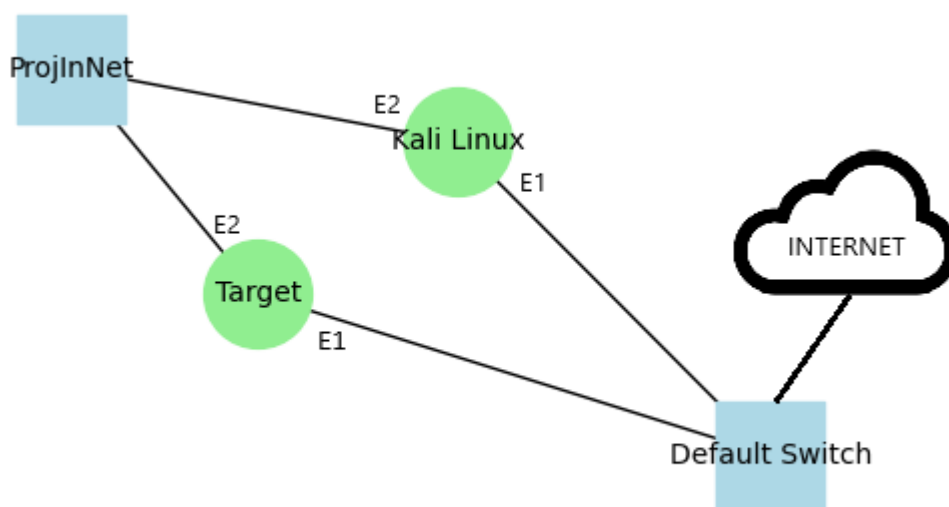


Security: Nmap: podstawy

Zadanie 1

Infrastruktura wirtualna wykorzystana do wykonania zadania



Schemat środowiska

wirtualnego

Do wykonania tego zadania wykorzystano następujące środowisko wirtualne:

- Hypervisor: Hyper-V 10.0.26100.1882
- Maszyna Target: Ubuntu 24.04 Noble Numbat
- Maszyna Kali Linux: Kali GNU/Linux 2024.4
- Switch wirtualny ProjInNet: wirtualny switch dodany do hyper-v na cele tego przedmiotu
- Switch wirtualny Default Switch: jest to switch który działa jak prosty router NAT i pozwala na dostęp do internetu z maszyn wirtualnych

Adresacja IP od strony switcha ProjInNet:

- Kali Linux - 10.10.10.1
- Target - 10.10.10.254

Treść:

Uruchom dwie maszyny (A – maszyna ofiary, B – maszyna atakującego).
Na maszynie A uruchom serwer Apache

Uruchom skanowanie maszyny (hosta) A z maszyny B za pomocą programu nmap.

Opcje uruchomienia programu nmap:

-sT – połączenie TCP

-p – numer portu

-O – zbieranie informacji o systemie operacyjnym

Składnia wywołania programu nmap:

nmap -sT -p 80 -O -v adres_IP_ofiary

Wyniki skanowania zapisz w sprawozdaniu.

Rozwiązanie:

```
kali@kali:~$ ping 10.10.10.254
PING 10.10.10.254 (10.10.10.254) 56(84) bytes of data.
64 bytes from 10.10.10.254: icmp_seq=1 ttl=64 time=0.348 ms
64 bytes from 10.10.10.254: icmp_seq=2 ttl=64 time=0.383 ms
64 bytes from 10.10.10.254: icmp_seq=3 ttl=64 time=0.700 ms
64 bytes from 10.10.10.254: icmp_seq=4 ttl=64 time=0.769 ms
^C
--- 10.10.10.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.348/0.550/0.769/0.186 ms

kali@kali:~$ nmap -sT -p 80 -O -v 10.10.10.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 09:03 EST
Initiating ARP Ping Scan at 09:03
Scanning 10.10.10.254 [1 port]
Completed ARP Ping Scan at 09:03, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:03
Completed Parallel DNS resolution of 1 host. at 09:03, 0.02s elapsed
Initiating Connect Scan at 09:03
Scanning 10.10.10.254 [1 port]
Discovered open port 80/tcp on 10.10.10.254
Completed Connect Scan at 09:03, 0.00s elapsed (1 total ports)
Initiating OS detection (try 1) against 10.10.10.254
Nmap scan report for 10.10.10.254
Host is up (0.00058s latency).

# --- Tutaj poniżej możemy zaobserwować serwis który sprawdzaliśmy
# --- Możemy również zauważyć że działa poprawnie

PORT      STATE SERVICE
80/tcp    open  http   # tutaj widzimy port/protokół warstwy transportowej
          status oraz rodzaj serwisu odkrytego przez NMAPa
MAC Address: 00:15:5D:38:01:1C (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 7.024 days (since Sun Feb 23 08:29:33 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
```

```
Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
Raw packets sent: 23 (1.806KB) | Rcvd: 15 (1.278KB)
```

```
kali@kali:~$
```

Zadanie 2

Treść:

Zadanie 2:

1. Uruchom dwie maszyny (A – maszyna ofiary, B – maszyna atakującego).

Na maszynie A uruchom usługi http (serwer Apache; apache2), ftp (vsftpd),
ssh, smtp (exim4)

2. Sprawdź czy usługi rzeczywiście działają wydając polecenia `lsof -i` a następnie `netstat -ltu`

Wynik z wykonania wyżej wymienionych poleceń umieść w sprawozdaniu.

3. Uruchom skanowanie portów z maszyny B za pomocą programu nmap:

```
nmap -sT -Pn -p 1-1024 -v adres_IP_ofiary
```

Wyniki skanowania zapisz w sprawozdaniu.

Odpowiedz na pytania:

Pytanie 1: Czy udało się wykryć wszystkie usługi ?

Pytanie 2: Co oznacza opcja `-Pn`? Dlaczego warto jej używać ?

Odpowiedzi zapisz w sprawozdaniu.

Rozwiązanie:

```
kali@kali:~$ nmap -sT -p 1-1024 -v 10.10.10.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 09:13 EST
Initiating ARP Ping Scan at 09:13
Scanning 10.10.10.254 [1 port]
Completed ARP Ping Scan at 09:13, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:13
Completed Parallel DNS resolution of 1 host. at 09:13, 0.02s elapsed
Initiating Connect Scan at 09:13
```

```
Scanning 10.10.10.254 [1024 ports]
Discovered open port 22/tcp on 10.10.10.254
Discovered open port 80/tcp on 10.10.10.254
Discovered open port 21/tcp on 10.10.10.254
Completed Connect Scan at 09:13, 0.02s elapsed (1024 total ports)
Nmap scan report for 10.10.10.254
Host is up (0.00029s latency).
Not shown: 1021 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp      # usługa VSFTPD
22/tcp    open  ssh      # usługa open ssh server
80/tcp    open  http     # usługa apache2 z poprzedniego zadania
MAC Address: 00:15:5D:38:01:1C (Microsoft)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

kali@kali:~$
```

Odpowiedzi na pytania

Czy udało się wykryć wszystkie usługi ?

Nie nie widać usługi EXIM4 (serwer poczty SMTP). Może to być związane z tym że nie wykonywałem żadnej dodatkowej konfiguracji EXIM4 na maszynie Target.

Co oznacza opcja -Pn? Dlaczego warto jej używać ?

Ten parametr służy do wyłączenia usługi wykrywania hostów za pomocą mechanizmu PING. Pozwala to na skanowanie hosta nawet jeżeli nie odpowiada na polecenie PING. Zaleca się stosowanie tego parametru wtedy gdy skanowana sieć jest ściśle zabezpieczona i ma np. zablokowane ICMP. Niestety ale może wydłużyć skanowanie.

Zadanie 3

Treść:

Zadanie 3:

Uruchom skanowanie z maszyny B wpisując poniższe polecenie w linii komend:

```
nmap -sV -Pn -p 1-1024 -v adres_IP_ofiary
```

Wyniki skanowania zapisz w sprawozdaniu.

Odpowiedz na pytanie:

Pytanie 3: Co oznacza opcja -sV ?

Odpowiedź zapisz w sprawozdaniu.

Rozwiązanie:

```
kali@kali:~$ nmap -sV -Pn -p 1-1024 -v 10.10.10.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 09:27 EST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 09:27
Scanning 10.10.10.254 [1 port]
Completed ARP Ping Scan at 09:27, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:27
Completed Parallel DNS resolution of 1 host. at 09:27, 0.03s elapsed
Initiating SYN Stealth Scan at 09:27
Scanning 10.10.10.254 [1024 ports]
Discovered open port 21/tcp on 10.10.10.254
Discovered open port 80/tcp on 10.10.10.254
Discovered open port 22/tcp on 10.10.10.254
Completed SYN Stealth Scan at 09:27, 0.04s elapsed (1024 total ports)
Initiating Service scan at 09:27
Scanning 3 services on 10.10.10.254
Completed Service scan at 09:27, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.10.254.
Initiating NSE at 09:27
Completed NSE at 09:27, 0.01s elapsed
Initiating NSE at 09:27
Completed NSE at 09:27, 0.00s elapsed
Nmap scan report for 10.10.10.254
Host is up (0.00025s latency).
Not shown: 1021 closed tcp ports (reset)
```

Tym razem poniżej możemy zaobserwować dużo więcej informacji na temat uruchomionych serwisów

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 00:15:5D:38:01:1C (Microsoft)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
Raw packets sent: 1025 (45.084KB) | Rcvd: 1025 (41.000KB)
```

```
kali@kali:~$
```

Odpowiedzi na pytania

Co oznacza opcja -sV ?

Parametr ten powoduje że NMAP wykrywa jaka jest odpowiedź serwera na danym porcie i w swojej bazie danych wyszukuje odpowiedzi na to jaka to może być wersja oprogramowania serwerowego.