Министр науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Лабораторная работа №1

Сетевая безопасность

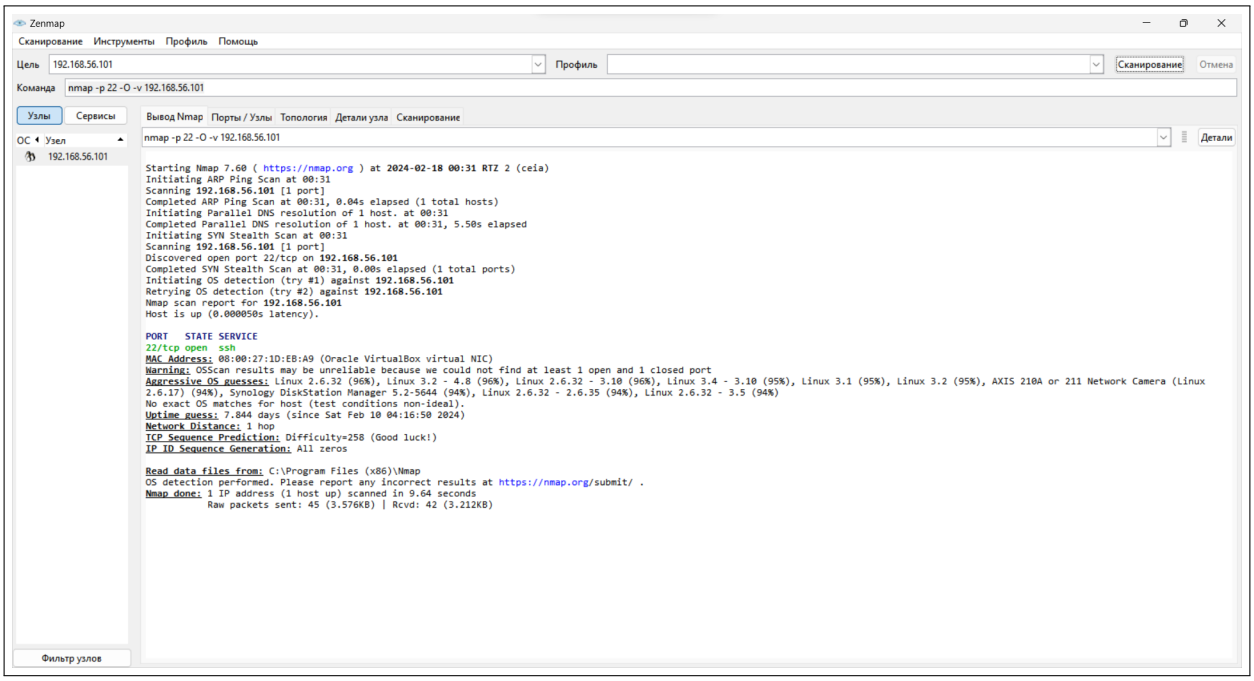
Выполнил студент группы № M34041
Титов Даниил Ярославович

Проверил:
Батоцыренов Павел Андреевич

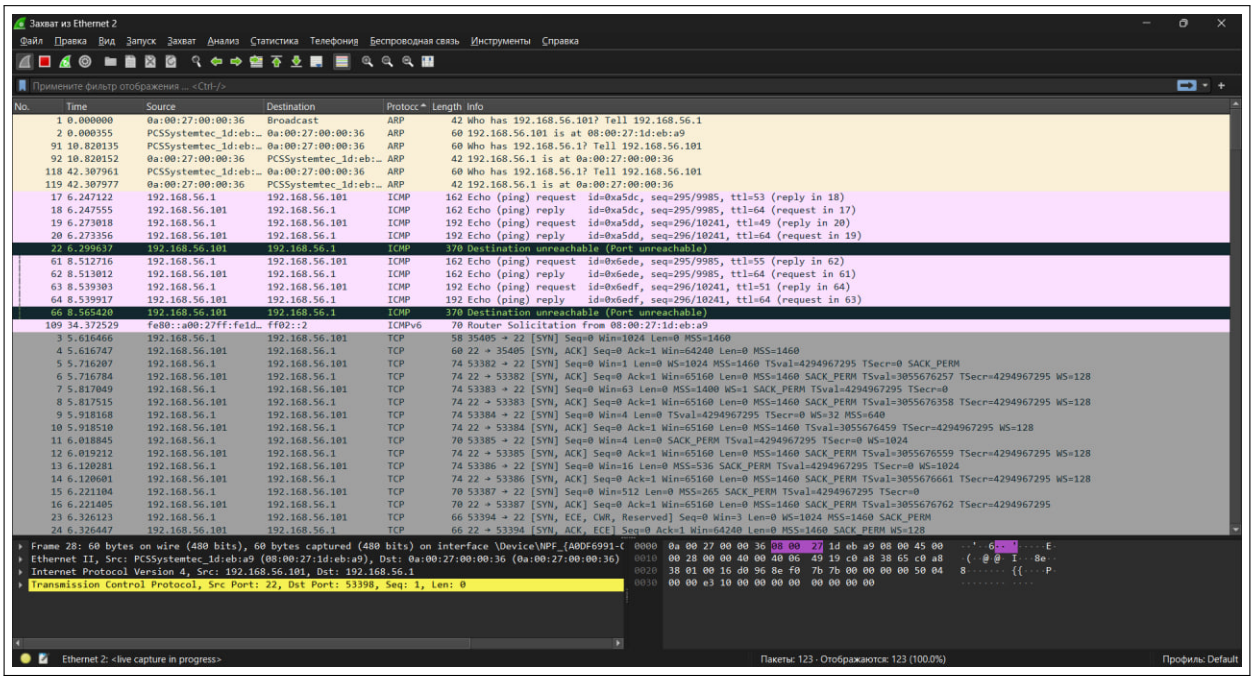
Санкт-Петербург

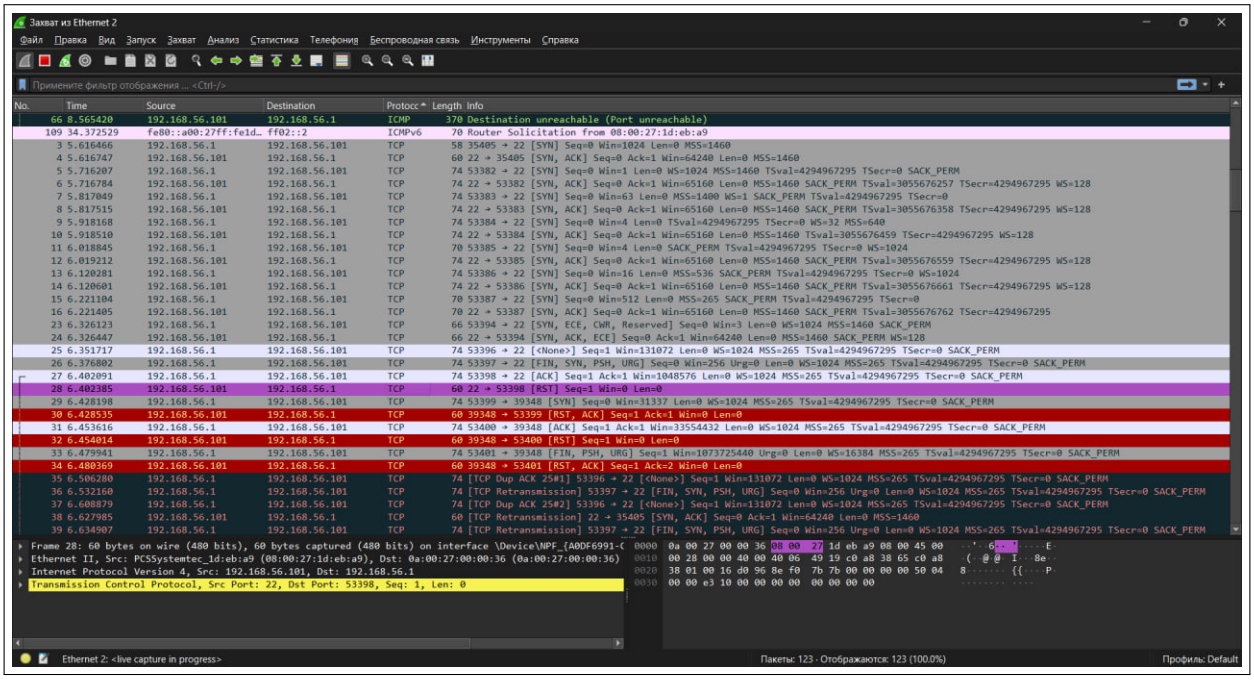
2024

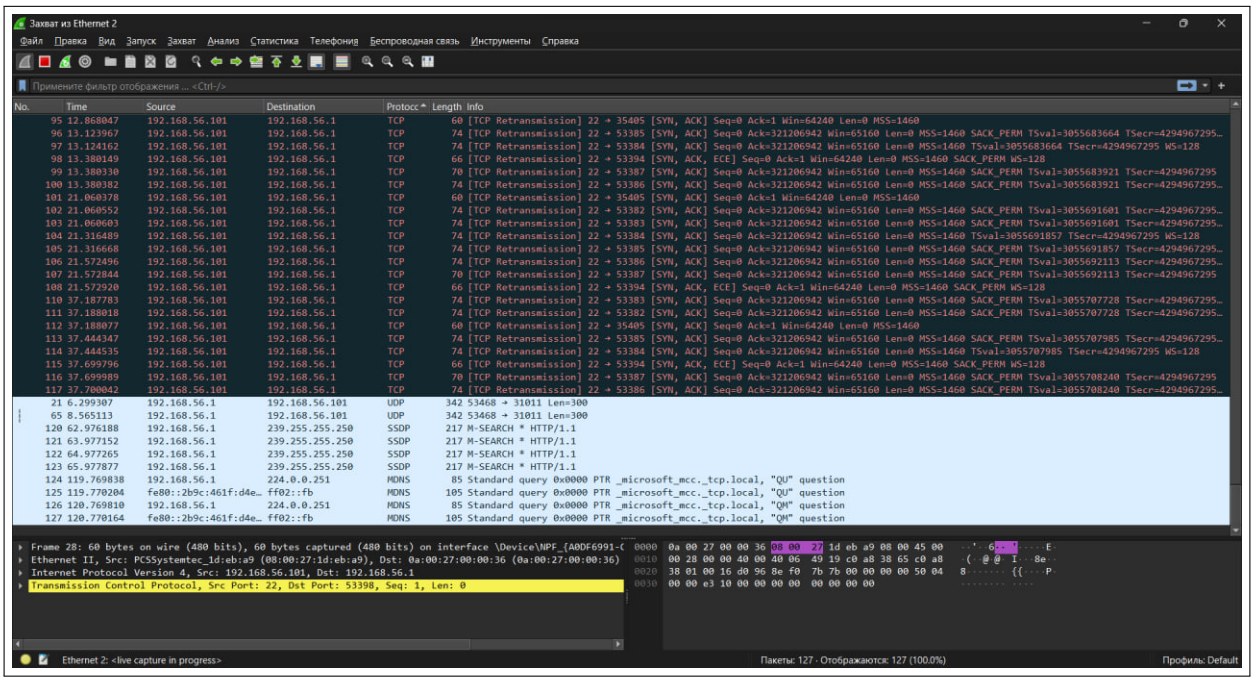
1 Запуск Nmap с опцией определения версии ОС



2 Виды отправленных пакетов, отображающиеся в Wireshark




Захват из Ethernet 2
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
Примените фильтр отображения ... <Ctrl-/>
No. Time Source Destination Protocc Length Info
66 8.565420 192.168.56.101 192.168.56.1 ICMP 370 Destination unreachable (Port unreachable)
109 34.372529 fe80::a00:27ff:fe1d… ff02::2 ICMPv6 70 Router Solicitation from 08:00:27:1d:eb:a9
3 5.616466 192.168.56.1 192.168.56.101 TCP 58 35405 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4 5.616747 192.168.56.101 192.168.56.1 TCP 60 22 → 35405 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5 5.716207 192.168.56.1 192.168.56.101 TCP 74 53382 → 22 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=4294967295 TSecr=0 SACK_PERM
6 5.716784 192.168.56.101 192.168.56.1 TCP 74 22 → 53382 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055676257 TSecr=4294967295 WS=128
7 5.817049 192.168.56.1 192.168.56.101 TCP 74 53383 → 22 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM TSval=4294967295 TSecr=0
8 5.817515 192.168.56.101 192.168.56.1 TCP 74 22 → 53383 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055676358 TSecr=4294967295 WS=128
9 5.918168 192.168.56.1 192.168.56.101 TCP 74 53384 → 22 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 WS=32 MSS=640
10 5.918510 192.168.56.101 192.168.56.1 TCP 74 22 → 53384 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 TSval=3055676459 TSecr=4294967295 WS=128
11 6.018845 192.168.56.1 192.168.56.101 TCP 70 53385 → 22 [SYN] Seq=0 Win=4 Len=0 SACK_PERM TSval=4294967295 TSecr=0 WS=1024
12 6.019212 192.168.56.101 192.168.56.1 TCP 74 22 → 53385 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055676559 TSecr=4294967295 WS=128
13 6.120281 192.168.56.1 192.168.56.101 TCP 74 53386 → 22 [SYN] Seq=0 Win=16 Len=0 MSS=536 SACK_PERM TSval=4294967295 TSecr=0 WS=1024
14 6.120601 192.168.56.101 192.168.56.1 TCP 74 22 → 53386 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055676661 TSecr=4294967295 WS=128
15 6.221104 192.168.56.1 192.168.56.101 TCP 70 53387 → 22 [SYN] Seq=0 Win=512 Len=0 MSS=265 SACK_PERM TSval=4294967295 TSecr=0
16 6.221405 192.168.56.101 192.168.56.1 TCP 70 22 → 53387 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055676762 TSecr=4294967295
23 6.326123 192.168.56.1 192.168.56.101 TCP 66 53394 → 22 [SYN, ECE, CWR, Reserved] Seq=0 Win=3 Len=0 WS=1024 MSS=1460 SACK_PERM
24 6.326447 192.168.56.101 192.168.56.1 TCP 66 22 → 53394 [SYN, ACK, ECE] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
25 6.351717 192.168.56.1 192.168.56.101 TCP 74 53396 → 22 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
26 6.376802 192.168.56.1 192.168.56.101 TCP 74 53397 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
27 6.402091 192.168.56.1 192.168.56.101 TCP 74 53398 → 22 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
28 6.402385 192.168.56.101 192.168.56.1 TCP 60 22 → 53398 [RST] Seq=1 Win=0 Len=0
29 6.428198 192.168.56.1 192.168.56.101 TCP 74 53399 → 39348 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
30 6.428535 192.168.56.101 192.168.56.1 TCP 60 39348 → 53399 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 6.453616 192.168.56.1 192.168.56.101 TCP 74 53400 → 39348 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
32 6.454014 192.168.56.101 192.168.56.1 TCP 60 39348 → 53400 [RST] Seq=1 Win=0 Len=0
33 6.479941 192.168.56.1 192.168.56.101 TCP 74 53401 → 39348 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
34 6.480369 192.168.56.101 192.168.56.1 TCP 60 39348 → 53401 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
35 6.506280 192.168.56.1 192.168.56.101 TCP 74 [TCP Dup ACK 25#1] 53396 → 22 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
36 6.532160 192.168.56.1 192.168.56.101 TCP 74 [TCP Retransmission] 53397 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
37 6.608879 192.168.56.1 192.168.56.101 TCP 74 [TCP Dup ACK 25#2] 53396 → 22 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
38 6.627985 192.168.56.101 192.168.56.1 TCP 60 [TCP Retransmission] 22 → 35405 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
39 6.634907 192.168.56.1 192.168.56.101 TCP 74 [TCP Retransmission] 53397 → 22 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MSS=265 TSval=4294967295 TSecr=0 SACK_PERM
Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A0DF6991-C
Ethernet II, Src: PCSSystemtec_1d:eb:a9 (08:00:27:1d:eb:a9), Dst: 0a:00:27:00:00:36 (0a:00:27:00:00:36)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1
Transmission Control Protocol, Src Port: 22, Dst Port: 53398, Seq: 1, Len: 0
0000 0a 00 27 00 00 36 08 00 27 1d eb a9 08 00 45 00
0010 00 28 00 00 40 00 40 06 49 19 c0 a8 38 65 c0 a8
0020 38 01 00 16 d0 96 8e f0 7b 7b 00 00 00 00 50 04
0030 00 00 e3 10 00 00 00 00
Ethernet 2: <live capture in progress>
Пакеты: 123 · Отображаются: 123 (100.0%)
Профиль: Default


Захват из Ethernet 2
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
Примените фильтр отображения ... <Ctrl-/>
No. Time Source Destination Protocc Length Info
95 12.868047 192.168.56.101 192.168.56.1 TCP 60 [TCP Retransmission] 22 → 35405 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
96 13.123967 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53385 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055683664 TSecr=4294967295…
97 13.124162 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53384 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 TSval=3055683664 TSecr=4294967295 WS=128
98 13.380149 192.168.56.101 192.168.56.1 TCP 66 [TCP Retransmission] 22 → 53394 [SYN, ACK, ECE] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
99 13.380330 192.168.56.101 192.168.56.1 TCP 70 [TCP Retransmission] 22 → 53387 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055683921 TSecr=4294967295
100 13.380382 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53386 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055683921 TSecr=4294967295…
101 21.060378 192.168.56.101 192.168.56.1 TCP 60 [TCP Retransmission] 22 → 35405 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
102 21.060552 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53382 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055691601 TSecr=4294967295…
103 21.060603 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53383 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055691601 TSecr=4294967295…
104 21.316489 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53384 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 TSval=3055691857 TSecr=4294967295 WS=128
105 21.316668 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53385 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055691857 TSecr=4294967295…
106 21.572496 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53386 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055692113 TSecr=4294967295…
107 21.572844 192.168.56.101 192.168.56.1 TCP 70 [TCP Retransmission] 22 → 53387 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055692113 TSecr=4294967295
108 21.572920 192.168.56.101 192.168.56.1 TCP 66 [TCP Retransmission] 22 → 53394 [SYN, ACK, ECE] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
110 37.187783 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53383 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055707728 TSecr=4294967295…
111 37.188018 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53382 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055707728 TSecr=4294967295…
112 37.188077 192.168.56.101 192.168.56.1 TCP 60 [TCP Retransmission] 22 → 35405 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
113 37.444347 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53385 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055707985 TSecr=4294967295…
114 37.444535 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53384 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 TSval=3055707985 TSecr=4294967295 WS=128
115 37.699796 192.168.56.101 192.168.56.1 TCP 66 [TCP Retransmission] 22 → 53394 [SYN, ACK, ECE] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
116 37.699989 192.168.56.101 192.168.56.1 TCP 70 [TCP Retransmission] 22 → 53387 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055708240 TSecr=4294967295
117 37.700042 192.168.56.101 192.168.56.1 TCP 74 [TCP Retransmission] 22 → 53386 [SYN, ACK] Seq=0 Ack=321206942 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3055708240 TSecr=4294967295…
21 6.299307 192.168.56.1 192.168.56.101 UDP 342 53468 → 31011 Len=300
65 8.565113 192.168.56.1 192.168.56.101 UDP 342 53468 → 31011 Len=300
120 62.976188 192.168.56.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
121 63.977152 192.168.56.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
122 64.977265 192.168.56.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
123 65.977877 192.168.56.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
124 119.769838 192.168.56.1 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
125 119.770204 fe80::2b9c:461f:d4e… ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
126 120.769810 192.168.56.1 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
127 120.770164 fe80::2b9c:461f:d4e… ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A0DF6991-C
Ethernet II, Src: PCSSystemtec_1d:eb:a9 (08:00:27:1d:eb:a9), Dst: 0a:00:27:00:00:36 (0a:00:27:00:00:36)
Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.1
Transmission Control Protocol, Src Port: 22, Dst Port: 53398, Seq: 1, Len: 0
0000 0a 00 27 00 00 36 08 00 27 1d eb a9 08 00 45 00
0010 00 28 00 00 40 00 40 06 49 19 c0 a8 38 65 c0 a8
0020 38 01 00 16 d0 96 8e f0 7b 7b 00 00 00 00 50 04
0030 00 00 e3 10 00 00 00 00
Ethernet 2: <live capture in progress>
Пакеты: 127 · Отображаются: 127 (100.0%)
Профиль: Default

3 Правила обнаружения атак для Snort

```
root@debian11:/etc/snort/rules# cat lab1.rules
alert icmp any any -> any any (msg: "Nmap: icmp 120"; dsize:120; sid:1;)
alert icmp any any -> any any (msg: "Nmap: icmp 150"; dsize:150; sid:2;)
alert tcp any any -> any any (msg: "Nmap: tcp SYN + ECE + CWR"; flags:SEC; sid:3;)
alert tcp any any -> any any (msg: "Nmap: tcp"; flags:0; Sid:4;)
alert tcp any any -> any any (msg: "Nmap: tcp FIN + SYN + PSH + URG"; flags:FSPU; sid:5;)
alert udp any any -> any any (msg: "Nmap: udp 300"; content:"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"; dsize:300; sid:6;)
root@debian11:/etc/snort/rules#
```

4 Обнаружение сканирования с помощью Snort

```
Администратор: Windows Pow  Администратор: Windows Pc
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
Commencing packet processing (pid=810)
02/18-00:31:32.415257  [**] [1:1:0] Nmap: icmp 120 [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
02/18-00:31:32.415275  [**] [1:1:0] Nmap: icmp 120 [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
02/18-00:31:32.441067  [**] [1:2:0] Nmap: icmp 150 [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
02/18-00:31:32.441082  [**] [1:2:0] Nmap: icmp 150 [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
02/18-00:31:32.467342  [**] [1:6:0] Nmap: udp 300 [**] [Priority: 0] {UDP} 192.168.56.1:53468 -> 192.168.56.101:31011
02/18-00:31:32.494154  [**] [1:3:0] Nmap: tcp SYN + ECE + CWR [**] [Priority: 0] {TCP} 192.168.56.1:53394 -> 192.168.56.101:22
02/18-00:31:32.519801  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:32.544867  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:32.648062  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.56.1:53401 -> 192.168.56
.101:39348
02/18-00:31:32.674352  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:32.700207  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:32.776927  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:32.802907  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:32.879990  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:32.906054  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:34.680727  [**] [1:1:0] Nmap: icmp 120 [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
02/18-00:31:34.680742  [**] [1:1:0] Nmap: icmp 120 [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
02/18-00:31:34.707633  [**] [1:2:0] Nmap: icmp 150 [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
02/18-00:31:34.707648  [**] [1:2:0] Nmap: icmp 150 [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
02/18-00:31:34.733132  [**] [1:6:0] Nmap: udp 300 [**] [Priority: 0] {UDP} 192.168.56.1:53468 -> 192.168.56.101:31011
02/18-00:31:34.759399  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:34.787006  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:34.889533  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.56.1:53401 -> 192.168.56
.101:38804
02/18-00:31:34.915391  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:34.941084  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:35.017411  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:35.042840  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:31:35.118059  [**] [1:4:0] Nmap: tcp [**] [Priority: 0] {TCP} 192.168.56.1:53396 -> 192.168.56.101:22
02/18-00:31:35.145570  [**] [1:5:0] Nmap: tcp FIN + SYN + PSH + URG [**] [Priority: 0] {TCP} 192.168.56.1:53397 -> 192.168.56.101:22
02/18-00:32:29.144424  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.
1:50803 -> 239.255.255.250:1900
02/18-00:32:30.145404  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.56.
```