open  ssl/http nginx

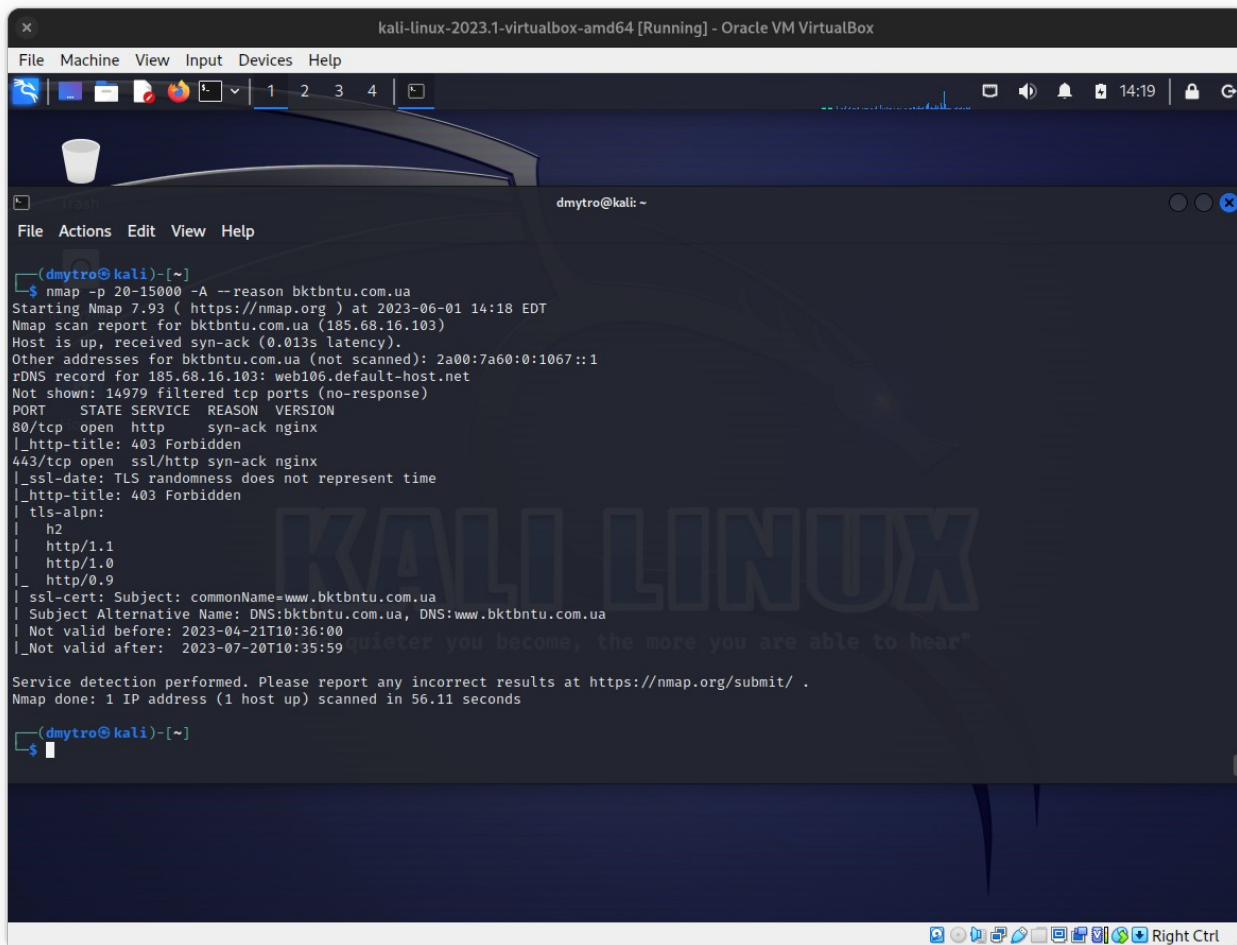
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds

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

Які порти і служби відкриті?

Лише веб сервер з портами 80 та 443(HTTP та HTTPS)

3. Ввести команду для сканування портів від 20 до 15000 з параметрами -A та --reason.



```
kali-linux-2023.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
dmytro@kali: ~
File Actions Edit View Help
(dmytro@kali)-[~]
$ nmap -p 20-15000 -A --reason bktbntu.com.ua
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 14:18 EDT
Nmap scan report for bktbntu.com.ua (185.68.16.103)
Host is up, received syn-ack (0.013s latency).
Other addresses for bktbntu.com.ua (not scanned): 2a00:7a60:0:1067::1
rDNS record for 185.68.16.103: web106.default-host.net
Not shown: 14979 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON VERSION
80/tcp    open  http   syn-ack nginx
|_http-title: 403 Forbidden
443/tcp    open  ssl/http syn-ack nginx
|_ssl-date: TLS randomness does not represent time
|_http-title: 403 Forbidden
|_tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|   http/0.9
|_ssl-cert: Subject: commonName=www.bktbntu.com.ua
| Subject Alternative Name: DNS:bktbntu.com.ua, DNS:www.bktbntu.com.ua
| Not valid before: 2023-04-21T10:36:00
|_Not valid after: 2023-07-20T10:35:59
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.11 seconds
(dmytro@kali)-[~]
$
```

Які порти і служби відкриті?

```
PORT    STATE SERVICE REASON  VERSION
80/tcp  open  http    syn-ack nginx
|_http-title: 403 Forbidden
443/tcp open  ssl/http syn-ack nginx
|_ssl-date: TLS randomness does not represent time
|_http-title: 403 Forbidden
|  tls-alpn:
|    h2
|    http/1.1
|    http/1.0
|_  http/0.9
|  ssl-cert: Subject: commonName=www.bktbntu.com.ua
| Subject Alternative Name: DNS:bktbntu.com.ua, DNS:www.bktbntu.com.ua
| Not valid before: 2023-04-21T10:36:00
|_Not valid after:  2023-07-20T10:35:59
```

Які порти і сервіси фільтруються?

14979 filtered tcp ports (no-response)

Яка IP-адреса сервера?

185.68.16.103

Яка використовується операційна система?

Ці дані встановити не вдалося

Для кожного з відкритих портів заповніть таблицю 1:

Таблиця 1

Номер порта	Сервіс	Програмне забезпечення та його версія
80	HTTPS	nginx
443	HTTPS	nginx

З якою метою використовується ключ -A? Використання яких ключів замінює один ключ -A?

Ця опція включає додаткові розширені та агресивні параметри. Зараз це дозволяє виявлення ОС (-O), сканування версій (-sV), сканування сценаріїв (-sC) і трасування (--traceroute). У майбутньому можуть бути додані інші функції. Суть полягає в тому, щоб увімкнути повний набір параметрів сканування без необхідності запам'ятовувати великий набір прапорців. Однак, оскільки сканування сценаріїв із набором за замовчуванням вважається нав'язливим, ви не повинні використовувати -A проти цільових мереж без дозволу. Цей параметр вмикає лише функції, а не параметри синхронізації (наприклад, -T4) або параметри докладності (-v), які вам також можуть знадобитися. Параметри, які потребують привілеїв (наприклад, root-доступ), такі як виявлення ОС і traceroute, будуть увімкнені, лише якщо ці привілеї доступні.

З якою метою використовується ключ --reason?

Показати причину, через яку порт перебуває в певному стані

Частина II. Робота з базами вразливостей

4. Використовуючи відкриті бази даних вразливостей NVD та CVE, визначити уразливості для версій програмного забезпечення, виявлених на відкритих портах.

Інформацію занести у таблицю 2:

Таблиця 2

Програмне забезпечення та його версія	Ідентифікатор уразливості	Опис	Рівень критичності (CVSS*)
Nginx	CVE-2009-3898	Уразливість проходження каталогу в <code>src/http/modules/nginx_http_dav_module.c</code> у nginx (так відомий як Engine X) до 0.7.63 та 0.8.x до 0.8.17 дозволяє віддаленим автентифікованим користувачам створювати або перезаписувати довільні файли через <code>..</code> (крапка крапка) у HTTP-заголовку призначення для методу WebDAV (1) COPY або (2) MOVE.	4.9
Nginx	CVE-2009-3896	<code>src/http/nginx_http_parse.c</code> у nginx (він же Engine X) від 0.1.0 до 0.4.14, 0.5.x до 0.5.38, 0.6.x до 0.6.39, 0.7.x до 0.7.62 та 0.8.x до 0.8.14 дозволяє віддаленим злоумисникам викликати відмову в обслуговуванні (розіменування NULL-вказівника та збій робочого процесу) через довгий URI.	5.0

***CVSS - Common Vulnerability Scoring System**