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

Технічний аудит

Лабораторна робота №2

Активне сканування та перерахування

Перевірив:
Котов Д. О.

Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.
Приходько І. Ю.
Корабельський Т. Б.

Київ 2023

1. Загальні методи сканування

Мета: зрозуміти процес сканування

Після роботи студент повинен

- **знати:** як виконується сканування;
- **вміти:** проводити різні види сканування, а також вміти пояснити результати.

Завдання:

- відсканувати сайт scanme.nmap.org
- відсканувати свою домашню мережу
- надати інформацію про служби, що працюють на віддаленій машині

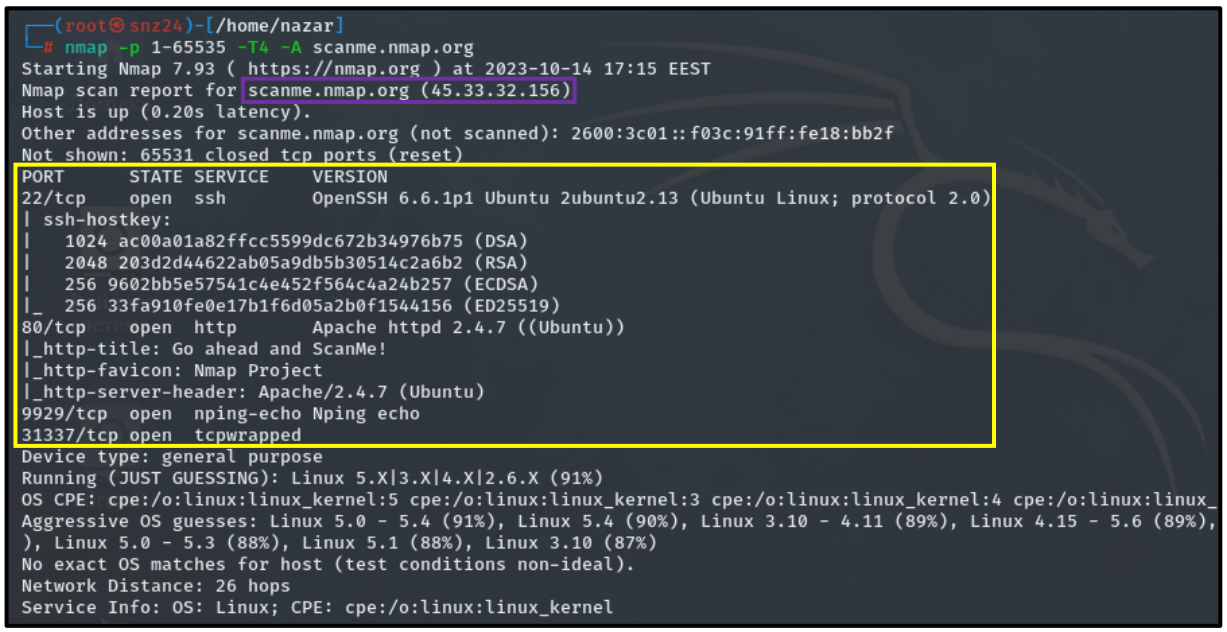
ЗАВДАННЯ 1

Виконайте всі види відомих сканувань на запропонованому хості. Скільки портів TCP відкрито на кожному? Чи відкриті UDP – порти на будь-якій з сканованих машині? Доведіть це за допомогою скріншотів.

Відповідь:

- Веб-сайт **scanme.nmap.org**

1. Скільки портів TCP відкрито на кожному?



```
TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   2.65 ms   RT-AX55-0590 (192.168.50.1)
2   4.52 ms   94.158.81.1
3   ...
4   5.36 ms   10.255.240.2
5   4.97 ms   fatb.maximuma.net (91.196.148.13)
6   4.46 ms   91.196.148.30
7   ...
8   4.46 ms   10.255.249.1
9   4.83 ms   172.27.0.0
10  15.94 ms  ae0-13.RT.LDC.WAW.PL.retn.net (87.245.233.56)
11  16.54 ms  ix-ae-35-0.tcore1.w1t-warsaw.as6453.net (80.231.124.38)
12  110.07 ms if-ae-28-2.tcore2.av2-amsterdam.as6453.net (80.231.152.170)
13  112.28 ms if-ae-14-2.tcore2.l78-london.as6453.net (80.231.131.160)
14  109.93 ms if-ae-2-2.tcore1.l78-london.as6453.net (80.231.131.2)
15  ... 16
17  114.46 ms 66.198.111.67
18  112.45 ms ae2.r02.ewr01.icn.netarch.akamai.com (23.203.154.40)
19  128.59 ms ae8.r02.ord01.icn.netarch.akamai.com (23.32.63.48)
20  178.01 ms ae4.r02.sjc01.icn.netarch.akamai.com (23.32.63.27)
21  178.45 ms ae2.r11.sjc01.ien.netarch.akamai.com (23.207.232.39)
22  348.01 ms a23-203-158-51.deploy.static.akamaitechnologies.com (23.203.158.51)
23  ... 25
26  347.75 ms scanme.nmap.org (45.33.32.156)

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 1784.80 seconds
```

2. Чи відкриті UDP – порти на будь-якій з сканованих машині?

```
┌──(root㉿snz24)-[/home/nazar]
└─# sudo nmap -sU -p 1-1024 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-14 18:06 EEST
Stats: 0:03:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 18.53% done; ETC: 18:23 (0:13:51 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 1020 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
123/udp open          ntp
319/udp open|filtered ptp-event
320/udp open|filtered ptp-general

Nmap done: 1 IP address (1 host up) scanned in 1117.81 seconds
```

- Домашня мережа **192.168.50.0/24**

1. Скільки портів TCP відкрито на кожному?

```
┌──(root㉿snz24)-[/home/nazar]
└─# nmap -p 1-65535 -T4 -A 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-14 15:49 EEST
Nmap scan report for RT-AX55-0590 (192.168.50.1)
Host is up (0.0038s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
53/tcp    open     domain        Cloudflare public DNS
80/tcp    open     http          ASUS WRT http admin
|_http-server-header: httpd/2.0
|_http-title: Site doesn't have a title (text/html).
5152/tcp  filtered sde-discovery
7788/tcp  open     unknown
8443/tcp  open     ssl/http      ASUS WRT http admin
|_http-server-header: httpd/2.0
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=router.asus.com/countryName=US
| Subject Alternative Name: DNS:router.asus.com
| Not valid before: 2018-05-05T05:05:14
|_Not valid after:  2028-05-05T05:05:14
|_http-title: Site doesn't have a title (text/html).
18017/tcp open     http          Asus wanduck WAN monitor httpd
|_http-server-header: wanduck
```

```
33686/tcp open     upnp          MiniUPnP 2.2.0 (AsusWRT 386; UPnP 1.1)
49152/tcp open     upnp          Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
58094/tcp open     sip           PJSUA v1.12.0/arm-unknown-linux-gnu (Status: 405 Method Not Allowed)
|_sip-methods: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, MESSAGE, OPTIONS
| fingerprint-strings:
|   SIPOptions:
|     SIP/2.0 405 Method Not Allowed
|     Via: SIP/2.0/TCP nm;received=192.168.50.97;branch=foo
|     Call-ID: 50000
|     From: <sip:nm@nm>;tag=root
|     <sip:nm2@nm2>;tag=foo
|     CSeq: 42 OPTIONS
|     Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, MESSAGE, OPTIONS
|     User-Agent: PJSUA v1.12.0/arm-unknown-linux-gnu
|_    Content-Length: 0
58095/tcp open     ssl/unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fi
SF-Port58094-TCP:V=7.93%I=7%D=10/14%Time=652A93CF%P=x86_64-pc-linux-gnu%r(
SF:SIPOptions,139,"SIP/2\.0\x20405\x20Method\x20Not\x20Allowed\r\nVia:\x20
SF:SIP/2\.0/TCP\x20nm;received=192\.168\.50\.97;branch=foo\r\nCall-ID:\x20
SF:50000\r\nFrom:\x20<sip:nm@nm>;tag=root\r\nTo:\x20<sip:nm2@nm2>;tag=foo\
SF:r\nCSeq:\x2042\x20OPTIONS\r\nAllow:\x20PRACK,\x20INVITE,\x20ACK,\x20BYE
SF:,\x20CANCEL,\x20UPDATE,\x20MESSAGE,\x20OPTIONS\r\nUser-Agent:\x20PJSUA\
SF:x20v1\.12\.0/arm-unknown-linux-gnu\r\nContent-Length:\x20\x200\r\n\r\n"
SF:);
MAC Address: 7C:10:C9:2E:05:90 (Asustek Computer)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
Network Distance: 1 hop
Service Info: Device: WAP; CPE: cpe:/o:asus:wrt_firmware, cpe:/o:asus:asuswrt:386, cpe:/h:cisco:e4200

TRACEROUTE
HOP RTT      ADDRESS
1   3.80 ms RT-AX55-0590 (192.168.50.1)

Nmap scan report for S20-koristuvaca-FB-01-Sahnij (192.168.50.30)
Host is up (0.0080s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
1467/tcp open  ssl/csdmbase?
|_ssl-date: TLS randomness does not represent time
8300/tcp open  tmi?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fi
SF-Port8300-TCP:V=7.93%I=7%D=10/14%Time=652A9370%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,2,"\r\n");
MAC Address: 9A:C8:AB:3D:B0:05 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=10/14%OT=1467%CT=1%CU=43220%PV=Y%DS=1%DC=D%G=Y%M=9AC8A
OS:B%TM=652A9420%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%I
OS:I=I%TS=9)OPS(O1=M5B4ST11NWA%O2=M5B4ST11NWA%O3=M5B4NNT11NWA%O4=M5B4ST11NW
OS:A%O5=M5B4ST11NWA%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF
OS:%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NNSNWA%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D
OS:FI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   7.98 ms S20-koristuvaca-FB-01-Sahnij (192.168.50.30)

Nmap scan report for DESKTOP-DRI0PBB (192.168.50.48)
Host is up (0.00060s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
5040/tcp open  unknown
5357/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
7680/tcp open  pando-pub?
MAC Address: F8:A2:D6:58:08:F9 (Liteon Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|firewall|router
Running (JUST GUESSING): FreeBSD 6.X (98%), Microsoft Windows 10|2008 (91%), Juniper JUNOS 12.X|9.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:
:/o:juniper:junos:12.1 cpe:/o:juniper:junos:12 cpe:/o:juniper:junos:9.0r2.10
Aggressive OS guesses: FreeBSD 6.2-RELEASE (98%), Microsoft Windows 10 (91%), Microsoft Windows Server 2008 or
, Juniper SRX-series firewall (JUNOS 12.1) (88%), Juniper Networks JUNOS 12 (88%), Juniper Networks JUNOS 9.0R2
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1   0.60 ms DESKTOP-DRI0PBB (192.168.50.48)
```

```
Nmap scan report for snz24 (192.168.50.97)
Host is up (0.00011s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.4p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   256 db368105ebb125e1f50dad09693629ca (ECDSA)
|_  256 53c6bcace408f8ab2d4f13c3bff4d536 (ED25519)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.2
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 1507.03 seconds
```

2. Чи відкриті UDP – порти на будь-якій з сканованих машині?

```
┌──(root㉿snz24)-[/home/nazar]
└─# sudo nmap -sU -p 1-1024 192.168.50.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-14 16:44 EEST
Nmap scan report for RT-AX55-0590 (192.168.50.1)
Host is up (0.0031s latency).
Not shown: 1022 closed udp ports (port-unreach)
PORT   STATE SERVICE
53/udp open  domain
67/udp open  dhcps
MAC Address: 7C:10:C9:2E:05:90 (Asustek Computer)

Nmap scan report for S20-koristuvaca-FB-01-Sahnij (192.168.50.30)
Host is up (0.30s latency).
Not shown: 1023 closed udp ports (port-unreach)
PORT    STATE         SERVICE
137/udp open|filtered netbios-ns
MAC Address: 9A:C8:AB:3D:B0:05 (Unknown)

Nmap scan report for DESKTOP-DRI0PBB (192.168.50.48)
Host is up (0.0011s latency).
Not shown: 1023 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: F8:A2:D6:58:08:F9 (Liteon Technology)

Nmap scan report for 192.168.50.113
Host is up (0.0032s latency).
All 1024 scanned ports on 192.168.50.113 are in ignored states.
Not shown: 1024 closed udp ports (port-unreach)
MAC Address: BC:14:85:15:73:FC (Samsung Electronics)

Nmap scan report for HUAWEI_P20_lite-2441f35f4 (192.168.50.248)
Host is up (0.27s latency).
Not shown: 1022 closed udp ports (port-unreach)
PORT    STATE         SERVICE
67/udp  open|filtered dhcps
405/udp open|filtered ncld
MAC Address: B4:CD:27:11:D5:5C (Huawei Technologies)

Nmap scan report for snz24 (192.168.50.97)
Host is up (0.0000060s latency).
All 1024 scanned ports on snz24 (192.168.50.97) are in ignored states.
Not shown: 1024 closed udp ports (port-unreach)

Nmap done: 256 IP addresses (6 hosts up) scanned in 1116.11 seconds
```

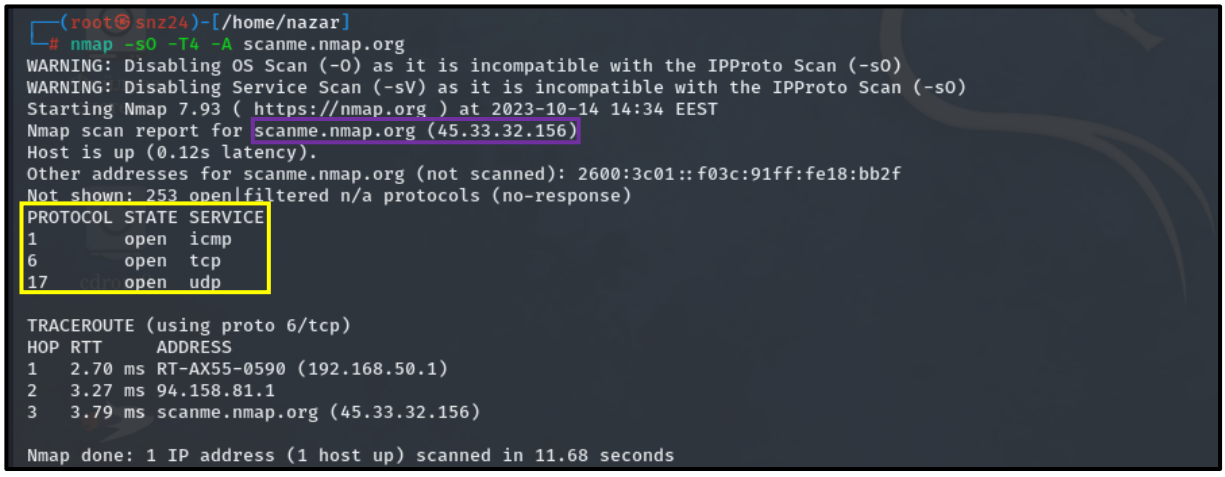
ЗАВДАННЯ 2

Виконайте сканування протоколу IP (з параметром -sO). Чи відрізняються результати від тих, що були досягнуті на попередньому кроці? Поясніть. Доведіть за допомогою скріншотів.

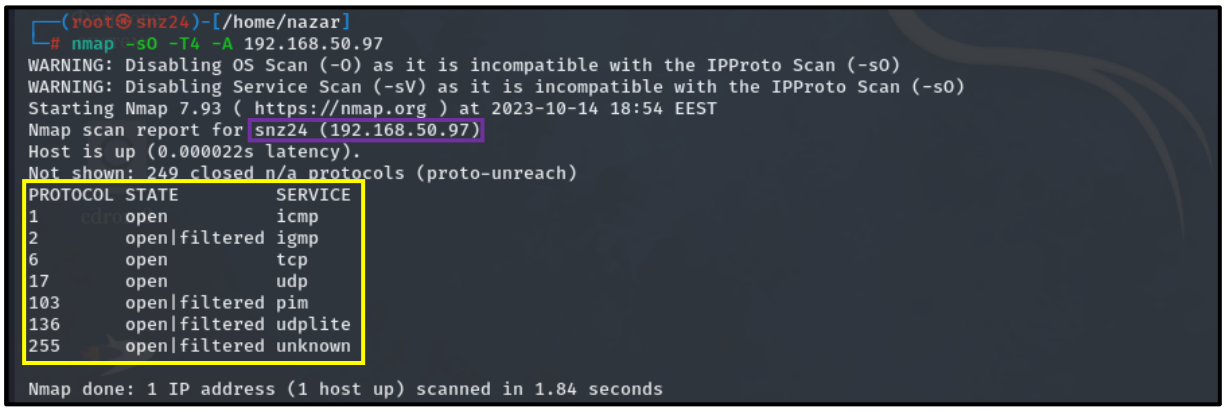
Відповідь:

Результати обох команд будуть різними в залежності від їхніх цілей. Попередній скан був спрямований на визначення відкритих портів та додаткової інформації про сервіси та ОС на хості, тоді як поточне сканування спрямоване на визначення підтримуваних протоколів IP.

- Веб-сайт **scanme.nmap.org**



- Домашня мережа **192.168.50.0/24**



ЗАВДАННЯ 3

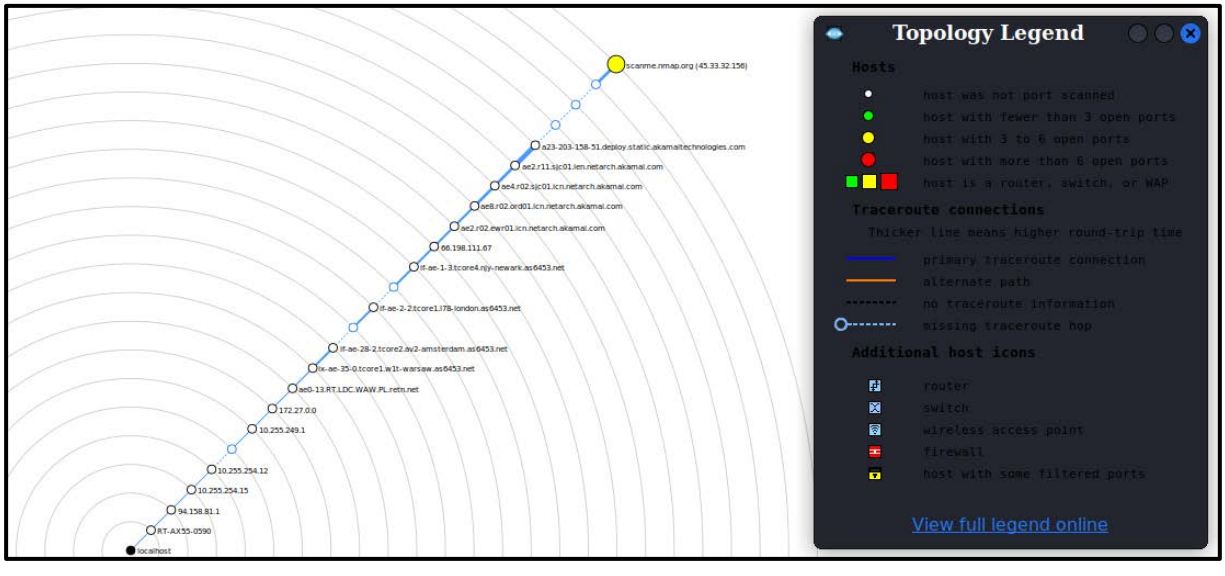
Виконайте визначення версії на сканованому хості. Яка операційна система, на думку nmap, працює на хості? Яка його MAC-адреса? Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост? Доведіть відповіді скріншотами.

Відповідь:

- Веб-сайт **scanme.nmap.org**

1. Яка ОС, на думку nmap, працює на хості? Яка його MAC-адреса?

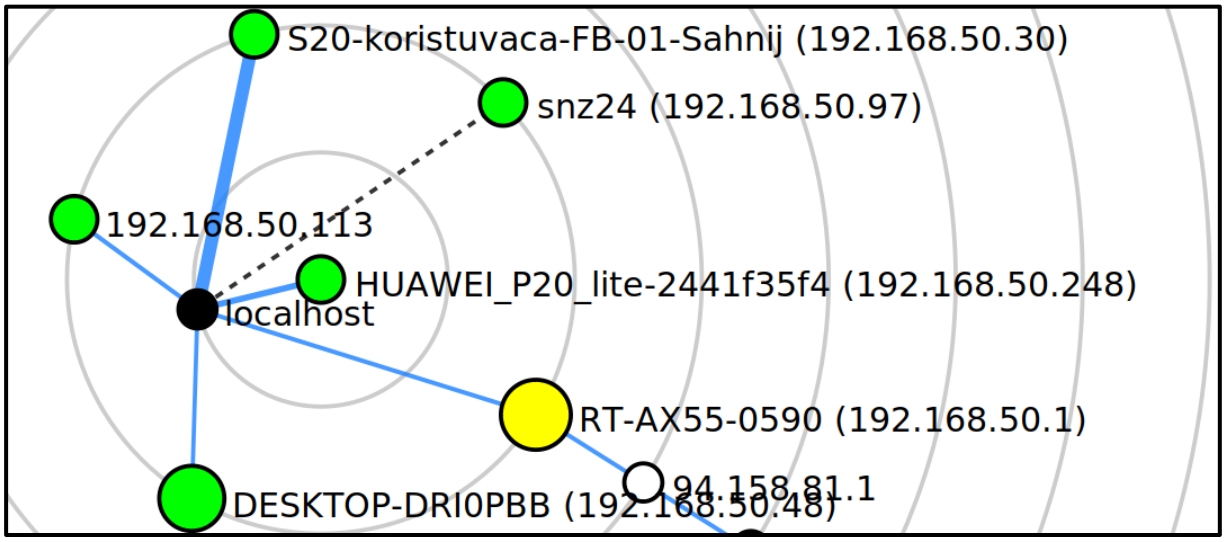
2. Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост?



- Домашня мережа **192.168.50.0/24**

1. Яка ОС, на думку nmap, працює на хості? Яка його MAC-адреса?

2. Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост?



2. Отримати загальну інформацію про вибраний домен за допомогою служби DNS

Мета: зрозуміти процес сканування

Після роботи студент повинен

- **знати:** як виконується сканування;
- **вміти:** проводити різні види сканування, а також вміти пояснити результати.

Завдання:

- Завантажте та встановіть віртуальну машину Metasploitable 2 (https://sourceforge.net/projects/metasploitable/).
- Проведіть сканування Metasploitable 2.
- Отримайте інформацію про служби, що працюють на віртуальній машині Metasploitable

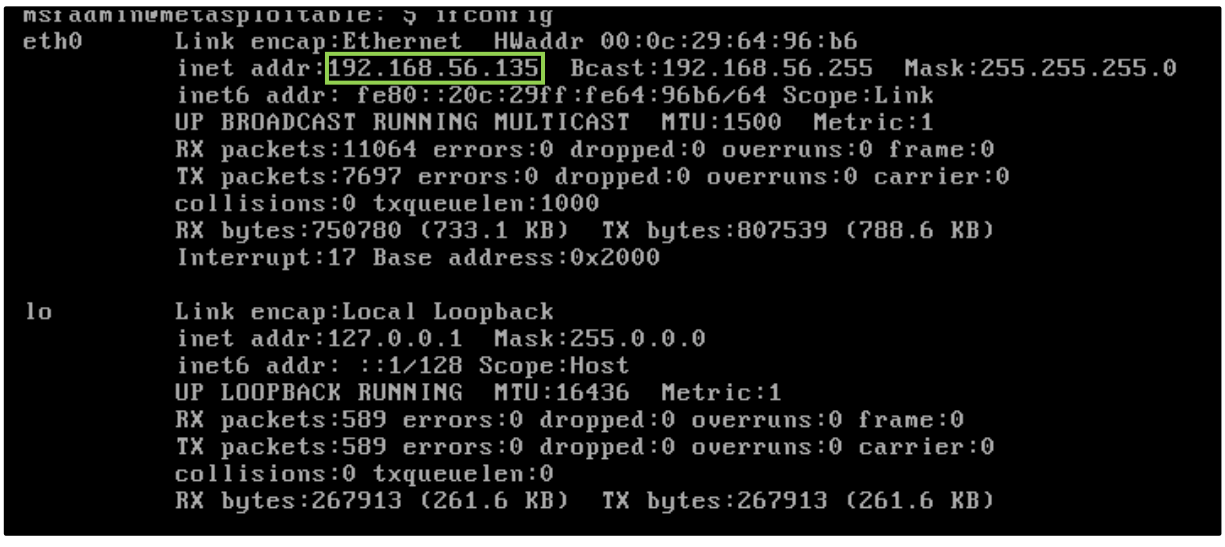
Технічне оснащення робочого місця:

- командна консоль
- утиліти nmap, zenmap

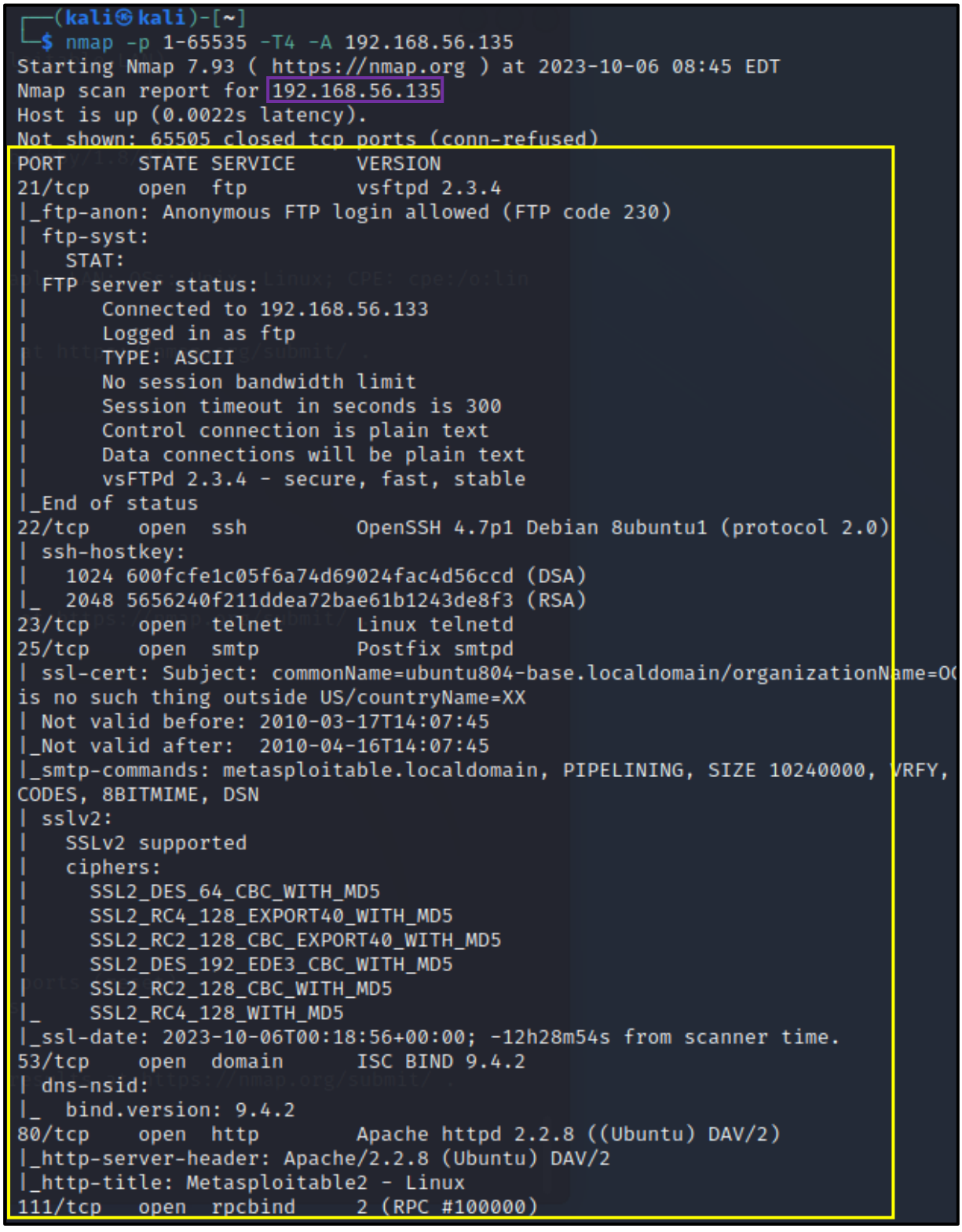
ЗАВДАННЯ 1

Виконайте всі види відомих сканувань на запропонованому хості. Скільки портів TCP відкрито на кожному? Чи відкриті UDP – порти на будь-якій з сканованих машині? Доведіть це за допомогою скріншотів.

Відповідь:



1. Скільки портів TCP відкрито на кожному?



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1-65535 -T4 -A 192.168.56.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 08:45 EDT
Nmap scan report for 192.168.56.135
Host is up (0.0022s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
CODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2023-10-06T00:18:56+00:00; -12h28m54s from scanner time.
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
```

```
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 2
|   servers: 1
|   lusers: 2
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 3:48:32
|   source ident: nmap
|   source host: A985D3F6.97684684.FFFA6D49.IP
|_  error: Closing Link: cncgpkkpu[192.168.56.133] (Quit: cncgpkkpu)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34811/tcp open  java-rmi    GNU Classpath grmiregistry
36445/tcp open  nlockmgr    1-4 (RPC #100021)
51213/tcp open  status      1 (RPC #100024)
53060/tcp open  mountd      1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux;
x:linux_kernel

Host script results:
|_clock-skew: mean: -11h28m54s, deviation: 2h00m00s, median: -12h28m54s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-05T20:18:20-04:00
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -T4 -O -F --version-light 192.168.56.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 09:03 EDT
Nmap scan report for 192.168.56.135
Host is up (0.00041s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login?
514/tcp  open  tcpwrapped
2049/tcp open  rpcbind
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 00:0C:29:64:96:B6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 13.10 seconds
```

2. Чи відкриті UDP – порти на будь-якій з сканованих машині?

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -O -F --traceroute 192.168.56.135
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 14:10 EDT
Nmap scan report for 192.168.56.135
Host is up (0.00033s latency).
Not shown: 53 closed udp ports (port-unreach), 43 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 00:0C:29:64:96:B6 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: proxy server|WAP
Running: Citrix embedded, Linksys embedded
OS CPE: cpe:/h:linksys:wrt610nv3
OS details: Citrix Access Gateway VPN gateway, Linksys WRT610Nv3 WAP
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 192.168.56.135

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.06 seconds
```

ЗАВДАННЯ 2

Виконайте сканування протоколу IP (з параметром -sO). Чи відрізняються результати від тих, що були досягнуті на попередньому кроці? Поясніть. Доведіть за допомогою скріншотів.

Відповідь:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sO -T4 -A 192.168.56.135
WARNING: Disabling OS Scan (-O) as it is incompatible with the IPProto Scan (-sO)
WARNING: Disabling Service Scan (-sV) as it is incompatible with the IPProto Scan (-sO)
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-05 17:13 EDT
Warning: 192.168.56.135 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.56.135
Host is up (0.00050s latency).
Not shown: 194 open|filtered n/a protocols (no-response), 60 closed n/a protocols (proto-unreach)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
MAC Address: 00:0C:29:64:96:B6 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms 192.168.56.135

Nmap done: 1 IP address (1 host up) scanned in 59.60 seconds
```

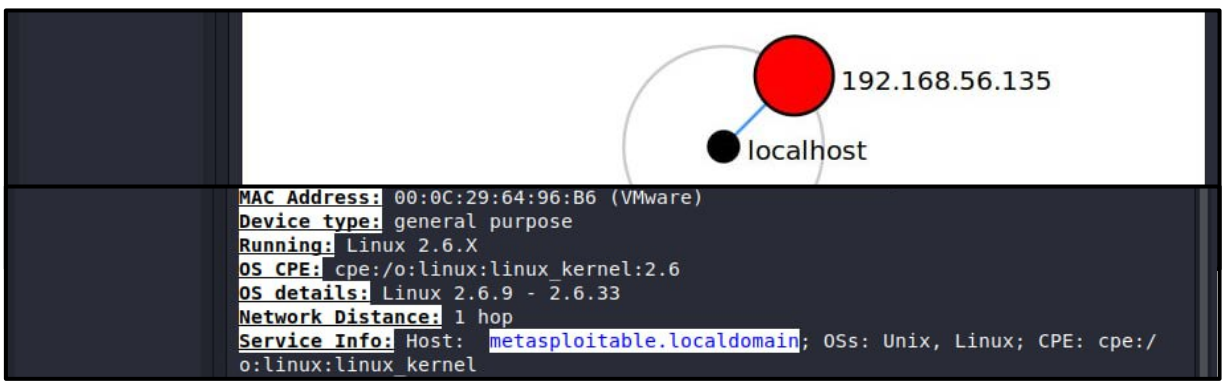
ЗАВДАННЯ 3

Виконайте визначення версії на сканованому хості. Яка операційна система, на думку nmap, працює на хості? Яка його MAC-адреса? Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост? Доведіть відповіді скріншотами.

Відповідь:

1. Яка ОС, на думку nmap, працює на хості? Яка його MAC-адреса?

2. Наскільки далеко знаходиться сканований хост? Між якими хостами знаходиться сканований хост?



3. Ручне та автоматичне перерахування

Мета: Зрозуміти процес перерахування

Після роботи студент повинен

- **знати:** як працює перерахування;
- **вміти:** проводити різні типи перерахувань, та пояснювати результати.

Завдання:

- Перелічити сервіси та користувачів у Metasploitable 2

Технічне оснащення робочого місця:

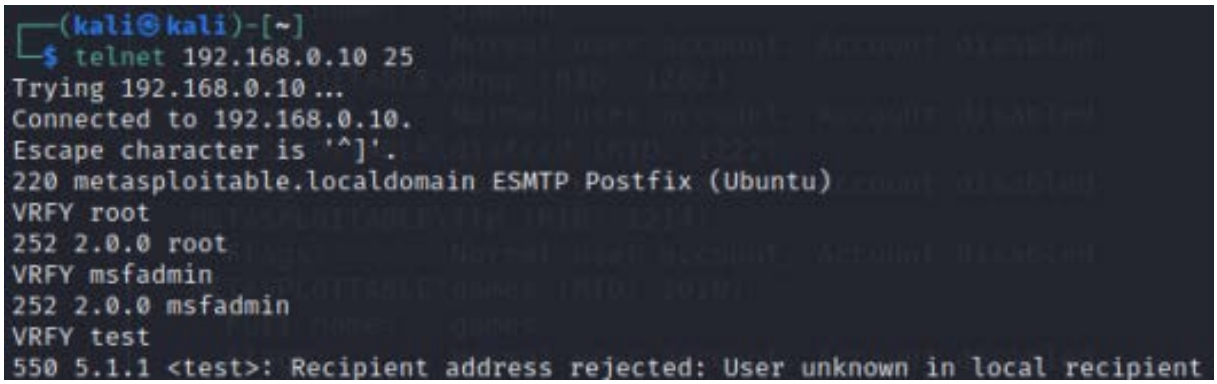
- командна консоль
  - nmap, zenmap, nmap scripts, nc, telnet

ЗАВДАННЯ 1

На основі попередніх результатів сканування спробуйте провести ручне перерахування на Metasploitable VM. Доведіть результати за допомогою скріншотів.

Відповідь:

Для перерахунку користувачів на Metasploitable VM, використаємо команду **telnet** на порт №25, а потім команду **VRFY** msfadmin.

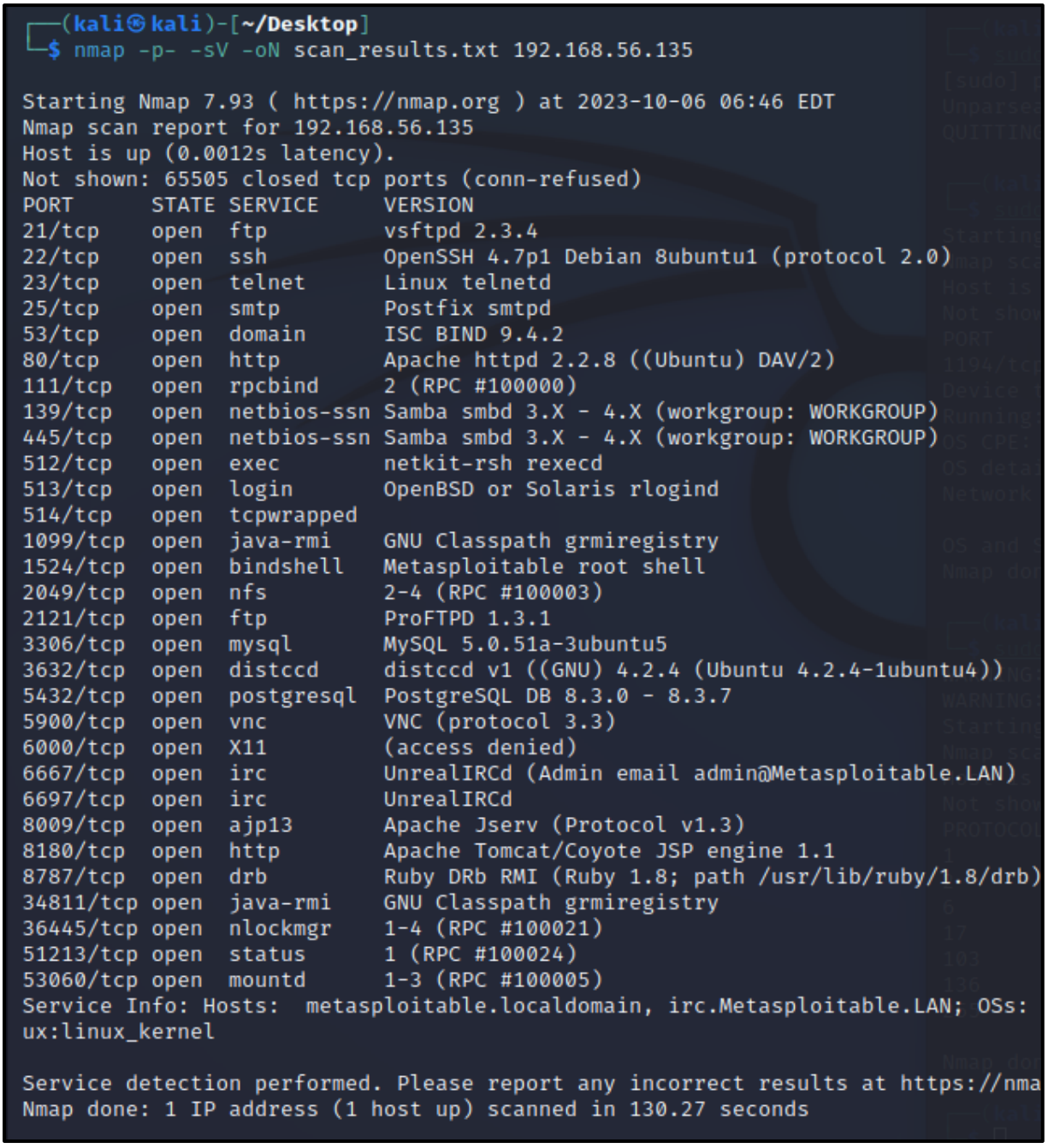


↑ Як бачимо, було знайдено таких користувачів, як root та msfadmin.

ЗАВДАННЯ 2

На основі попередніх результатів сканування спробуйте провести автоматичне перерахування на Metasploitable VM за допомогою скриптів nmap. Доведіть результати за допомогою скріншотів.

Відповідь:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p- -sV -oN scan_results.txt 192.168.56.135

Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 06:46 EDT
Nmap scan report for 192.168.56.135
Host is up (0.0012s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34811/tcp open  java-rmi    GNU Classpath grmiregistry
36445/tcp open  nlockmgr    1-4 (RPC #100021)
51213/tcp open  status      1 (RPC #100024)
53060/tcp open  mountd      1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
ux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
Nmap done: 1 IP address (1 host up) scanned in 130.27 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script smb-enum-users.nse -p 445 192.168.56.135
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 14:30 EDT
Nmap scan report for 192.168.56.135
Host is up (0.00024s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:64:96:B6 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
```

```
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
```

```
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Account disabled, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```