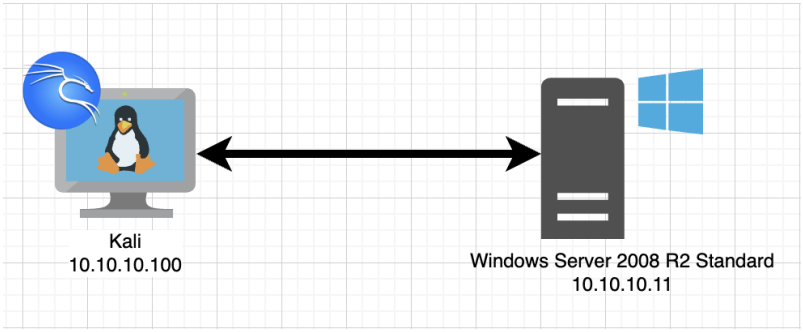
ชื่อ-นามสกุล อดิศนต์ ทนุพันธ์ รหัสนักศึกษา 6604062636739

Lab 2: nmap

จุดประสงค์การทดลอง

1. เพื่อศึกษาวิธีสแกนโฮสต์โดยใช้ nmap และทำความเข้าใจผลลัพธ์จากแต่ละคำสั่ง

Lab Topology



ใน VirtualBox, ให้ตั้งค่าการเชื่อมต่อเครือข่ายแบบ NAT network (ถ้าทั้ง 2 เครื่อง ไม่สามารถได้ IP address)

ถ้านักศึกษาใช้โพรโทคอล DHCP เติมข้อมูลต่อไปนี้ให้สมบูรณ์

Kali

IP address = 10.0.2.4

Subnet Mask = 255.255.255.0

Gateway = 10.0.2.1

Windows Server 2008

IP address = 10.0.2.15

Subnet Mask = 255.255.255.0

Gateway = 10.0.2.1

ชื่อ-นามสกุล อดิเทพ์ ทนุพันธ์ รหัสนักศึกษา 6604062636739

บทนำ

nmap (Network Mapper) เป็นหนึ่งในเครื่องมือที่ใช้กันมากที่สุดในหมู่แฮกเกอร์และผู้ดูแลระบบ มีความสามารถในการสแกนโฮสต์ไม่ว่าจะเป็น เครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เครือข่าย การสแกนด้วย nmap จะเป็นการค้นหาข้อมูลต่างๆ เกี่ยวกับระบบหรือเครือข่ายเป้าหมาย เช่น อุปกรณ์ที่เชื่อมต่ออยู่ในเครือข่าย พอร์ตที่เปิดอยู่บนอุปกรณ์ หรือบริการ (Services) ที่ทำงานบนพอร์ตเหล่านั้น

เครื่องมือ

Kali Linux หรือเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรม nmap

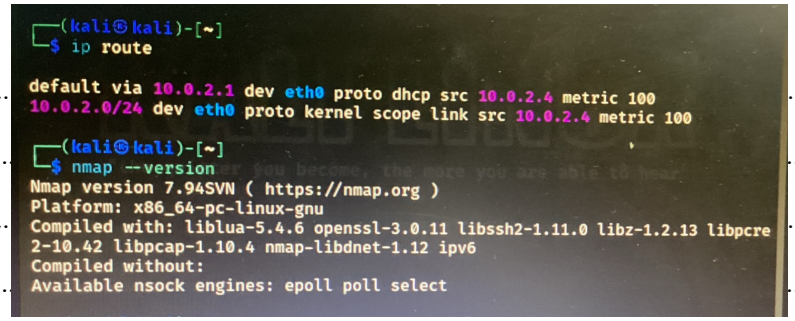
ขั้นตอนการทดลอง

nmap มีโฮสต์เพื่อให้ผู้ใช้งานทดสอบ คือ scanme.nmap.org

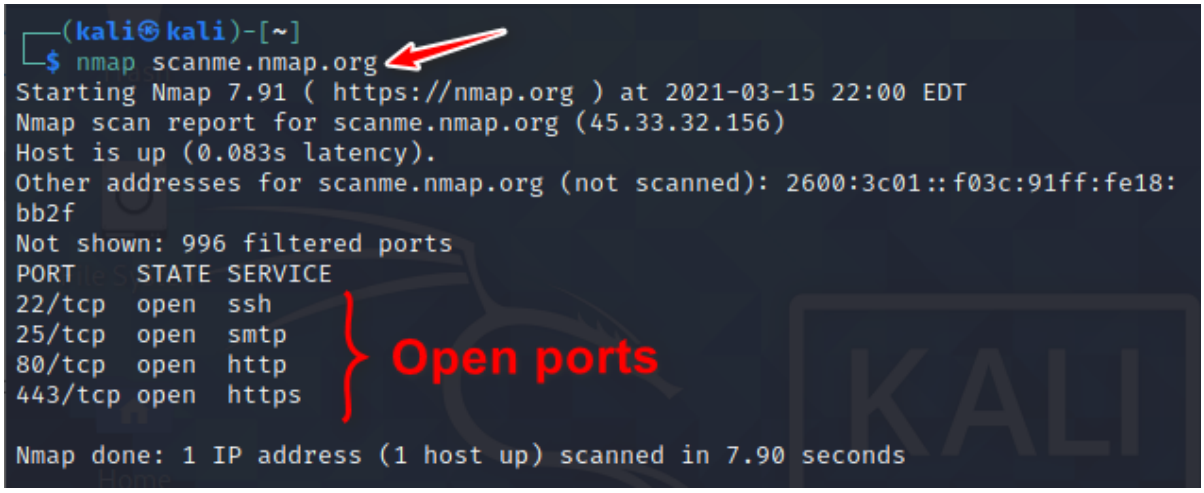
การสแกนโฮสต์ของหน่วยงานโดยไม่ได้รับอนุญาตมีความสุ่มเสี่ยงที่จะผิด พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 (ฉบับที่ 2)

1. nmap เป็นเครื่องมือที่พร้อมใช้งานใน Kali Linux การเรียกใช้งานเปิดเทอร์มินัลแล้วพิมพ์ nmap --version เพื่อตรวจสอบเวอร์ชันของ nmap

บันทึกผล

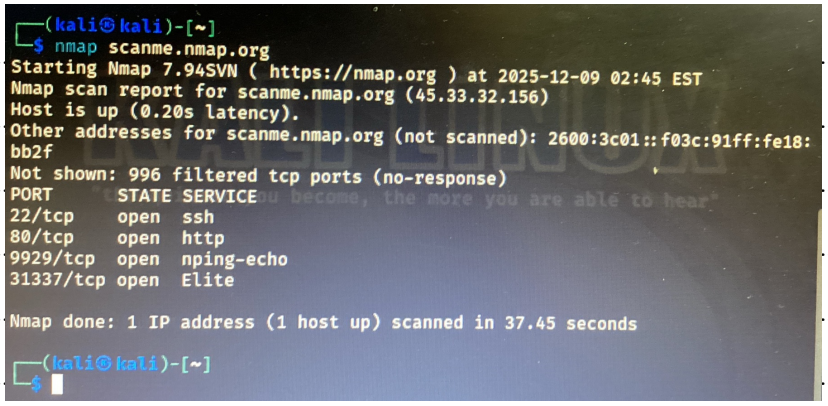


2. พิมพ์ nmap scanme.nmap.org โปรแกรมจะเริ่มต้นการสแกนเป้าหมาย โดยพยายามตรวจสอบว่าพอร์ตใดเปิดอยู่และบริการใดบ้างที่เปิดอยู่บนพอร์ตเหล่านั้น



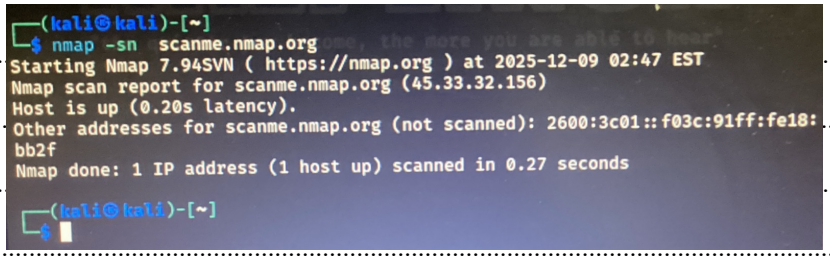
เราจะเห็นจากผลการสแกนว่ามีพอร์ตเปิดอยู่ 4 พอร์ต และมีบริการ (Service) ที่แตกต่างกันทำงานในแต่ละพอร์ต โดยการสแกนนี้เป็นการสแกนขั้นพื้นฐาน คือ สแกนเฉพาะพอร์ต 1,000 อันดับแรกเพื่อดูข้อมูลพื้นฐานเท่านั้น

<u>บันทึกผล</u>

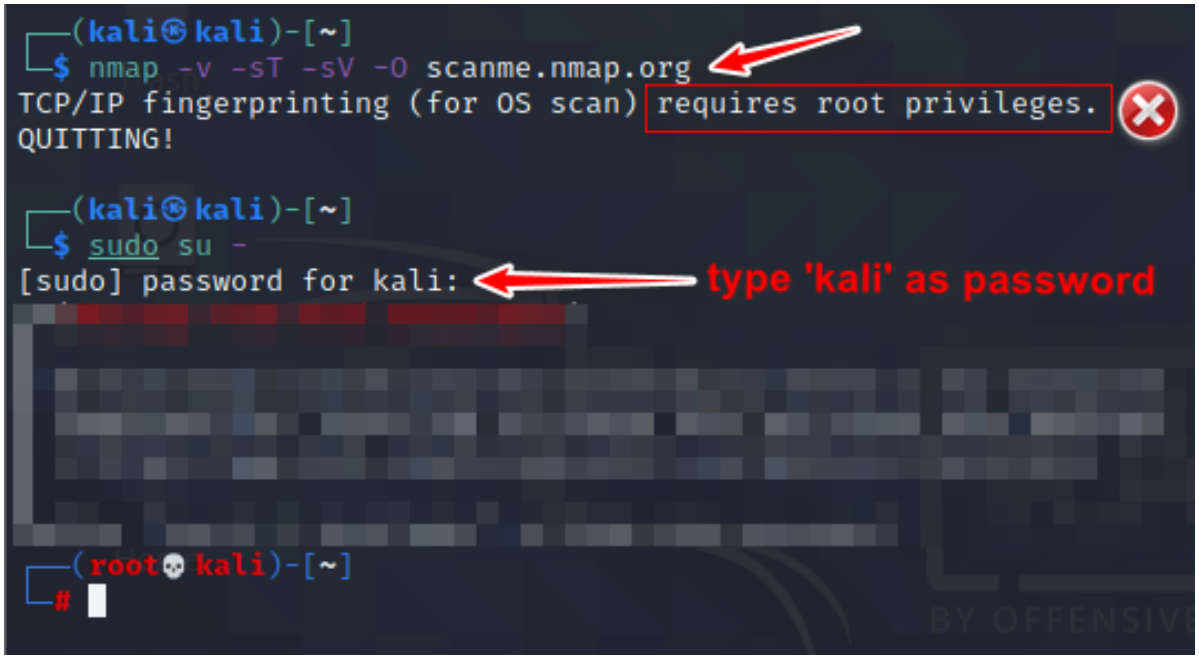


3. ในกรณีต้องการตรวจสอบการมีอยู่ของเครื่องเป้าหมาย เพื่อให้ได้ผลอย่างรวดเร็วและไม่ต้องการความละเอียดในการตรวจสอบ ให้ใส่ command-line flags -sn ตัวอย่างเช่น nmap -sn scanme.nmap.org

บันทึกผล



4. ดำเนินการสแกนเป้าหมายเดียวกัน คือ scanme.nmap.org แต่ใช้การสแกนขั้นสูง เพื่อตรวจสอบเวอร์ชันของบริการ (Service) ที่ทำงานบนแต่ละพอร์ต ซึ่งถ้าหากเป็นเวอร์ชันที่ล้าสมัยอาจมีช่องโหว่ และเสี่ยงต่อการถูกโจมตีจากผู้ไม่หวังดีได้ และในการสแกนขั้นสูงเรายังสามารถรู้ถึงระบบปฏิบัติการของเว็บเซิร์ฟเวอร์ที่ใช้ในโฮสต์เว็บไซต์เป้าหมายด้วย หรือสามารถตรวจสอบเฉพาะ Protocol TCP หรือ UDP ที่เครื่องเป้าหมายเปิดอยู่ก็ได้



การสแกนขั้นสูงจำเป็นต้องใช้สิทธิของผู้ดูแลระบบดังนั้นให้พิมพ์ sudo นำหน้า ตัวอย่างเช่น

sudo nmap -v -sT -sU -O scanme.nmap.org == > ใช้เวลานาน 15-20 นาทีในการรัน

```
Initiating Connect Scan at 23:16
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to max_successful_tryno increase to 4
Discovered open port 9929/tcp on 45.33.32.156
Completed Connect Scan at 23:17, 25.47s elapsed (1000 total ports)
Initiating Service scan at 23:17
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 23:17, 6.48s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.88s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.79s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) (1)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu)) (2)
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 5.0 (94%), Linux 5.4 (94%), Linux 5.0 - 5.4 (94%), HP P2000 G3 NAS device (93%), Linux 4.15 - 5.
6 (92%), Linux 5.3 - 5.4 (92%), Linux 2.6.32 - 3.13 (92%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.1 (91%), Ubiquiti AirMax Nano
Station WAP (Linux 2.6.32) (91%) (3)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.162 days (since Wed Mar 10 18:23:46 2021) (4)
Network Distance: 16 hops
TCP Sequence Prediction: Difficulty=238 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.05 seconds
           Raw packets sent: 54 (4.068KB) | Rcvd: 28 (2.500KB)
```

จากผลการทดลองจะเป็นว่า nmap สามารถแสดงเวอร์ชันของบริการ (Service) ที่ทำงานบนแต่ละพอร์ต ความน่าจะเป็นของระบบปฏิบัติของเซิร์ฟเวอร์ที่ใช้โฮสต์เว็บไซต์

command-line flags ที่น่าสนใจ

-sT เพื่อดูพอร์ต TCP

-sU เพื่อดูพอร์ต UDP

-O เพื่อดูระบบปฏิบัติการ (Operating system) ของเครื่องเป้าหมาย

สามารถหาข้อมูลเพิ่มเติมเกี่ยวกับการใส่ค่า command-line flags ได้จาก

https://nmap.org/book/port-scanning-options.html

ชื่อ-นามสกุล อัลกนต์ ทนมั่นย์ รหัสนักศึกษา 660406263739

คำถามท้ายการทดลอง

1. เครื่อง Windows Server 2008 R2 Standard เปิด port อะไรบ้าง

135/tcp msrpc	49152/tcp	49156/tcp
139/tcp netbios-ssn	49153/tcp	49157/tcp
445/tcp microsoft-ds	49154/tcp	49158/tcp
3389/tcp ms-wbt-server	49155/tcp	

2. พิมพ์คำสั่ง sudo nmap -A scanme.nmap.org

ผลที่ได้บอกข้อมูลอะไรบ้าง

1.) ข้อมูลพื้นฐานของเป้าหมาย

2) พอร์ตที่เปิด เช่น 21/tcp 22/tcp 80/tcp

3) รายละเอียด service เช่น version และ web server

4) SSH-keys

5) ค้นสิ่งอ่อนแอ

6) OS

7) ข้อมูล webserver

8) Traceroute

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-09 03:15 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
21/tcp    open  tcpwrapped
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
OS fingerprint not ideal because: Host distance (15 network hops) is greater
than five
No OS matches for host
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   3.43 ms  172.20.10.1
2   ...
3   29.87 ms 192.168.8.193
4   30.28 ms 10.118.210.16
5   29.10 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.46 seconds
```

3. คำสั่งใดใน nmap ที่นักศึกษาคิดว่าน่าใช้มากที่สุด เพราะเหตุใด

nmap -sS -sV เพราะ: เป็นการแสกนแบบ stealthy แม่นยำ และเร็ว สามารถได้ข้อมูลเยอะ

ชื่อ-นามสกุล อดิศักดิ์ หนูพันธ์ รหัสนักศึกษา 6604062636739

NMAP CHEATSHEET

Scan Types

-sS : TCP SYN(Stealth) Scan
-sT : TCP Connect Scan
-sS : UDP Scan
-sS : ACK Scan
-sS : Null Scan
-sS : Xmas Scan

Host Discovery

-sn : Ping Scan
-Pn : Skip host discovery
-PS : TCP SYN ping
-PE : ICMP Echo ping

Output Formats

-oN : Normal Output
-oX : XML Output
-oG : Grepable Output
-oA : Output in all formats

Useful Commands

nmap -v : Verbose Mode
nmap -6 : IPv6 scan
nmap --reason : show reasons of Host
nmap --open : Show only open ports

Timing and Performance

-T0 to -T5 : Version Detection
--min-rate / --max-rate : OS Detection

Port Specification

-p 80 : Scan specific port
-p 1-1000 : Scan port range
--top-ports 100 : Scan top 100 ports

Service and OS Detection

-sV : Version Detection
-O : OS Detection
--osscan-guess : Guess OS aggressively

Script Scanning (NSE)

-sC : Default scripts
--script=scriptname : Run specific script
--script=vuln : Run vulnerability scripts

Bypass Firewalls/IDS

-f : Fragment Packets
--data-length : Append random data
--source-port : Set source port(e.g, 53)