Politechnika Wrocławska, Informatyka Stosowana

Rekonesans sieciowy

Cyberbezpieczeństwo, Laboratorium nr.11 - raport

Autor: Aleksander Stepaniuk
Nr. Indeksu: 272644

4. Pytania

Pytanie 1;

Te wyniki uzyskane przez nmap mogą być wiarygodne (w granicach możliwości narzędzia), ale zależy to od wielu czynników, między innymi od konfiguracji skanowania lub od tego czy system jest odpowiednio skonfigurowany, a także od poziomu zabezpieczeń badanego hosta lub sieci w której się znajduje. Dodatkowo jeżeli host posiada zabezpieczenia firewalla, to ochrona sieci może blokować dostęp do niektórych portów i pokazywać je fałszywie jako zamknięte. Ponadto usługi przypisane do określonych portów mogą różnic się od tych domyślnie rozpoznawanych przez bazę danych nmap.

Pytanie 2;

Uzyskane informacje o hoście docelowym mogą zależeć od opcji skanowania. Opcje które wymagają dostępu administratora umożliwiają bardziej szczegółowe analizy, ponieważ dostarczają więcej różnych danych o portach i usługach tam uruchomionych. Opcja skanowania SYN wykrywa otwarte porty bez pełnego ustanawiania połączenia. Z kolei opcje z wyborem konkretnych flag TCP nawiązują pełne połączenie, ale przez to takie które jest bardziej widoczne. Opcja skanowania wersji próbuje zidentyfikować usługę i jej wersję na danym porcie. Opcja skanowania systemu operacyjnego podejmuje próbę wykrycia systemu operacyjnego. Im bardziej szczegółowe skanowanie tym więcej informacji można uzyskać.

Pytanie 3;

Nie, skanowanie hostów bez pozwolenia może być nielegalne (zależnie od prawa w danym kraju) i traktowane jako próba włamania lub działanie nieautoryzowane. Jednak samo narzędzie nmap jest legalne i można go normalnie używać bez zewnętrznego pozwolenia, o ile nie zakłóca to w żaden sposób działania skanowanego systemu. Zależy to od prawa w danym kraju, ale w wielu miejscach takie działania mogą prowadzić do konsekwencji prawnych.

5. Zadania

Zadanie 0;

Adresy IP maszyn:
Metasploitable: 192.168.188.36
Kali linux: 192.168.188.35
Adres sieci: 192.168.188.0/24

Zadanie 1;

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap 192.168.188.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 15:25 CET
Nmap scan report for fritz.box (192.168.188.1)
Host is up (0.00082s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5060/tcp open  sip
8181/tcp open  intermapper
MAC Address: 34:81:C4:B4:3B:B4 (AVM GmbH)
```

```
Nmap scan report for 192.168.188.36
Host is up (0.0059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

```
Nmap scan report for kali-vm.fritz.box (192.168.188.35)
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Zadanie 2;

a) Typy skanów TCP:

- –sT (skanowanie TCP connect):

```
Nmap scan report for 192.168.188.36
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for kali-vm.fritz.box (192.168.188.35)
Host is up (0.00022s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

- –sS (skanowanie TCP SYN):

```
┌──(stud㉿kali-vm)-[~]
└─$ nmap 192.168.188.0/24 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 15:40 CET
Nmap scan report for fritz.box (192.168.188.1)
Host is up (0.0016s latency).
```

```
Nmap scan report for 192.168.188.36
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
```

- –sN (skanowanie null, brak flag tcp w nagłówku pakietów):

```
Nmap scan report for 192.168.188.36
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
```

- –sM (skanowanie TCP Maimon FIN+ACK):

```
Nmap scan report for 192.168.188.36
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.188.36 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
```

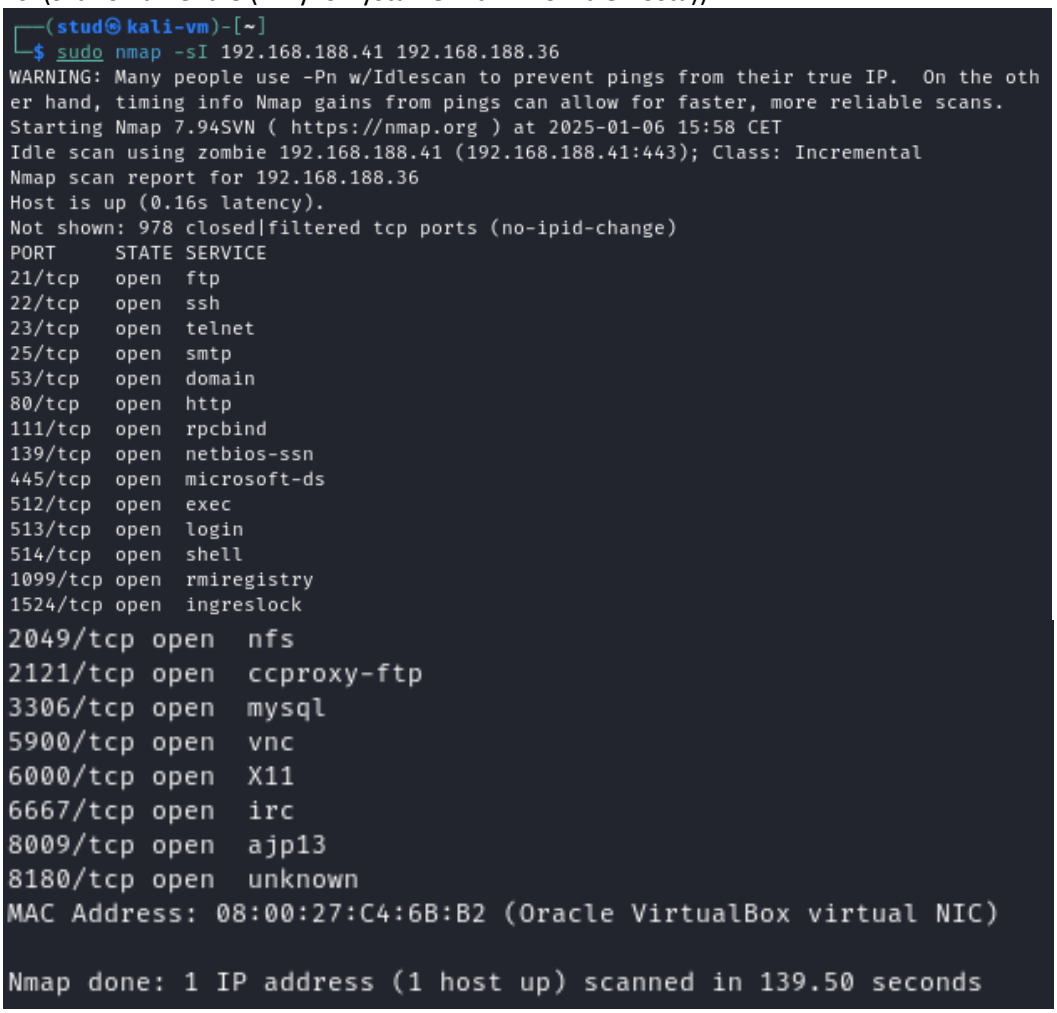
- –sA (skanowanie TCP ACK):

```
Nmap scan report for 192.168.188.36
Host is up (0.0096s latency).
All 1000 scanned ports on 192.168.188.36 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
```

- –sW (skanowanie TCP Window):

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap -sW 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 15:54 CET
Nmap scan report for 192.168.188.36
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.188.36 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

- –sl (skanowanie Idle (z wykorzystaniem tzw. Zombie hosta)):



b) Opis różnic:

-sT (TCP Connect Scan)

- wykonuje pełne połączenie TCP (trzyetapowy handshake)
- jest najbardziej widoczny dla systemu docelowego, ale działa bez potrzeby uprawnień root

-sS (SYN Scan)

- wysyła pakiet SYN i czeka na odpowiedź (SYN-ACK oznacza otwarty port)
- bardziej dyskretny niż -sT, bo nie kończy pełnego połączenia (brak handshake)

-sN (TCP Null Scan)

- wysyła pakiety bez ustawionych flag TCP
- może wykrywać otwarte/filtrujące porty na systemach bez ścisłego RFC

-sM (TCP Maimon Scan)

- specjalna metoda, która działa podobnie do -sN, ale z flagą FIN+ACK
- służy do omijania słabo skonfigurowanych zapór sieciowych

-sA (ACK Scan)

- sprawdza odpowiedź na pakiety ACK, aby określić, czy port jest filtrowany
- nie identyfikuje otwartych portów, ale pomaga mapować reguły firewalla

-sW (Window Scan)

- podobny do -sA, ale wykorzystuje różnice w oknach TCP do rozpoznania stanu portów
- działa tylko na niektórych systemach

-sI (Idle Scan)

- ukryte skanowanie przy użyciu hosta zombie, aby ukryć adres atakującego
- bardzo dyskretne, ale wymaga odpowiedniego hosta zombie

Zadanie 3;

```
└─$ sudo nmap -sU 192.168.188.36
[sudo] password for stud:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-06 20:28 CET
Warning: 192.168.188.36 giving up on port because retransmission cap hit (10)
.
Stats: 0:22:23 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 61.29% done; ETC: 21:04 (0:14:08 remaining)
Stats: 0:38:26 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 21:06 (0:00:00 remaining)
Stats: 0:42:19 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 21:10 (0:00:00 remaining)
Nmap scan report for 192.168.188.36
Host is up (0.0063s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open          nfs
20710/udp open|filtered unknown
MAC Address: 08:00:27:C4:6B:B2 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 2647.68 seconds
```

Zadanie 4;

- -T 5:

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap -T 5 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:11 CET
Nmap scan report for 192.168.188.36
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

- -T 4:

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap -T 4 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:13 CET
Nmap scan report for 192.168.188.36
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

```
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

- -T 3:

```
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

- -T 2, 1, 0: czas oczekiwania dłuższy niż 15min

Wniosek: Czas oczekiwania na wykonanie procedury rośnie wraz ze spadkiem podawanej wartości argumentu „-T”.

Zadanie 5;

Port 21: (sSH)

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap -sV 192.168.188.36 -p 21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:22 CET
Nmap scan report for 192.168.188.36
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Port 22: FTP

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap -sV 192.168.188.36 -p 22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:22 CET
Nmap scan report for 192.168.188.36
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

Zadanie 6;

```
┌──(stud㉿kali-vm)-[~]
└─$ sudo nmap 192.168.188.0/24 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:23 CET
```

Dla Metasploitable nie znaleziono jednoznacznej informacji o OS, jedynie mniej lub bardziej dokładne strzały. (Linux 2.6.9 - 2.6.24)

```
Nmap scan report for 192.168.188.36
Host is up (0.0047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6
.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.9 (97%), Linux 2.6.24 - 2.6.28
 (96%), Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.22 - 2.6.23 (96%), Linux 2.6.18 (Debian 4
, VMware) (96%), Linux 2.6.23 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Zadanie 7;

```
┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ ls
acarsd-info.nse                         ip-geolocation-ipinfodb.nse
address-info.nse                        ip-geolocation-map-bing.nse
afp-brute.nse                           ip-geolocation-map-google.nse
afp-ls.nse                              ip-geolocation-map-kml.nse
afp-path-vuln.nse                       ip-geolocation-maxmind.nse
afp-serverinfo.nse                      ip-https-discover.nse
afp-showmount.nse                       ipidseq.nse
ajp-auth.nse                            ipmi-brute.nse
ajp-brute.nse                           ipmi-cipher-zero.nse
ajp-headers.nse                         ipmi-version.nse
ajp-methods.nse                         ipv6-multicast-mld-list.nse
ajp-request.nse                         ipv6-node-info.nse
allseeingeye-info.nse                   ipv6-ra-flood.nse
amqp-info.nse                           irc-botnet-channels.nse
asn-query.nse                           irc-brute.nse
auth-owners.nse                         irc-info.nse
auth-spoof.nse                          irc-sasl-brute.nse
backorifice-brute.nse                   irc-unrealircd-backdoor.nse
backorifice-info.nse                    iscsi-brute.nse
bacnet-info.nse                         iscsi-info.nse
banner.nse                              isns-info.nse
bitcoin-getaddr.nse                     jdwp-exec.nse
bitcoin-info.nse                        jdwp-info.nse
bitcoinrpc-info.nse                     jdwp-inject.nse
```

Wybrane skrypty z folderu /usr/share/nmap/scripts/

- **http-traceroute.nse**: Wykonuje traceroute przez serwer HTTP, śledząc ścieżkę pakietów do hosta docelowego.
- **ssh-hostkey.nse**: Pobiera i wyświetla klucze hosta SSH z serwera, umożliwiając weryfikację tożsamości serwera.
- **dns-brute.nse**: Przeprowadza atak brute force na serwer DNS w celu odkrycia subdomen dla określonej domeny.
- **mysql-audit.nse**: Audytuje konfigurację bezpieczeństwa serwera MySQL zgodnie z wytycznymi CIS MySQL v1.0.2.

a) nmap -sC

```
└─$ sudo nmap -sC 192.168.188.36
[sudo] password for stud:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:39 CET
Nmap scan report for 192.168.188.36
Host is up (0.0061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.188.35
|      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
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STAR
TTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

```
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STAR
TTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateO
rProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-01-06T14:48:50+00:00; -51m53s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 23m34s, deviation: 2h30m11s, median: -51m29s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-06T09:48:20-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)

Nmap done: 1 IP address (1 host up) scanned in 75.10 seconds
```

http-enum

b)

```
┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script http-enum 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:44 CET
Nmap scan report for 192.168.188.36
Host is up (0.0097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
```

```
8180/tcp open  unknown
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
```

http-headers

```
┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script http-headers 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:46 CET
Nmap scan report for 192.168.188.36
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-headers:
|   Date: Mon, 06 Jan 2025 14:51:04 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
```

```
8180/tcp open  unknown
| http-headers:
|   Server: Apache-Coyote/1.1
|   Content-Type: text/html;charset=ISO-8859-1
|   Date: Mon, 06 Jan 2025 14:51:04 GMT
|   Connection: close
|
|_  (Request type: HEAD)
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

http-methods

```
┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script http-methods 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:47 CET
Nmap scan report for 192.168.188.36
Host is up (0.0084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp  open  rpcbind
```

```
80/tcp   open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:C4:6B:B2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

http-php-version

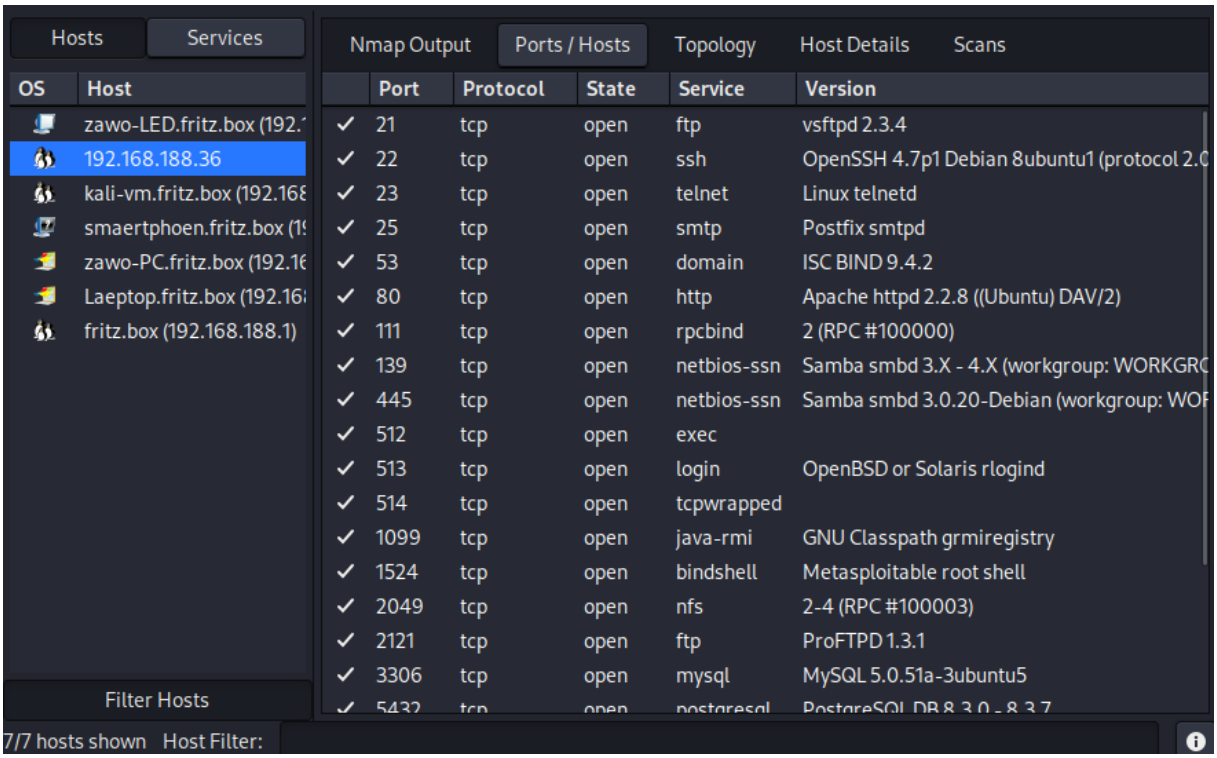
```
┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script http-phpversion 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:47 CET
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'http-phpversion' did not match a category, filename,
or directory
stack traceback:
        [C]: in function 'error'
        /usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
        /usr/share/nmap/nse_main.lua:1364: in main chunk
        [C]: in ?

QUITTING!

┌──(stud㉿kali-vm)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script http-php-version 192.168.188.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 16:48 CET
Nmap scan report for 192.168.188.36
Host is up (0.0075s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2
```

```
80/tcp   open  http
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2
.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
111/tcp  open  rpcbind
```

Zadanie 8;

- 192.168.188.36
  - **Host Status**
    - State: up
    - Open ports: 23
    - Filtered ports: 0
    - Closed ports: 977
    - Scanned ports: 1000
    - Up time: 6109
    - Last boot: Mon Jan 6 15:22:43 2025
  - **Addresses**
    - IPv4: 192.168.188.36
    - IPv6: Not available

- **Addresses**
  - IPv4: 192.168.188.36
  - IPv6: Not available
  - MAC: 08:00:27:C4:6B:B2
- **Operating System**
  - Name: Linux 2.6.9 - 2.6.33
  - Accuracy:
  - **Ports used**
    - Port-Protocol-State: 21 - tcp - open
    - Port-Protocol-State: 1 - tcp - closed
    - Port-Protocol-State: 34323 - udp - closed



Zadanie 9;

```
┌──(stud㉿kali-vm)-[~]
└─$ amap -bq 192.168.188.36 80 3306
amap v5.4 (www.thc.org/thc-amap) started at 2025-01-06 17:17:24 - APPLICATION
 MAPPING mode

Protocol on 192.168.188.36:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nD
ate Mon, 06 Jan 2025 150407 GMT\r\nServer Apache/2.2.8 (Ubuntu) DAV/2\r\nX-Po
wered-By PHP/5.2.4-2ubuntu5.10\r\nContent-Length 891\r\nConnection close\r\nC
ontent-Type text/html\r\n\r\n<html><head><title>Metasploitable2 - Linux</titl
e><
Protocol on 192.168.188.36:80/tcp matches http-apache-2 - banner: HTTP/1.1 20
0 OK\r\nDate Mon, 06 Jan 2025 150407 GMT\r\nServer Apache/2.2.8 (Ubuntu) DAV/
2\r\nX-Powered-By PHP/5.2.4-2ubuntu5.10\r\nContent-Length 891\r\nConnection c
lose\r\nContent-Type text/html\r\n\r\n<html><head><title>Metasploitable2 - Li
nux</title><
Protocol on 192.168.188.36:3306/tcp matches mysql - banner: >\n5.0.51a-3ubunt
u5$q;pD@Uk<,'L+2XG9*a/c(Bad handshake

amap v5.4 finished at 2025-01-06 17:17:30
```

Nmap skanuje sieć, wykrywa porty, usługi, wersje i systemy operacyjne. Amap skupia się bardziej na prostym rozpoznawaniu usług za pomocą „banner grabbing”, działa szybciej, ale dostarcza mniej szczegółowych danych. Nmap jest lepszy do ogólnych analiz sieci, a Amap sprawdza się przy identyfikacji usług na nietypowych portach lub w niestandardowych środowiskach.