

Оглавление

Тема и цель работы	3
Оборудование, ПО	3
Часть 1	4
Часть 2	37
Вывод.....	39
Контрольные вопросы	40

Тема и цель работы

Тема лабораторной работы: Honeypot, Nmap

Цель работы: получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.

Оборудование, ПО

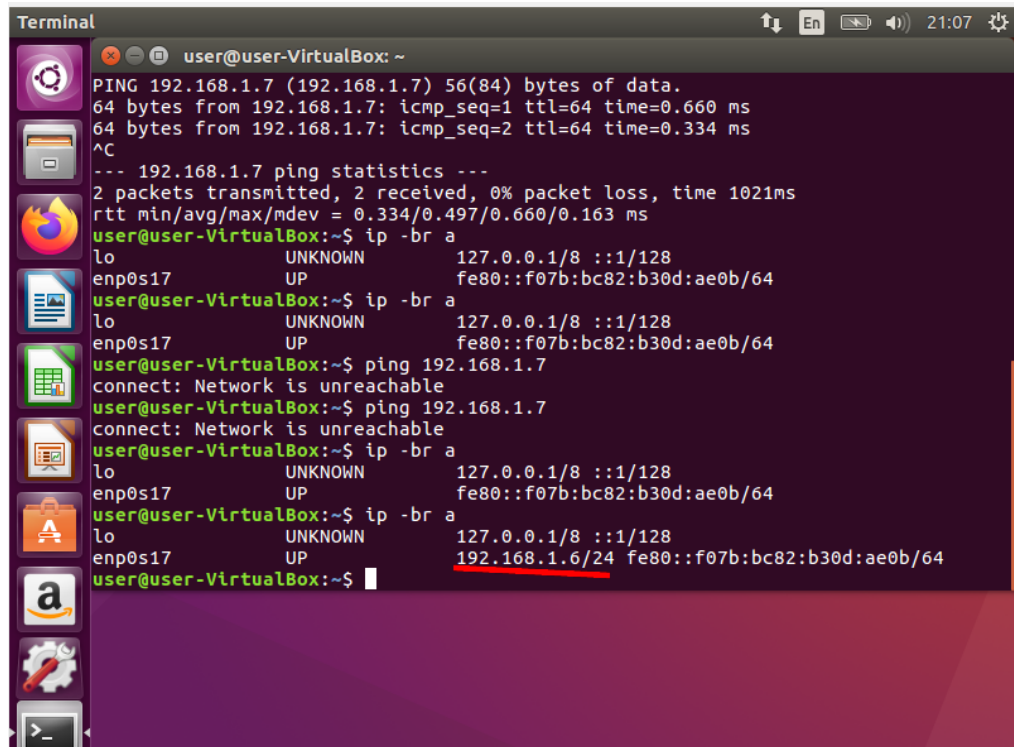
Таблица 1 - Оборудование, ПО

Устройство	Операционная система	IP адрес/Маска	Шлюз	DNS
Server	Ubuntu	DHCP (NAT network VBox)	NAT network	NAT network
Hacker	Ubuntu	DHCP (NAT network VBox)	NAT network	NAT network

Часть 1

Ход лабораторной работы

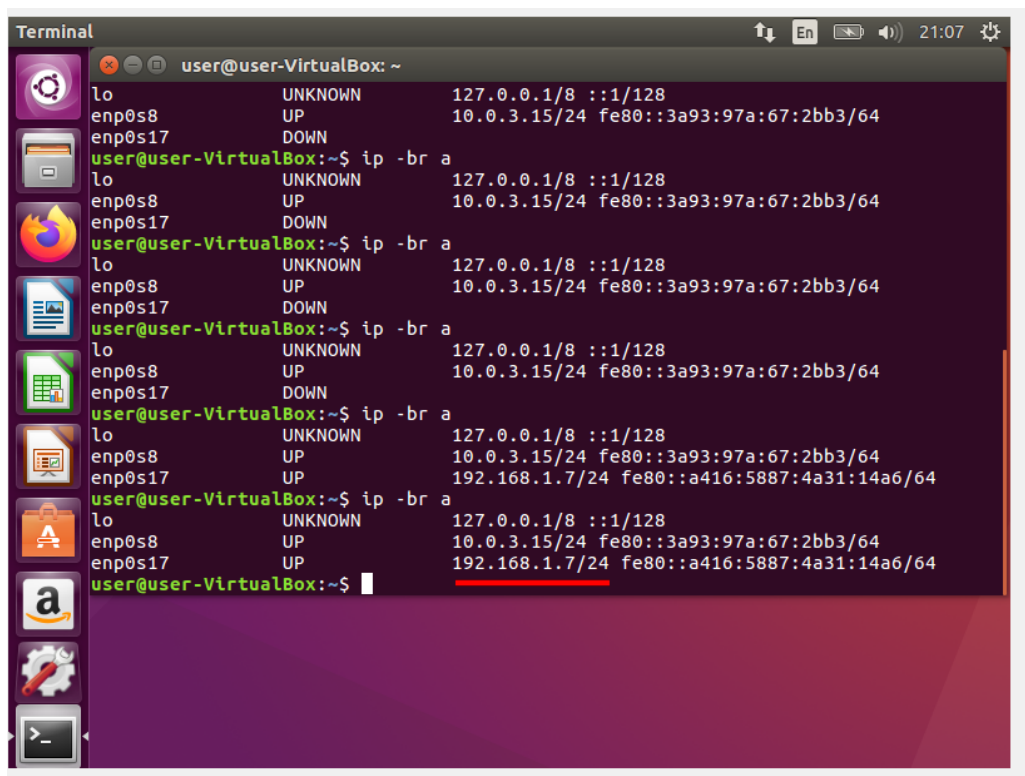
Определим ip-адрес машины “hacker” (см. рисунок 1)



```
Terminal
user@user-VirtualBox: ~
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data.
64 bytes from 192.168.1.7: icmp_seq=1 ttl=64 time=0.660 ms
64 bytes from 192.168.1.7: icmp_seq=2 ttl=64 time=0.334 ms
^C
--- 192.168.1.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1021ms
rtt min/avg/max/mdev = 0.334/0.497/0.660/0.163 ms
user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s17           UP         fe80::f07b:bc82:b30d:ae0b/64
user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s17           UP         fe80::f07b:bc82:b30d:ae0b/64
user@user-VirtualBox:~$ ping 192.168.1.7
connect: Network is unreachable
user@user-VirtualBox:~$ ping 192.168.1.7
connect: Network is unreachable
user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s17           UP         fe80::f07b:bc82:b30d:ae0b/64
user@user-VirtualBox:~$ ip -br a
lo                UNKNOWN    127.0.0.1/8 ::1/128
enp0s17           UP         192.168.1.6/24 fe80::f07b:bc82:b30d:ae0b/64
user@user-VirtualBox:~$
```

Рисунок 1 - hacker

Определим ip-адрес сервера (см. рисунок 2).

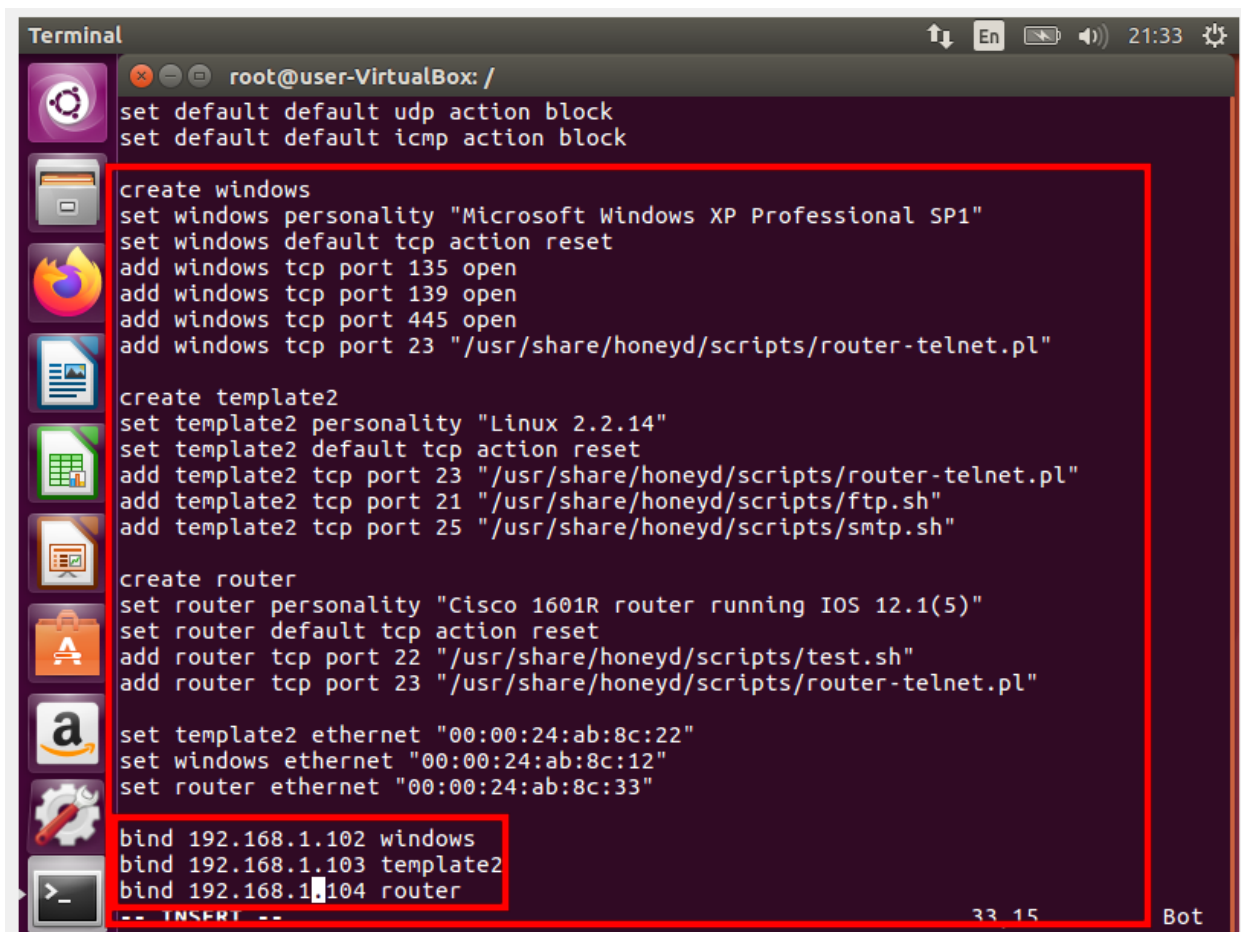


The image shows a terminal window titled "Terminal" with a dark background. The prompt is "user@user-VirtualBox: ~". The user has entered the command "ip -br a" multiple times. The output shows the status of network interfaces: "lo" is UNKNOWN with IP 127.0.0.1/8; "enp0s8" is UP with IP 10.0.3.15/24; "enp0s17" is DOWN with IP 10.0.3.15/24. In the fourth execution, "enp0s17" is UP with IP 192.168.1.7/24. The terminal window has a sidebar with application icons and a top bar with system status icons and the time 21:07.

```
user@user-VirtualBox: ~  
lo UNKNOWN 127.0.0.1/8 ::1/128  
enp0s8 UP 10.0.3.15/24 fe80::3a93:97a:67:2bb3/64  
enp0s17 DOWN  
user@user-VirtualBox:~$ ip -br a  
lo UNKNOWN 127.0.0.1/8 ::1/128  
enp0s8 UP 10.0.3.15/24 fe80::3a93:97a:67:2bb3/64  
enp0s17 DOWN  
user@user-VirtualBox:~$ ip -br a  
lo UNKNOWN 127.0.0.1/8 ::1/128  
enp0s8 UP 10.0.3.15/24 fe80::3a93:97a:67:2bb3/64  
enp0s17 DOWN  
user@user-VirtualBox:~$ ip -br a  
lo UNKNOWN 127.0.0.1/8 ::1/128  
enp0s8 UP 10.0.3.15/24 fe80::3a93:97a:67:2bb3/64  
enp0s17 UP 192.168.1.7/24 fe80::a416:5887:4a31:14a6/64  
user@user-VirtualBox:~$ ip -br a  
lo UNKNOWN 127.0.0.1/8 ::1/128  
enp0s8 UP 10.0.3.15/24 fe80::3a93:97a:67:2bb3/64  
enp0s17 UP 192.168.1.7/24 fe80::a416:5887:4a31:14a6/64  
user@user-VirtualBox:~$
```

Рисунок 2 - сервер

Настроим конфиг honeyd.conf (см. рисунок 3).



```
Terminal
root@user-VirtualBox: /
set default default udp action block
set default default icmp action block

create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open
add windows tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

create template2
set template2 personality "Linux 2.2.14"
set template2 default tcp action reset
add template2 tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
add template2 tcp port 21 "/usr/share/honeyd/scripts/ftp.sh"
add template2 tcp port 25 "/usr/share/honeyd/scripts/smtp.sh"

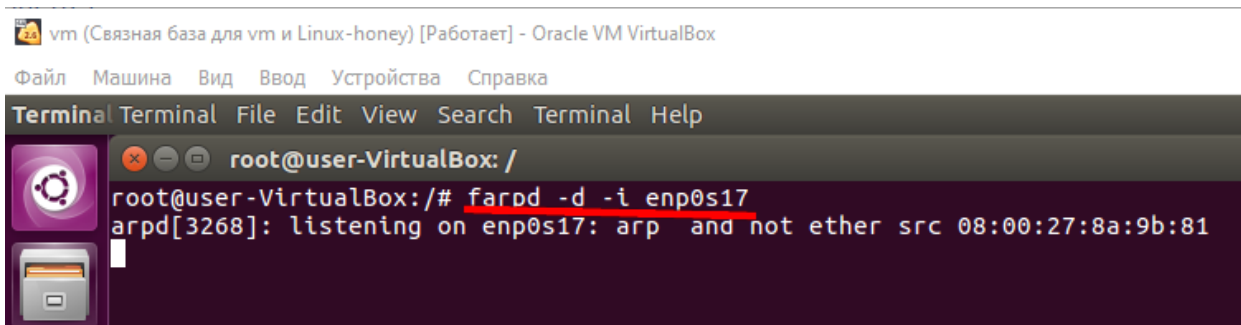
create router
set router personality "Cisco 1601R router running IOS 12.1(5)"
set router default tcp action reset
add router tcp port 22 "/usr/share/honeyd/scripts/test.sh"
add router tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

set template2 ethernet "00:00:24:ab:8c:22"
set windows ethernet "00:00:24:ab:8c:12"
set router ethernet "00:00:24:ab:8c:33"

bind 192.168.1.102 windows
bind 192.168.1.103 template2
bind 192.168.1.104 router
-- INSERT --
33 15 Bot
```

Рисунок 3 – honeyd.conf

Запустим honeypot командой **farpd -d -i enp0s17** (см. рисунок 4).



```
vm (Связная база для vm и Linux-honey) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Terminal Terminal File Edit View Search Terminal Help
root@user-VirtualBox: /
root@user-VirtualBox:/# farpd -d -i enp0s17
arpd[3268]: listening on enp0s17: arp and not ether src 08:00:27:8a:9b:81
```

Рисунок 4 – запуск honeypot

Запустим honeypot командой **honeypot honeyd -d -f etc/honeypot/honeyd.conf -i enp0s17** (см. рисунок 5).

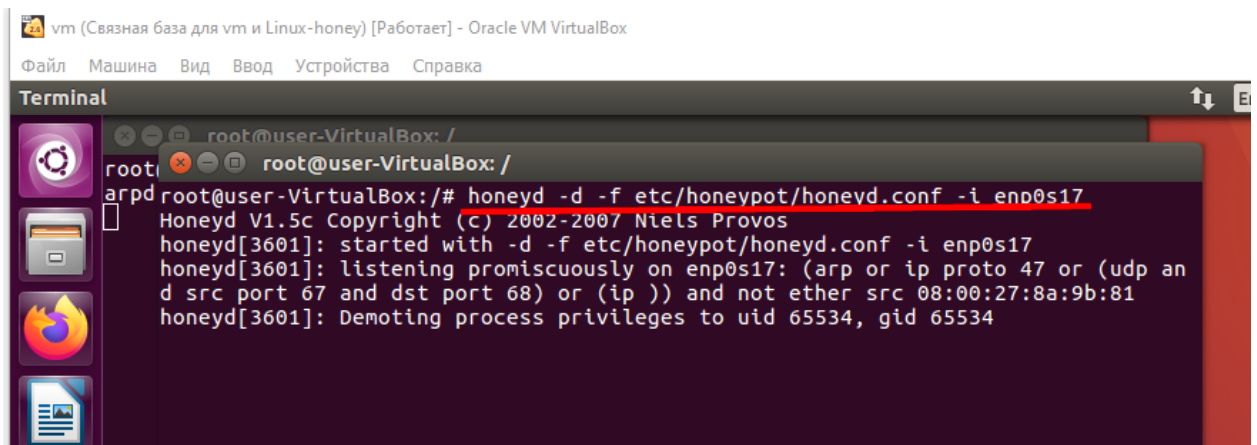


Рисунок 5 – запуск honeyd

При сканировании методом TCP-Connect nmap обнаружил на каждой «ловушке» ожидаемые открытые порты. На Windows-эмуляторе (192.168.1.102) были открыты порты 23 (telnet), 135 (msrpc), 139 (netbios-ssn) и 445 (microsoft-ds). На шаблоне template2 (192.168.1.103) открылись порты 21 (ftp), 23 (telnet) и 25 (smtp). На роутере (192.168.1.104) оказались открыты порты 22 (ssh) и 23 (telnet) (см. рисунок 6).

```
nmap -sT 192.168.1.102
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:00:24:F5:43:16 (Connect AS)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
nmap -sT 192.168.1.103
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.103
Host is up (0.033s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.05 seconds
nmap -sT 192.168.1.104
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.104
Host is up (0.050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 00:00:24:77:71:D3 (Connect AS)
```

Рисунок 6 – TCP connect

При TCP-SYN сканировании результаты не отличались от TCP-Connect: те же порты оказались открытыми на тех же хостах, что подтверждает заданную в конфигурации `honeypd` фильтрацию и эмуляцию (см. рисунок 7).

```

nmap -sS 192.168.1.102
|
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.10s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
nmap -sS 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.103
Host is up (0.13s latency).
Not shown: 886 closed ports, 111 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
nmap -sS 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.104
Host is up (0.046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 00:00:24:77:71:D3 (Connect AS)

```

Рисунок 7 – TCP SYN

При FIN-сканировании все перечисленные порты находились в состоянии open|filtered. Это означает, что либо они действительно открыты и не отправляют RST-ответ на пакеты с флагом FIN, либо фильтрация пакетов мешает однозначно определить их состояние. Особенно важно отметить порт 23, по которому работает небезопасный telnet (см. рисунок 8).


```

nmap -sF 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.030s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
23/tcp    open|filtered telnet
135/tcp   open|filtered msrpc
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
nmap -sF 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.103
Host is up (0.070s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 9.31 seconds
nmap -sF 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.104
Host is up (0.059s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
MAC Address: 00:00:24:77:71:D3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 11.18 seconds

```

Рисунок 8 – FIN сканирование

Xmas-сканирование показало, что все 1000 проверенных портов на каждом эмуляторе закрыты. Пакеты с флагами FIN+PSH+URG были либо проигнорированы, либо получили ответ RST, что типично для современных систем и фаерволов. (см. рисунок 9).

```

nmap -sX 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.053s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
nmap -sX 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.103
Host is up (0.033s latency).
All 1000 scanned ports on 192.168.1.103 are closed
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
nmap -sX 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.104
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.1.104 are closed
MAC Address: 00:00:24:77:71:D3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
nmap -sX 192.168.1.102

```

Рисунок 9 – XMAS сканирование

При Null-сканировании первая ловушка (Windows) проигнорировала пакеты без флагов и отразила все порты как закрытые. Вторая ловушка (template2) показала состояние open|filtered для портов 21, 23 и 25, а третья (router) вновь продемонстрировала все порты закрытыми (см. рисунок 10).

```

nmap -sN 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.024s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds
nmap -sN 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.103
Host is up (0.049s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
nmap -sN 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.104
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.104 are closed
MAC Address: 00:00:24:77:71:D3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds

```

Рисунок 10 – NULL сканирование

Сканирование IP-протоколов выявило поддержку на всех трёх хостах протоколов ICMP (1), TCP (6) и UDP (17). Все они имели состояние open|filtered, что означает принятие соответствующих пакетов (см. рисунок 11).

```

nmap -sO 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:51 MSK
Nmap scan report for 192.168.1.102
Host is up (0.066s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1          open  icmp
6          open  tcp
17         open  udp
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds
nmap -sO 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.103
Host is up (0.072s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1          open  icmp
6          open  tcp
17         open  udp
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds
nmap -sO 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.104
Host is up (0.077s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1          open  icmp
6          open  tcp
17         open  udp
MAC Address: 00:00:24:77:71:D3 (Connect AS)

```

Рисунок 11 – сканирование ip протоколов

В ходе ACK-сканирования все три хоста ответили RST-пакетами на отправленные пакеты ACK, поэтому все порты классифицированы как unfiltered, то есть без фильтрации на транспортном уровне. (см. рисунок 12).

```
nmap -sA 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.102
Host is up (0.062s latency).
All 1000 scanned ports on 192.168.1.102 are unfiltered
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
nmap -sA 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.103
Host is up (0.028s latency).
All 1000 scanned ports on 192.168.1.103 are unfiltered
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
nmap -sA 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.104
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.104 are unfiltered
MAC Address: 00:00:24:77:71:D3 (Connect AS)
```

Рисунок 12 – ACK сканирование

При TCP Window сканировании nmap получил RST-ответы на запросы с изменённым размером окна на всех трёх хостах, и порты были определены как закрытые (см. рисунок 13).

```

nmap -sW 192.168.1.102

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.102
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.1.102 are closed
MAC Address: 00:00:24:F5:43:16 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 3.31 seconds
nmap -sW 192.168.1.103

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.103
Host is up (0.15s latency).
All 1000 scanned ports on 192.168.1.103 are closed
MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
nmap -sW 192.168.1.104

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
Nmap scan report for 192.168.1.104
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.1.104 are closed
MAC Address: 00:00:24:77:71:D3 (Connect AS)

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds

```

Рисунок 13 – TCP window

RPC-сканирование (опция `-sR`, эквивалент `-sV` плюс `RPC-scan`) позволило получить баннеры и приблизительные версии сервисов. На Windows-ловушке telnet отдал предупреждение о перехвате и согласии пользователя, а порты `msrpc`, `netbios-ssn` и `microsoft-ds` были помечены с вопросительным признаком. На шаблоне `template2` FTP и SMTP оказались обёрнутыми (`tcpwrapped`), а telnet вернул свой баннер. На роутере nmap распознал SSH версии 1.5 и telnet-баннер Cisco.

```
nmap -sR 192.168.1.102
```

WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.

```
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-15 09:52 MSK
```

Nmap scan report for 192.168.1.102

Host is up (0.039s latency).

Not shown: 996 closed ports

<i>PORT</i>	<i>STATE</i>	<i>SERVICE</i>	<i>VERSION</i>
-------------	--------------	----------------	----------------

<i>23/tcp</i>	<i>open</i>	<i>telnet</i>	
---------------	-------------	---------------	--

<i>135/tcp</i>	<i>open</i>	<i>msrpc?</i>	
----------------	-------------	---------------	--

<i>139/tcp</i>	<i>open</i>	<i>netbios-ssn?</i>	
----------------	-------------	---------------------	--

<i>445/tcp</i>	<i>open</i>	<i>microsoft-ds?</i>	
----------------	-------------	----------------------	--

I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port23-TCP:V=7.01%I=7%D=4/15%Time=67FE0247%P=x86_64-pc-linux-gnu%r(NULL

SF:.,385,"\\xff\\xfe\\x01\\xff\\xfb\\x01\\xff\\xfb\\x03Users\\x20\\(authorized\\x20or\\x

SF:20unauthorized\\)\\x20have\\x20no\\x20explicit\\x20or\\r\\nimplicit\\x20expect

a

SF:tion\\x20of\\x20privacy\\.\\x20\\x20Any\\x20or\\x20all\\x20uses\\x20of\\x20this

r

SF:\\nsystem\\x20may\\x20be\\x20intercepted,\\x20monitored,\\x20recorded,\\x20

cop

SF:ied,\\r\\naudited,\\x20inspected,\\x20and\\x20disclosed\\x20to\\x20authorized

SF:x20site,\\r\\nand\\x20law\\x20enforcement\\x20personnel,\\x20as\\x20well\\x2

0as

SF:\\x20to\\x20authorized\\r\\nofficials\\x20of\\x20other\\x20agencies,\\x20both\\x

SF: domestic and foreign. By using this system, the
he
SF: user consents to such interception, monitoring, r
r
SF: recording, copying, auditing, inspection, and disclosure
SF: at the discretion of authorized site. Unautho
SF: rized or improper use of this system may re
sult
SF: in administrative disciplinary action and civil a
SF: nd criminal penalties. By continuing to use x2
0t
SF: his system you indicate your awareness of and x
20c
SF: onsent to these terms and conditions of use
.|
SF: LOG OFF IMMEDIATELY if you do not x
20agree x20
SF: to the conditions stated in this warning. r n r n r
SF: n r n User Access Verification r n r n Username: ")%(GenericLin
es,3
SF: A3, "\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20(authorized\x20or\x20
SF: unauthorized)\x20have\x20no\x20explicit\x20or\x20implicit\x20expectati
SF: on\x20of\x20privacy. \x20Any\x20or\x20all\x20uses\x20of\x20this r
n

*SF:system\may\be\intercepted,\monitored,\recorded,\c
opie*

SF:d,\r\naudited,\inspected,\and\disclosed\to\authorized
2

SF:0site,\r\and\law\enforcement\personnel,\as\well
s\

SF:2to\authorized\r\nofficials\of\other\agencies,\both
0

SF:domestic\and\foreign\.\r\nBy\using\this\system,\the
x

SF:2user\consents\to\such\r\ninterception,\monitoring,
ec

SF:ording,\copying,\auditing,\r\ninspection,\and\disclosure
2

SF:0at\the\discretion\of\authorized\r\nsite\.\r\n\r\nUnauthori

SF:zed\or\improper\use\of\this\system\may\resu
lt\

SF:2in\r\nadministrative\disciplinary\action\and\civil
d

SF:\criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x20th
i

SF:s\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x2
0con

SF:sent\to\these\terms\and\conditions\r\n\x20of\x20use\.
2

SF:0\x20LOG\x20OFF\x20IMMEDIATELY\x20if\x20you\x20do\x20not\x20agree\x20to

SF:\x20the\r\nconditions\x20stated\x20in\x20this\x20warning\.\r\n\r\n\r\n\r\n\r\n

SF:r\nUser\x20Access\x20Verification\r\n\r\n\r\nUsername:");

MAC Address: 00:00:24:F5:43:16 (Connect AS)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 144.32 seconds

nmap -sR 192.168.1.103

WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.

Starting Nmap 7.01 (<https://nmap.org>) at 2025-04-15 09:55 MSK

Nmap scan report for 192.168.1.103

Host is up (0.014s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

21/tcp open tcpwrapped

23/tcp open telnet

25/tcp open tcpwrapped

I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port23-TCP:V=7.01%I=7%D=4/15%Time=67FE02D7%P=x86_64-pc-linux-gnu%(NULL

SF:;,385,"\\xff\\xfe\\x01\\xff\\xfb\\x01\\xff\\xfb\\x03Users\\x20\\(authorized\\x20or\\x

SF:20unauthorized\\x20have\\x20no\\x20explicit\\x20or\\r\\nimplicit\\x20expect

a

SF:tion\\x20of\\x20privacy\\x20\\x20Any\\x20or\\x20all\\x20uses\\x20of\\x20this

r

SF:\\nssystem\\x20may\\x20be\\x20intercepted,\\x20monitored,\\x20recorded,\\x20

cop

SF:ied,\\r\\naudited,\\x20inspected,\\x20and\\x20disclosed\\x20to\\x20authorized

SF:x20site,\\r\\nand\\x20law\\x20enforcement\\x20personnel,\\x20as\\x20well\\x2

0as

SF:\\x20to\\x20authorized\\r\\nofficials\\x20of\\x20other\\x20agencies,\\x20both\\x

SF:20domestic\\x20and\\x20foreign\\x20\\r\\nBy\\x20using\\x20this\\x20system,\\x20t

he

SF:\\x20user\\x20consents\\x20to\\x20such\\r\\ninterception,\\x20monitoring,\\x20

r

SF:ecording,\\x20copying,\\x20auditing,\\r\\ninspection,\\x20and\\x20disclosure

SF:x20at\\x20the\\x20discretion\\x20of\\x20authorized\\r\\nsite\\x20\\r\\n\\r\\nUnautho

SF:rized\\x20or\\x20improper\\x20use\\x20of\\x20this\\x20system\\x20may\\x20re

sult

SF:\\x20in\\r\\nadministrative\\x20disciplinary\\x20action\\x20and\\x20civil\\x20a

SF:nd\x20criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x20
0t
SF:his\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x20
20c
SF:onsent\x20to\x20these\x20terms\x20and\x20conditions\r\n\x20of\x20use
.
SF:\x20\x20LOG\x20OFF\x20IMMEDIATELY\x20if\x20you\x20do\x20not\x20
20agree\x20
SF:to\x20the\r\nconditions\x20stated\x20in\x20this\x20warning\.\r\n\r\n\r\n
SF:n\r\nUser\x20Access\x20Verification\r\n\r\nUsername:")%(GenericLin
es,3
SF:A3,"'\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\ (authorized\x20or\x20
SF:unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expectati
SF:on\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\r\n
n
SF:system\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20c
opie
SF:d,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized\x20
2
SF:0site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x20a
s\x20
SF:20to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\x20
0
SF:domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20the
x

nmap -sR 192.168.1.104

WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.

Starting Nmap 7.01 (<https://nmap.org>) at 2025-04-15 09:55 MSK

Nmap scan report for 192.168.1.104

Host is up (0.038s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh (protocol 1.5)

23/tcp open telnet

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port22-TCP:V=7.01%I=7%D=4/15%Time=67FE02FE%P=x86_64-pc-linux-gnu%r(NULL

SF:;D,"SSH-1\5-2\40\n");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port23-TCP:V=7.01%I=7%D=4/15%Time=67FE02FE%P=x86_64-pc-linux-gnu%r(NULL

SF:;385,"\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\(\authorized\x20or\x

SF:20unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expect
a
SF:tion\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this
r
SF:\nsystem\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20
cop
SF:ied,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized
SF:x20site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x2
0as
SF:\x20to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\x
SF:20domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20t
he
SF:\x20user\x20consents\x20to\x20such\r\ninterception,\x20monitoring,\x20
r
SF:ecording,\x20copying,\x20auditing,\r\ninspection,\x20and\x20disclosure
SF:x20at\x20the\x20discretion\x20of\x20authorized\r\nsite\.\r\n\r\nUnautho
SF:rized\x20or\x20improper\x20use\x20of\x20this\x20system\x20may\x20re
sult
SF:\x20in\r\nadministrative\x20disciplinary\x20action\x20and\x20civil\x20a
SF:nd\x20criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x2
0t
SF:his\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x
20c
SF:onsent\x20to\x20these\x20terms\x20and\x20conditions\r\n\x20of\x20use
.

SF:x20\x20LOG\x20OFF\x20IMMEDIATELY\x20if\x20you\x20do\x20not\x20
20agree\x20

SF:to\x20the\r\nconditions\x20stated\x20in\x20this\x20warning\.\r\n\r\n\r\n\r\n

SF:n\r\nUser\x20Access\x20Verification\r\n\r\n\r\nUsername:")%r(GenericLin
es,3

SF:A3,"'\xff\xfe\x01\xff\xfb\x01\xff\xfb\x03Users\x20\ (authorized\x20or\x20

SF:unauthorized\)\x20have\x20no\x20explicit\x20or\r\nimplicit\x20expectati

SF:on\x20of\x20privacy\.\x20\x20Any\x20or\x20all\x20uses\x20of\x20this\r\n
n

SF:system\x20may\x20be\x20intercepted,\x20monitored,\x20recorded,\x20c
opie

SF:d,\r\naudited,\x20inspected,\x20and\x20disclosed\x20to\x20authorized\x20
2

SF:0site,\r\nand\x20law\x20enforcement\x20personnel,\x20as\x20well\x20a
s\x20x

SF:2to\x20authorized\r\nofficials\x20of\x20other\x20agencies,\x20both\x20
0

SF:domestic\x20and\x20foreign\.\r\nBy\x20using\x20this\x20system,\x20the\
x

SF:2user\x20consents\x20to\x20such\r\ninterception,\x20monitoring,\x20or
ec

SF:ording,\x20copying,\x20auditing,\r\ninspection,\x20and\x20disclosure\x20
2

SF:0at\x20the\x20discretion\x20of\x20authorized\r\nsite\.\r\n\r\nUnauthori

*SF:zed\x20or\x20improper\x20use\x20of\x20this\x20system\x20may\x20resu
lt\x20*

*SF:20in\r\nadministrative\x20disciplinary\x20action\x20and\x20civil\x20an
d*

*SF:\x20criminal\r\npenalties\.\x20\x20By\x20continuing\x20to\x20use\x20th
i*

*SF:s\x20system\x20you\x20indicate\r\nyour\x20awareness\x20of\x20and\x2
0con*

*SF:sent\x20to\x20these\x20terms\x20and\x20conditions\r\n\x20of\x20use\.\x2
2*

*SF:0\x20LOG\x20OFF\x20IMMEDIATELY\x20if\x20you\x20do\x20not\x20
agree\x20to*

SF:\x20the\r\nconditions\x20stated\x20in\x20this\x20warning\.\r\n\r\n\r\n\r\n

SF:r\nUser\x20Access\x20Verification\r\n\r\n\r\nUsername:");

MAC Address: 00:00:24:77:71:D3 (Connect AS)

*Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.*

Nmap done: 1 IP address (1 host up) scanned in 40.72 seconds

При попытке определения ОС (опция -O) Windows-ловушка дала множество догадок без точного совпадения (Sony PSP, Windows 2000 SP4, FreeBSD и другие), а на двух других хостах точное определение ОС не удалось, что характерно для эмуляторов или нестандартных систем.

nmap -O 192.168.1.102

Starting Nmap 7.01 (<https://nmap.org>) at 2025-04-15 09:56 MSK

Nmap scan report for 192.168.1.102

Host is up (0.021s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

23/tcp open telnet

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

MAC Address: 00:00:24:F5:43:16 (Connect AS)

Device type: game console/general purpose/phone

Running (JUST GUESSING): Sony embedded (87%), Microsoft Windows 2000/Me (87%), FreeBSD 4.X (85%), QNX 6.X (85%), Sony Ericsson Symbian OS 9.X (85%)

<i>OS</i>	<i>CPE:</i>
<i>cpe:/h:sony:playstation_portable</i>	
<i>cpe:/o:microsoft:windows_2000::sp4</i>	<i>cpe:/o:microsoft:windows_me</i>
<i>cpe:/o:freebsd:freebsd:4.11</i>	<i>cpe:/o:qnx:qnx:6.2.1</i>
	<i>cpe:/h:sonyericsson:pli</i>
<i>cpe:/o:sonyericsson:symbian_os:9.1</i>	

Aggressive OS guesses: Sony PSP game console (modified, running Custom Firmware 3.90 - 5.50) (87%), Microsoft Windows 2000 SP4 (87%), Microsoft Windows 2000 Professional SP4 (85%), Microsoft Windows 2000 Server SP4 (85%), Microsoft Windows Millenium Edition (Me) 4.90.3000 (85%), FreeBSD 4.11-STABLE (85%), QNX 6.2.1 (x86) (85%), Sony Ericsson P1i mobile phone (Symbian OS 9.1) (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 18.92 seconds

nmap -O 192.168.1.103

Starting Nmap 7.01 (<https://nmap.org>) at 2025-04-15 09:56 MSK

Nmap scan report for 192.168.1.103

Host is up (0.021s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp open telnet

25/tcp open smtp

MAC Address: 00:00:24:5F:0B:A3 (Connect AS)

No OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

*OS:SCAN(V=7.01%E=4%D=4/15%OT=21%CT=1%CU=31679%PV=Y%
DS=1%DC=D%G=Y%M=000024%T*

*OS:M=67FE0343%P=x86_64-pc-linux-
gnu)SEQ(SP=D2%GCD=1%ISR=D9%TI=I%CI=I)SEQ(SP*

OS:=D2%GCD=1%ISR=DA%TI=I%CI=I%II=I%SS=S)OPS(OI=M5B4N
NT11NW0%O2=M5B4NNT11NW0

OS:%O3=M5B4NNT11NW0%O4=M5B4NNT11NW0%O5=M5B4NNT11N
W0%O6=M5B4NNT11NW0)WIN(W1=

OS:7C38%W2=7C38%W3=7C38%W4=7C38%W5=7C38%W6=7C38)EC
N(R=Y%DF=Y%T=40%W=7C38%O=

OS:M5B4NNT10NW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
%F=AS%RD=0%Q=)T2(R=N)T3(R=

OS:Y%DF=Y%T=40%W=7C38%S=O%A=S+%F=AS%O=M5B4NNT11N
W0%RD=0%Q=)T4(R=Y%DF=N%T=40

OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40
%W=0%S=A%A=S+%F=AR%O=%RD=0%Q

OS:=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
=)T7(R=Y%DF=N%T=40%W=0%S=A%A

OS:=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=164%U
N=0%RIPL=G%RID=G%RIPCK=G%RU

OS:CK=G%RUD=I)IE(R=Y%DFI=N%T=FF%CD=1)

Network Distance: 1 hop

*OS detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.*

Nmap done: 1 IP address (1 host up) scanned in 18.64 seconds

nmap -O 192.168.1.104

Starting Nmap 7.01 (<https://nmap.org>) at 2025-04-15 09:57 MSK

Nmap scan report for 192.168.1.104

Host is up (0.018s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

23/tcp open telnet

MAC Address: 00:00:24:77:71:D3 (Connect AS)

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=7.01%E=4%D=4/15%OT=22%CT=1%CU=33061%PV=Y%
DS=1%DC=D%G=Y%M=000024%T*

*OS:M=67FE0357%P=x86_64-pc-linux-
gnu)SEQ(SP=41%GCD=1%ISR=47%TI=Z%CI=Z%II=Z%T*

*OS:S=U)SEQ(SP=41%GCD=1%ISR=48%TI=Z%CI=Z%TS=U)OPS(O1=
M5B4%O2=M5B4%O3=M5B4%O4*

*OS:=M5B4%O5=M5B4%O6=M5B4)WIN(W1=1020%W2=1020%W3=102
0%W4=1020%W5=1020%W6=102*

*OS:0)ECN(R=Y%DF=N%T=40%W=1020%O=M5B4%CC=N%Q=)T1(R=
Y%DF=N%T=40%S=O%A=S+%F=AS*

*OS:%RD=0%Q=)T2(R=Y%DF=N%T=40%W=0%S=A%A=S%F=AR%O
=%RD=0%Q=)T3(R=Y%DF=N%T=40%W*

*OS:=1020%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=N
%T=40%W=0%S=A%A=Z%F=R%O=%R*

*OS:D=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=A%A=S+%F=AR%O=
%RD=0%Q=)T6(R=Y%DF=N%T=40%W=*

*OS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0
%S=A%A=S%F=AR%O=%RD=0%Q=)U1*

*OS:(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=
G%RUCK=G%RUD=G)IE(R=Y%DFI=*

OS:N%T=40%CD=Z)

Network Distance: 1 hop

*OS detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.*

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds

Изменим honeyd.conf (добавим два новых устройства и изменим предыдущие):

HONEYD.conf:

/etc/honeypot/honeyd.conf

*# Глобальные настройки: блокировка всего трафика по умолчанию
create default*

set default default tcp action block

set default default udp action block

set default default icmp action block

```
#####
#####
# Ловушка 1: Windows
#####
#####

create windows

set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open
add windows tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
set windows ethernet "00:00:24:ab:8c:12"

#####
#####

# Ловушка 2: Linux-сервер (базируется на Linux 2.2.14)
#####
#####

create template2

set template2 personality "Linux 2.2.14"
set template2 default tcp action reset
add template2 tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
add template2 tcp port 21 "/usr/share/honeyd/scripts/ftp.sh"
add template2 tcp port 25 "/usr/share/honeyd/scripts/smtp.sh"
set template2 ethernet "00:00:24:ab:8c:22"

#####
#####
```

```

# Ловушка 3: Роутер (Cisco)
#####
#####

create router

set router personality "Cisco 1601R router running IOS 12.1(5)"
set router default tcp action reset
add router tcp port 22 "/usr/share/honeyd/scripts/test.sh"
add router tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
add router udp port 161 "/usr/share/honeyd/scripts/snmp.sh"
set router ethernet "00:00:24:ab:8c:33"

#####
#####

# Ловушка 4: IoT-устройство (например, IP-камера)
#####
#####

create iot_camera

# Используем личность "Linux 2.4.20" – если такой нет, то можно
использовать другую версию Linux,
# которая присутствует в базе Honeyd
set iot_camera personality "Linux 2.4.20"
set iot_camera default tcp action reset
add iot_camera tcp port 80 "/usr/share/honeyd/scripts/httpd.sh"
add iot_camera tcp port 554 "/usr/share/honeyd/scripts/rtsp.sh"
set iot_camera ethernet "00:00:24:ab:8c:44"

#####
#####

# Ловушка 5: Сетевой принтер

```



```
#####
#####

create printer

# В качестве личности для принтера выбран "Linux 2.2.14", так как
обычно для эмуляции

# принтера выбирают Linux-подобный профиль (либо можно оставить
дефолтный, если специальной

# подписи для принтера нет в базе)
set printer personality "Linux 2.2.14"
set printer default tcp action reset
add printer tcp port 515 "/usr/share/honeyd/scripts/lpd.sh"
add printer tcp port 9100 "/usr/share/honeyd/scripts/print.sh"
add printer tcp port 80 "/usr/share/honeyd/scripts/httpd.sh"
set printer ethernet "00:00:24:ab:8c:55"

#####
#####

# Привязка виртуальных хостов к IP-адресам
#####
#####

bind 192.168.1.102 windows
bind 192.168.1.103 template2
bind 192.168.1.104 router
bind 192.168.1.105 iot_camera
bind 192.168.1.106 printer
```

Проведем снова сканирование различными видами (так как лог сканирования слишком большой, будут даны только комментарии о нём):

При сканировании методом TCP-Connect nmap на каждой «ловушке» обнаружил открытые порты, соответствующие их конфигурации. На Windows-эмуляторе (192.168.1.102) открыты порты 23 (telnet), 135 (msrpc), 139 (netbios-ssn) и 445 (microsoft-ds). На шаблоне template2 (192.168.1.103) открыты порты 21 (ftp), 23 (telnet) и 25 (smtp). На роутере (192.168.1.104) открыты порты 22 (ssh) и 23 (telnet). На IoT-камере (192.168.1.105) открыты порты 80 (http) и 554 (rtsp). На принтере (192.168.1.106) открыты порты 80 (http), 515 (printer) и 9100 (jetdirect).

При TCP-SYN сканировании результаты повторяют TCP-Connect: те же порты открыты на тех же хостах, что подтверждает корректную эмуляцию сервисов.

При FIN-сканировании все вышеуказанные порты на всех пяти эмуляторах оказались в состоянии open|filtered. Это означает, что на пакеты с флагом FIN не пришли однозначные RST-ответы, либо порты действительно открыты и не отвечают, либо фильтрация мешает определить их статус. Особенно критично наличие telnet-порта 23 и незашифрованного RTSP-порта 554 в таком состоянии.

Xmas-сканирование показало, что все 1000 проверенных портов на всех пяти хостах закрыты. Пакеты с флагами FIN+PSH+URG были проигнорированы или сброшены, что свойственно многим ОС и фаерволам.

При Null-сканировании Windows-ловушка проигнорировала пакеты без флагов и все порты оказались закрытыми. Template2 показал open|filtered для портов 21, 23 и 25. Роутер вновь отразил все порты закрытыми. IoT-камера проигнорировала null-пакеты на всех портах, все 1000 портов закрыты. Принтер в null-скане отреагировал как open|filtered на порты 80, 515 и 9100, что говорит о фильтрации или открытых сервисах, не отправляющих RST.

Сканирование IP-протоколов выявило на всех пяти эмуляторах поддержку протоколов ICMP (1), TCP (6) и UDP (17), все они в состоянии open|filtered, то есть принимаются.

АСК-сканирование показало, что на Windows, template2, роутере и принтере все 1000 портов unfiltered (получены RST-ответы). У IoT-камеры 945 портов unfiltered и 55 портов filtered, что может указывать на частичную фильтрацию на уровне TCP.

TCP Window сканирование на всех пяти хостах завершилось получением RST-ответов на запросы с изменённым размером окна, и все порты были классифицированы как closed.

RPC-сканирование (version detection) для Windows-ловушки выявило баннер telnet с предупреждением о перехвате и вопросительные метки у msrpc, netbios-ssn и microsoft-ds. Для template2 FTP и SMTP оказались tcpwrapped, а telnet вернул свой баннер. На роутере были распознаны SSH protocol 1.5 и telnet-баннер Cisco. На IoT-камере HTTP и RTSP оказались tcpwrapped. На принтере HTTP и LPD (515) tcpwrapped, а jetdirect определился с вопросительным признаком.

Определение ОС (-O) не дало точных совпадений для Windows-ловушки, template2 и принтера, что характерно для эмуляторов. Роутер показал открытые 22 и 23 портов с 117 фильтрованными и 881 закрытым, но без точного профиля ОС. IoT-камера и принтер открыли свои сервисные порты и частично отфильтрованные порты (37 у камеры), но nmap не сумел выбрать точную ОС, лишь предоставил TCP/IP-отпечатки.

Часть 2

Произвести сканирование ip адреса 44.241.66.173 **nmap -T4 -A -v 44.241.66.173** (см. рисунок 1).

```
root@hacker:/home/user# nmap -T4 -A -v 44.241.66.173
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-19 17:11 MSK
NSE: Loaded 132 scripts for scanning
```

Рисунок 1 – сканирование адреса

Открыть wireshark командой **sudo wireshark** и после сканирования поставить фильтр ftp (см. рисунок 2).

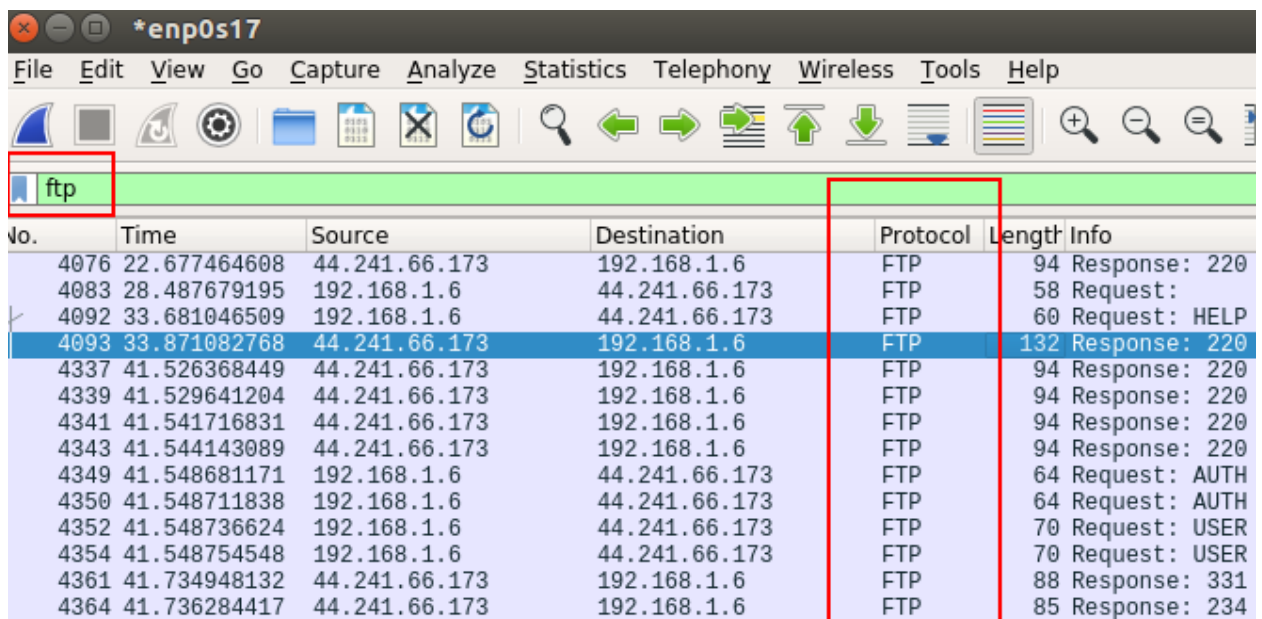


Рисунок 2 – FTP

Анализ пакетов показал, что при установлении соединения сервер многократно присылал приветствие 220 Welcome to the DLP Test FTP Server. Клиент отправлял команду AUTH TLS для начала защиты TLS, после чего сервер отвечал 234 Proceed with negotiation. Затем клиент передавал зашифрованные фрагменты TLS-рукопожатия на порты, соответствующие исходным и целевым. Кроме того, в незашифрованной части трафика были видны команды USER и PASS (см. рисунок 3).

4108	44.030984252	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4125	49.757968257	192.168.1.6	44.241.66.173	FTP	58 Request:
4135	55.946181091	192.168.1.6	44.241.66.173	FTP	60 Request: HELP
4137	56.123083636	44.241.66.173	192.168.1.6	FTP	132 Response: 220 Welcome to the DLP Test FTP Server
4337	62.664316549	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4342	62.907668271	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4352	63.234250790	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4361	63.295871355	192.168.1.6	44.241.66.173	FTP	64 Request: AUTH TLS
4362	63.295941857	192.168.1.6	44.241.66.173	FTP	64 Request: AUTH TLS
4363	63.295962486	192.168.1.6	44.241.66.173	FTP	70 Request: USER anonymous
4368	63.478088203	44.241.66.173	192.168.1.6	FTP	88 Response: 331 Please specify the password.
4370	63.482919289	44.241.66.173	192.168.1.6	FTP	85 Response: 234 Proceed with negotiation.
4372	63.487540482	44.241.66.173	192.168.1.6	FTP	85 Response: 234 Proceed with negotiation.
4374	63.498757329	192.168.1.6	44.241.66.173	FTP	112 Request: \026\003\000\0005\001\000\0001\003\003h\003...
4375	63.499193758	192.168.1.6	44.241.66.173	FTP	571 Request: \026\003\001\002\000\001\000\001\374\003\00...
4376	63.499241888	192.168.1.6	44.241.66.173	FTP	68 Request: PASS IEUser@
4388	63.683095013	44.241.66.173	192.168.1.6	FTP	1269 Response: \026\003\003\000:\002\000\0006\003\003,\27...
4389	63.685595440	44.241.66.173	192.168.1.6	FTP	879 Response: \026\003\003\000J\002\000\000F\003\003\235...
4390	63.686365925	192.168.1.6	44.241.66.173	FTP	280 Request: \026\003\003\000\av\000\000\003\000\000\00...
4403	63.867462362	44.241.66.173	192.168.1.6	FTP	304 Response: \026\003\003\000\252\004\000\000\246\177\3...
4407	63.917973230	192.168.1.6	44.241.66.173	FTP	107 Request: \025\003\003\0000\353\021\222\227qn\200\Fxz...
4416	64.053557870	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4418	64.070904408	192.168.1.6	44.241.66.173	FTP	64 Request: AUTH TLS
4424	64.248528266	44.241.66.173	192.168.1.6	FTP	85 Response: 234 Proceed with negotiation.
4427	64.294589323	192.168.1.6	44.241.66.173	FTP	112 Request: \026\003\000\0005\001\000\0001\003\003h\003...
4429	64.373948982	44.241.66.173	192.168.1.6	FTP	94 Response: 220 Welcome to the DLP Test FTP Server
4434	64.395173119	192.168.1.6	44.241.66.173	FTP	70 Request: USER anonymous
4435	64.473162800	44.241.66.173	192.168.1.6	FTP	879 Response: \026\003\003\000J\002\000\000F\003\003\312...
4445	64.635717669	44.241.66.173	192.168.1.6	FTP	88 Response: 331 Please specify the password.
4446	64.664724847	192.168.1.6	44.241.66.173	FTP	68 Request: PASS IEUser@
4447	64.694574744	44.241.66.173	192.168.1.6	FTP	134 Response: 500 OOPS: error:00000000:lib(0):func(0):re...
4451	64.703814064	44.241.66.173	192.168.1.6	FTP	134 Response: 500 OOPS: error:00000000:lib(0):func(0):re...
4506	68.095312318	44.241.66.173	192.168.1.6	FTP	76 Response: 530 Login incorrect.
4520	68.403126864	44.241.66.173	192.168.1.6	FTP	76 Response: 530 Login incorrect.

Рисунок 3 – пакеты FTP

Для входа на FTP-сервер использовалась учётная запись: логин anonymous и пароль IEUser@.

Вывод

В ходе лабораторной работы была проведена настройка и запуск honeypot-среды с использованием Honeyd, а также выполнено подробное сканирование различных типов ловушек с помощью утилиты Nmap. Были изучены и применены методы TCP Connect, TCP SYN, FIN, Xmas, Null, ACK, IP протокольное, TCP Window и RPC сканирования. На основе полученных данных подтверждена корректность конфигурации эмуляторов, так как открытые порты совпадали с заданными в конфиге honeyd. Особое внимание уделено порту 23 (telnet), который является потенциально уязвимым. Разные типы сканирования позволили выявить особенности фильтрации и поведения системы при получении нестандартных сетевых пакетов. Также были получены баннеры и версии эмулируемых сервисов, что демонстрирует возможности сбора информации о системе без её фактического взлома. Работа позволила на практике освоить принципы использования honeypot'ов для защиты сетей и методы сканирования, применяемые злоумышленниками. Полученные знания полезны для анализа потенциальных угроз и создания более устойчивой инфраструктуры безопасности.

Контрольные вопросы

1. Что такое статический и динамический IP-адреса? В чём разница?

Статический IP-адрес назначается вручную и неизменен вплоть до ручного переназначения, тогда как динамический IP-адрес выделяется сервером DHCP и может меняться при каждом подключении или обновлении аренды. Основное различие состоит в том, что статические адреса удобны для серверов и служб, требующих постоянного адреса, а динамические более экономны и просты в управлении для клиентских устройств.

2. В чём заключается метод сканирование протоколов IP?

Метод сканирования протоколов IP заключается в отправке пакетов с разными значениями поля «Protocol» (например, ICMP, TCP, UDP и т. д.) и анализе ответов, чтобы определить, какие протоколы поддерживает хост. Такой подход позволяет получить представление о сетевых возможностях целевой машины и настроенных фильтрах.

3. На какие пакеты большинство ОС должны ответить флагом RST?

Большинство операционных систем при получении TCP-пакетов с флагами SYN к закрытым портам или при неожиданных пакетах типа ACK, FIN, NULL и XMAS к любым портам должны ответить флагом RST. Это позволяет однозначно отличить закрытые порты от фильтруемых.

4. Назначение, цели, описание Honeypot.

Honeypot представляет собой специально сконфигурированный «приманочный» сервер или сервис, имитирующий уязвимые системы для привлечения злоумышленников. Его цели — обнаружение и анализ атак, изучение тактик злоумышленников и отвлечение их от реальных ресурсов.

5. Какие цели может преследовать злоумышленник, взламывая сервера?

Злоумышленник может стремиться украсть конфиденциальные данные, получить несанкционированный доступ для дальнейшего распространения вредоносного ПО или использовать ресурсы сервера в ботнетах, для майнинга или скрытой компрометации сети. Также возможны цели шпионаж, вымогательство и порча репутации.

6. Как выявлять Honeypot?

Выявлять honeypot можно по нетипичному поведению сервисов, завышенной скорости отклика, отсутствию реальной нагрузки или по аномалиям в отпечатках ОС и версий сервисов. Ограниченный набор функций и единообразие конфигурации также выдают искусственный характер «ловушки».

7. Перечислите основные методы сканирования Nmap.

Основные методы сканирования Nmap включают TCP Connect (-sT), SYN или «half-open» скан (-sS), FIN (-sF), Xmas (-sX), Null (-sN), ACK (-sA), UDP (-sU), а также версии сканирования и RPC/версии (-sV/-sR) и обнаружение ОС (-O). Каждый из этих методов позволяет получать разную степень информации о состоянии портов и характеристиках хоста.