

ЛАБОРАТОРНА РОБОТА 3

Тема: Безпека ресурсів мережі

Мета: Дослідження безпеки вузлів в мережі за допомогою nmap

ПРАКТИЧНА ЧАСТИНА

Nmap (“Network Mapper”) це утиліта з відкритим кодом для дослідження мережі та перевірки безпеки вузлів. Її було розроблено для швидкого сканування великих мереж, але вона може застосовуватись і для одиничних цілей.

Nmap використовує необроблені IP пакети у оригінальний спосіб, для визначення які вузли (хости) доступні у мережі, які сервіси (назва додатку та версія) вони використовують, які операційні системи (тип та версії ОС) вони використовують, які типи пакетних фільтрів/брандмауерів використовуються та інші характеристики. Зазвичай Nmap використовується для перевірки безпеки, але вона також може бути корисною для звичайних задач, таких як контролювання структури мережі, керування розкладом запуску сервісів та облік часу роботи вузлу (хосту) або сервісу.

1. Для визначення активних вузлів у мережі без сканування відкритих у них портів nmap запускається з наступними параметрами (приклад для мережі 192.168.1.0/24)

```
nmap -sn 192.168.1.0/24
```

Відповідь формується тільки з доступних вузлів:

```
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0067s latency).
Nmap scan report for 192.168.0.100
Host is up (0.079s latency).
Nmap scan report for 192.168.0.101
Host is up (0.077s latency).
Nmap scan report for 192.168.0.105
Host is up (0.016s latency).
Nmap scan report for 192.168.0.106
Host is up (0.0077s latency).
Nmap scan report for 192.168.0.107
Host is up (0.0077s latency).
Nmap scan report for 192.168.0.109
Host is up (0.0077s latency).
Nmap scan report for 192.168.0.110
Host is up (0.011s latency).
Nmap done: 255 IP addresses (8 hosts up) scanned in 2.88 seconds
```

2. Для певного вузла можна визначити тип операційної системи, для чого використовується ключ -A:

```
nmap -A 192.168.0.110
```

Відповідь може містити як назву операційної системи, її версію, так і стан та доступність специфічних для неї портів:

```
Nmap scan report for 192.168.0.110
Host is up (0.015s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE          VERSION
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp    closed https
445/tcp    open  microsoft-ds    Windows XP microsoft-ds
2869/tcp   open  http            Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/1.0
|_http-title: Site doesn't have a title (text/html).
5800/tcp   closed vnc-http
5900/tcp   closed vnc
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -1h30m00s, deviation: 2h07m16s, median: -3h00m00s
|_nbstat: NetBIOS name: HOME-SFQWABF53D, NetBIOS user: <unknown>, NetBIOS MAC: 00:1b:9e:4f:f4:6e (Askey Computer)
|_smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: home-sfqwabf53d
|   NetBIOS computer name: HOME-SFQWABF53D\x00
|   Workgroup: MSHOME\x00
|_  System time: 2021-04-19T20:40:39+03:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.17 seconds
```

За допомогою 153 скриптів nmap визначає доступні сервіси на вузлі. Для цього необхідно скористатись наступною командою:

```
nmap -v -A 192.168.0.110
```

Для визначення захищеності вузла або мережі фаєрволом (не працює при використанні WiFi) використовується команда

```
nmap -sA 192.168.1.110
```

Якщо вузол захищено фаєрволом, то його порти можна просканувати за допомогою команди

```
nmap -Pn 192.168.1.110
```

3. Отримати повну інформацію про інтерфейси та маршрути вузла, на якому запускається команда, можна за допомогою:

nmap --iflist

```
*****INTERFACES*****
DEV          (SHORT)          IP/MASK          TYPE    UP  MTU  MAC
lo           (lo)             127.0.0.1/8     loopback up  65536
lo           (lo)             ::1/128         loopback up  65536
enp0s25     (enp0s25)       (none)/0       ethernet up  1500  10:1F:74:F0:07:7C
enx028037ec0200 (enx028037ec0200) (none)/0       ethernet up  1500  02:80:37:EC:02:00
wlo1        (wlo1)          192.168.0.111/24 ethernet up  1500  24:77:03:51:BD:E8
wlo1        (wlo1)          fe80::412c:77da:cdee:7311/64 ethernet up  1500  24:77:03:51:BD:E8
docker0     (docker0)       172.17.0.1/16   ethernet up  1500  02:42:FC:48:22:86

*****ROUTES*****
DST/MASK    DEV    METRIC GATEWAY
192.168.0.0/24 wlo1    600
172.17.0.0/16  docker0 0
169.254.0.0/16 wlo1    1000
0.0.0.0/0     wlo1    600    192.168.0.1
::1/128      lo      0
fe80::412c:77da:cdee:7311/128 wlo1    0
::1/128      lo      256
fe80::/64    wlo1    600
ff00::/8     wlo1    256
```

4. Сканування усіх портів певного вузла можна виконати за допомогою наступної команди

```
nmap -p "1-" 192.168.0.110
```

Результат сканування, наприклад, може виглядати наступним чином:

```
Nmap scan report for 192.168.0.110
Host is up (0.019s latency).
Not shown: 65529 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds
2869/tcp  closed icslap
5800/tcp  closed vnc-http
5900/tcp  closed vnc

Nmap done: 1 IP address (1 host up) scanned in 135.27 seconds
```

Для визначення номеру версії віддалених сервісів можна виконати команду

```
nmap -sV 192.168.1.110
```

```

Nmap scan report for 192.168.0.110
Host is up (0.0090s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE          VERSION
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
2869/tcp  closed iclslap
5800/tcp  closed vnc-http
5900/tcp  closed vnc
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds

```

Завдання

1. Визначте мережеву конфігурацію комп'ютера, за яким виконується лабораторна робота і занесіть її у звіт.
2. Виконайте сканування підмережі цього комп'ютера (приклад у пункті 1) і його результат занесіть у звіт.
3. Для проведення наступних експериментів необхідно мати доступ до другого комп'ютера (за його відсутності, встановіть віртуальну машину, інсталюйте на неї операційну систему та налагодіть її мережеве з'єднання).
4. Виконайте дії, що представлено в 2-4 пунктах практичної частини, до обраного (другого) комп'ютера. Їх результат занесіть у звіт.
5. Встановіть на другий комп'ютер пакет Wireshark — аналізатор мережевих пакетів та запустіть його під правами рівня системного адміністратора. Запустіть його на захоплення пакетів з опцією "host IP_address", де замість IP_address вкажіть IP адресу цього комп'ютеру.
6. За допомогою наступної команди проскануйте у другого комп'ютера один відкритий порт (за результатом завдання 4) та будь-який порт, що у скануванні не був визначений:

```
nmap -p 80 192.168.0.110
```

де -p 80 — вказує, що сканується порт 80 (http).

Визначить як відбувалось сканування: скільки і які пакети надіслав перший комп'ютер, і які пакети надсилались у відповідь; які прапорці використовували комп'ютери на рівні транспортного протоколу TCP, і що вони означають; в чому різниця між скануванням відкритого порту та невизначеного порту.

7. Налаштуйте Wireshark на захоплення пакетів, як описано вище у п.5. Виконайте сканування портів комп'ютера з маскуванням, яке виконується з використанням фіктивних вузлів для відволікання від реального джерела сканування. Навіть при виявленні факту сканування, як правило, встановити система не може виявити з якої адреси відбувалось справжнє сканування, а які були фіктивними. Загальний вигляд такого запиту:

```
nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3 remote-host-ip
```

Наприклад,

nmap -p 80 -D 10.1.100.5,10.5.1.2,192.168.0.111,3.4.2.1 192.168.0.110

Визначить як відбувалось сканування: скільки і які пакети сканування надійшли до комп'ютера, які IP адреси були у цих пакетів, які пакети надсилались у відповідь.

8. Підготуйте та надайте звіт.

Список рекомендованої літератури

1. Э.Таненбаум. Компьютерные сети / Э.Таненбаум, Д.Уэзеролл. – СПб: Питер, 2012. – 1104с.
2. <http://nmap.org>