

Лабораторная работа №4
Курс: Защита информации

Патраков Николай

25 сентября 2015 г.

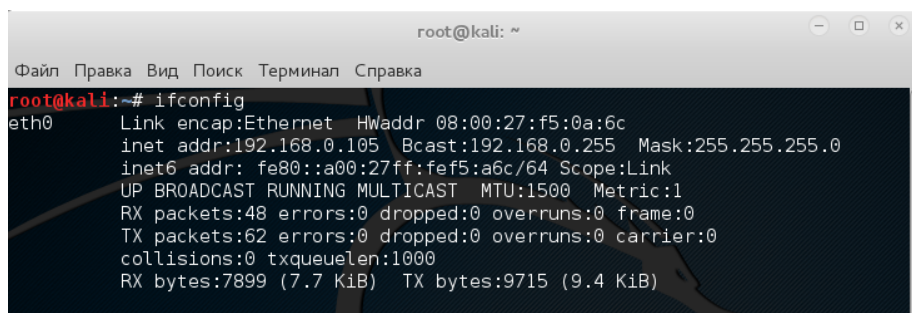
Содержание

1	Работа с утилитой nmap	3
1.1	Начальные настройки	3
1.2	Поиск активных портов	5
1.3	Определить открытые порты	6
1.4	Определить версии портов	7
1.5	Изучить файлы nmap-services, nmap-os-db,nmap-service-probes	8
1.6	Добавить новую сигнатуру службы в файл nmap-service-probes	12
1.7	Сохранить вывод утилиты в XML	12
1.8	Исследовать работу nmap с применением WIRESHARK	13
2	Вывод	15

1 Работа с утилитой nmap

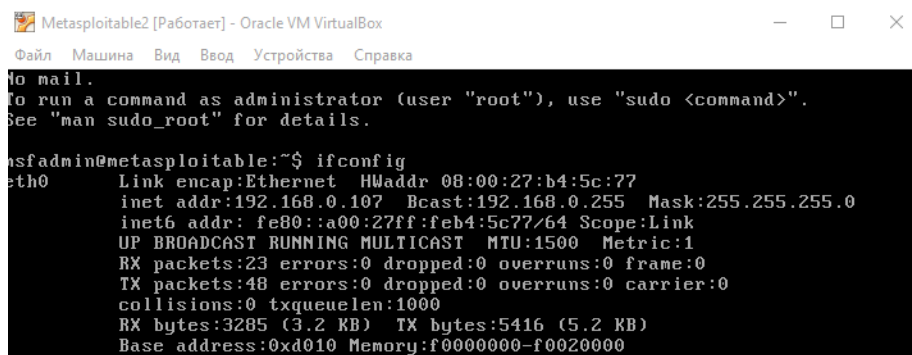
1.1 Начальные настройки

В ходе данной работы будут использоваться две виртуальные машины: одна для сканирования, другая- как цель для сканирования. Для сканирования используется система Kali Linux с предустановленными утилитами. В качестве объекта для сканирования используется metasploitable. Обе эти системы запускаются в с настройками сети в режиме сетевого моста. Так виртуальные машины смогут видеть друг друга в локальной сети и это обезопасит работу с ними. Используем команду ifconfig и убедимся, что машины получили свои ip-адреса (Рис. 1 и Рис. 2).



```
root@kali: ~  
Файл Правка Вид Поиск Терминал Справка  
root@kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:f5:0a:6c  
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5:a6c/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:7899 (7.7 KiB)  TX bytes:9715 (9.4 KiB)
```

Рис. 1: IP Kali



```
Metasploitable2 [Работаer] - Oracle VM VirtualBox  
Файл Машина Вид Ввод Устройства Справка  
No mail.  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:b4:5c:77  
          inet addr:192.168.0.107  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:feb4:5c77/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:3285 (3.2 KB)  TX bytes:5416 (5.2 KB)  
          Base address:0xd010 Memory:f0000000-f0020000
```

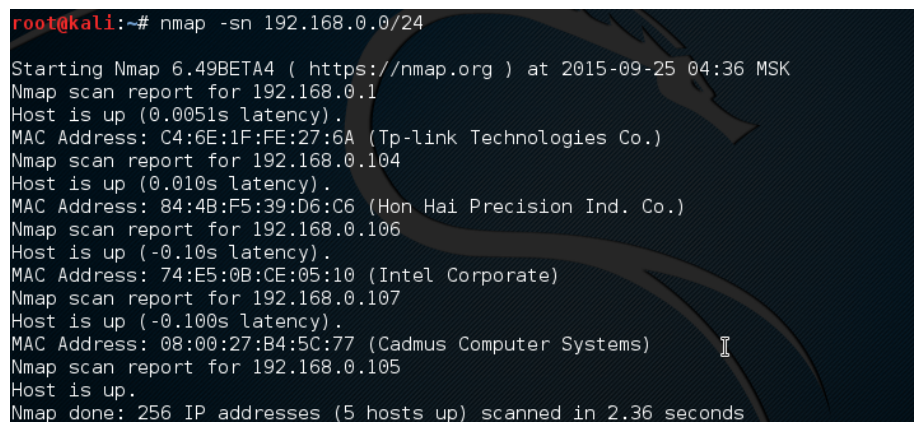
Рис. 2: IP Metasploitable

1.2 Поиск активных портов

Поиск активных хостов осуществляется с помощью следующей команды.

```
nmap -sn 192.168.0.0/24
```

Эта команда просканирует локальную сеть на наличие открытых хостов и покажет все доступные для прозванивания IP адреса(Рис 3). Вот результат.



```
root@kali:~# nmap -sn 192.168.0.0/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-25 04:36 MSK
Nmap scan report for 192.168.0.1
Host is up (0.0051s latency).
MAC Address: C4:6E:1F:FE:27:6A (Tp-link Technologies Co.)
Nmap scan report for 192.168.0.104
Host is up (0.010s latency).
MAC Address: 84:4B:F5:39:D6:C6 (Hon Hai Precision Ind. Co.)
Nmap scan report for 192.168.0.106
Host is up (-0.10s latency).
MAC Address: 74:E5:0B:CE:05:10 (Intel Corporate)
Nmap scan report for 192.168.0.107
Host is up (-0.100s latency).
MAC Address: 08:00:27:B4:5C:77 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.105
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.36 seconds
```

Рис. 3: Список активных хостов.

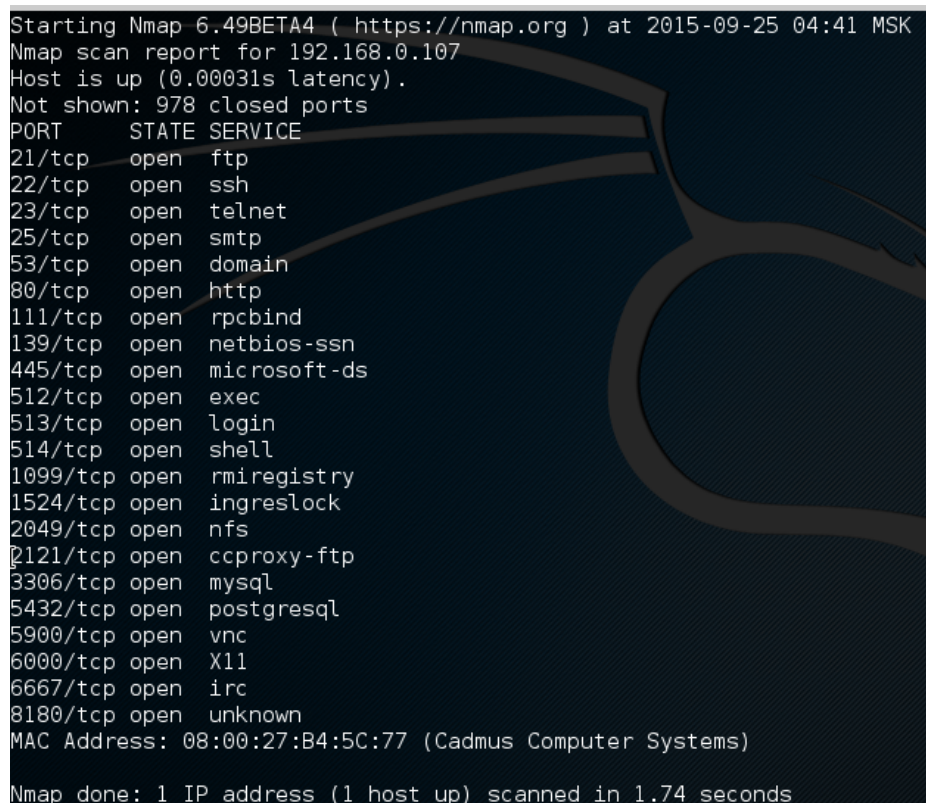
Последние 2 адреса - это адреса виртуальных машин запущенных на данном компьютере. Адрес 192.168.0.107 это адрес metasploitable к которому мы будем обращаться в течении работы.

1.3 Определить открытые порты

Поиск открытых портов осуществляется с помощью следующей команды.

```
nmap -open 192.168.0.107
```

Эта команда просканирует IP адрес на наличие открытых портов и покажет все доступные для прозванивания порты(Рис 4). Вот результат.



```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-25 04:41 MSK
Nmap scan report for 192.168.0.107
Host is up (0.00031s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:B4:5C:77 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

Рис. 4: Список всех открытых портов по данному IP адресу.

Стоит отметить что показываются только открытые порты на данном адресе. Для отображения всех портов следует использовать другую команду.

```
nmap -p 0-65536 192.168.0.107
```

Обработка такого запроса анимает гораздо больше времени, чем предыдущего, так как программа обращается ко всем возможным портам по данному IP адресу.

1.4 Определить версии портов

Отображение версий портов осуществляется следующей командой.

```
nmap -sV 192.168.0.107
```

Результат обработки такого запроса представлен на рисунке 5.



```
Nmap scan report for 192.168.0.107
Host is up (0.00019s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rshcd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry   GNU Classpath grmiregistry
1524/tcp  open  shell         Metasploitable root shell
2049/tcp  open  nfs           2.4 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           Unreal ircd
8180/tcp  open  unknown
MAC Address: 08:00:27:B4:5C:77 (Cadmus Computer Systems)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Рис. 5: Список открытых портов с версиями сервисов.

1.5 Изучить файлы nmap-services, nmap-os-db, nmap-service-probes

Файл nmap-services содержит набор наиболее часто используемых портов и сервисов на них. Подключение этого файла к процессу сканирования позволяет ускорить обработку команды, так как опрос будет проводиться не по всем 65536 портам а только по тем, которые указаны в файле. Содержимое файла представлено на рисунке 6.

```
tcpmux 1/udp 0.001236 # TCP Port Service Multiplexer
compressnet 2/tcp 0.000013 # Management Utility
compressnet 2/udp 0.001845 # Management Utility
compressnet 3/tcp 0.001242 # Compression Process
compressnet 3/udp 0.001532 # Compression Process
unknown 4/tcp 0.000477
rje 5/udp 0.000593 # Remote Job Entry
unknown 6/tcp 0.000502
echo 7/sctp 0.000000
echo 7/tcp 0.004855
echo 7/udp 0.024679
unknown 8/tcp 0.000013
discard 9/sctp 0.000000 # sink null
discard 9/tcp 0.003764 # sink null
discard 9/udp 0.015733 # sink null
unknown 10/tcp 0.000063
systat 11/tcp 0.000075 # Active Users
systat 11/udp 0.000577 # Active Users
unknown 12/tcp 0.000063
daytime 13/tcp 0.003927
daytime 13/udp 0.004827
unknown 14/tcp 0.000038
netstat 15/tcp 0.000038
unknown 16/tcp 0.000050
qotd 17/tcp 0.002346 # Quote of the Day
qotd 17/udp 0.009209 # Quote of the Day
msp 18/udp 0.000610 # Message Send Protocol
chargen 19/tcp 0.002559 # ttytst source Character Generator
chargen 19/udp 0.015865 # ttytst source Character Generator
ftp-data 20/sctp 0.000000 # File Transfer [Default Data]
ftp-data 20/tcp 0.001079 # File Transfer [Default Data]
```

Рис. 6: Содержимое файла nmap-services.

Этот файл задействуется с помощью опции -F. Выглядит это примерно так.

```
nmap -F 192.168.0.107
```



```
Host is up (0.00021s latency).
Not shown: 83 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
MAC Address: 08:00:27:B4:5C:77 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Рис. 7: Результат работы nmap с опцией -F.

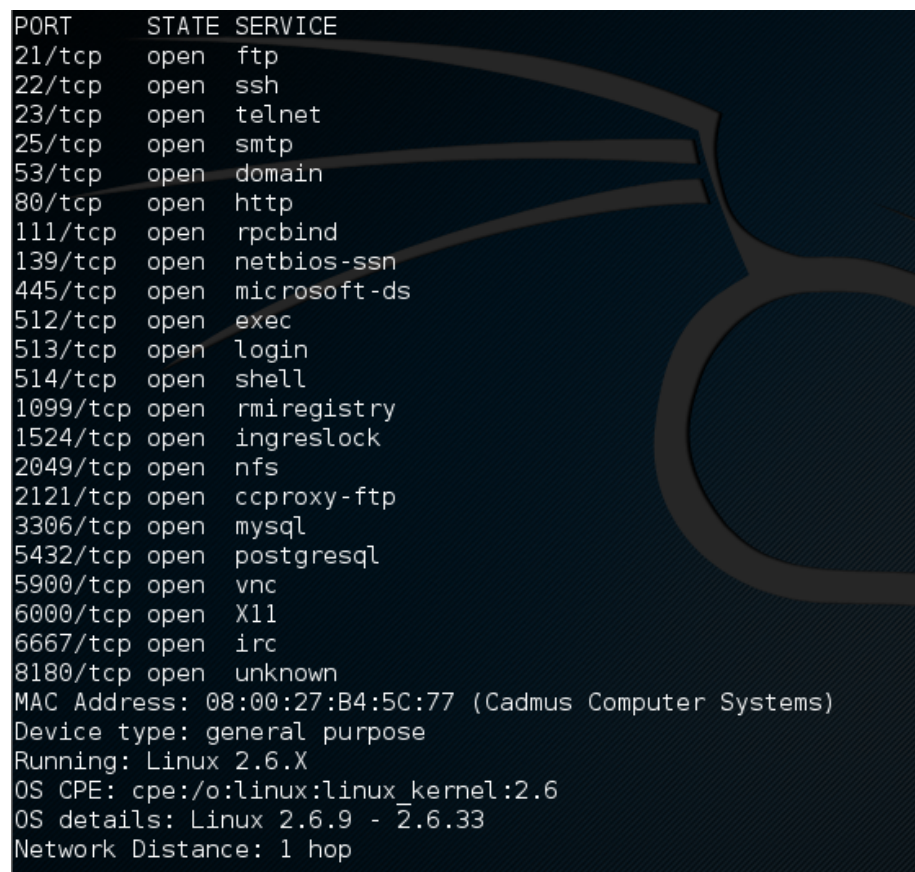
Как видно на рисунке 7, результат не на много, но все же быстрее обычного.

Файл `nmap-os-db` содержит слепки откликов различных операционных систем на запрос `nmap`. Благодаря этому файлу утилита может распознавать различные операционные системы с которыми она в данный момент работает.

Для задействования этого файла используется опция `-O`. Команда выглядит так

```
nmap -O 192.168.0.107
```

В результате работы помимо информации о портах так же выводится информация о опрашиваемой системе.

A screenshot of a terminal window showing the output of an nmap scan. The background is dark blue with a faint, stylized graphic of a person's head and shoulders in a lighter blue. The text is white and lists open ports, their states, and the services running on them. Below the port list, it shows the MAC address, device type, operating system, and network distance.

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8180/tcp	open	unknown

MAC Address: 08:00:27:B4:5C:77 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Рис. 8: Дополнительный вывод утилиты.

```
match 1c-server m|^\S*\x5c\x61a{| p/1C:Enterprise business management server/

match 4d-server m|^\0\0\0H\0\0\0\x02.[^\0]*\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0$ p/4th Dimension database server/

match acap m|^\* ACAP \(\IMPLEMENTATION \"CommuniGate Pro ACAP (\d[-.\w]+)\") | p/CommuniGate Pro ACAP server/ v/$1/ i/for mail client preference sharing/
match acarsd m|^g\0\0\0\0x1b\0\0\0\0\0\0\0\0\0\0acarsd:t{([w_-]+)}\tAPI-([w_-]+)}\0\0\0\0\0x06\0x05\0\0\0\0\0\0\0<?xml | p/acarsd/ v/$1/ i/API $2/ cpe:/a:acarsd:acarsd:$1/
match acmp m|^ACMP Server Version ([w_-]+)\r\n| p/Aagon ACMP Inventory/ v/$1/
match activemq m|^\0\0\0\0.x01ActiveMQ\0\0\0\0$ p/Apache ActiveMQ/ cpe:/a:apache:activemq/

# Microsoft ActiveSync Version 3.7 Build 3083 (It's used for syncing
# my ipaq it disappears when you remove the ipaq.)
match activesync m|^.\0x01\0[^\0]\0[^\0]\0[^\0]\0[^\0]\0.*\0\0\0$ p/Microsoft
ActiveSync/ o/Windows/ cpe:/a:microsoft:activesync/ cpe:/o:microsoft:windows/a
match activesync m|^\(^\0\0\0\0x02\0\0\0\0x03\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0$ p/Citrix ActiveSync/ o/Windows/ cpe:/o:microsoft:windows/a

match adabas-d m|^Adabas D Remote Control Server Version ([\d.]+) Date [\d-]+ \[(key is
[\0-9a-f]+)\r\nOK> | p/Adabas D database remote control/ v/$1/
```

11

1.6 Добавить новую сигнатуру службы в файл nmap-service-probes

Напишем простой tcp-сервер, который просто ждет подключения клиента и отправляет ему сообщение. В файл nmap-service-probes добавим следующую строку:

```
match tcp-server m|^1337| v/1.0.X/ p/Nikolay / i/Kak dela /
```

Таким образом теперь nmap знает, что если при пустом запросе с сервера приходит строка 1337, значит нужно выводить информацию, которая указана на рисунке ниже.

```
root@kali:~# nmap -sV 192.168.0.106 -p9596
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-25 05:39 MSK
Nmap scan report for 192.168.0.106
Host is up (0.00026s latency).
PORT      STATE SERVICE      VERSION
9596/tcp  open  tcp-server  Nikolay 1.0 (kak dela, brat?)
MAC Address: 74:E5:0B:CE:05:10 (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

Рис. 10: Информация о сервисе

1.7 Сохранить вывод утилиты в XML

Сохранение вывода утилиты в формате xml осуществляется всего командой:

```
nmap -sV -oX -p 2404 -scanme.nmap.org 192.168.0.124.4
```

```
<?xml-stylesheet href="file:///usr/bin/.../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 6.49BETA4 scan initiated Fri Sep 25 05:45:47 2015 as: nmap -sV -p 2404 -oX - scanme.nmap.org 192.168.124.4 -->
<nmaprun scanner="nmap" args="nmap -sV -p 2404 -oX - scanme.nmap.org 192.168.124.4" start="1443149147" startstr="Fri Sep 25 05:45:47 2015" version="6.49BETA4" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1" services="2404"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1443149148" endtime="1443149158"><status state="up" reason="echo-reply" reason_ttl="54"/>
<address addr="45.33.32.156" addrtype="ipv4"/>
<hostnames>
<hostname name="scanme.nmap.org" type="user"/>
<hostname name="scanme.nmap.org" type="PTR"/>
</hostnames>
<ports><port protocol="tcp" portid="2404"><state state="closed" reason="reset" reason_ttl="54"/></port>
</ports>
<times srtd="179491" rttvar="134633" to="718023"/>
</host>
<runstats><finished time="1443149158" timestr="Fri Sep 25 05:45:58 2015" elapsed="11.46" summary="Nmap done at Fri Sep 25 05:45:58 2015; 2 IP addresses (1 host up) scanned in 11.46 seconds" exit="success"/><hosts up="1" down="1" total="2"/>
</runstats>
```

Рис. 11: Содержимое файла

1.8 Исследовать работу nmap с применением WIRESHARK

Проанализируем с помощью wireshark каким путем nmap работает с компьютером.

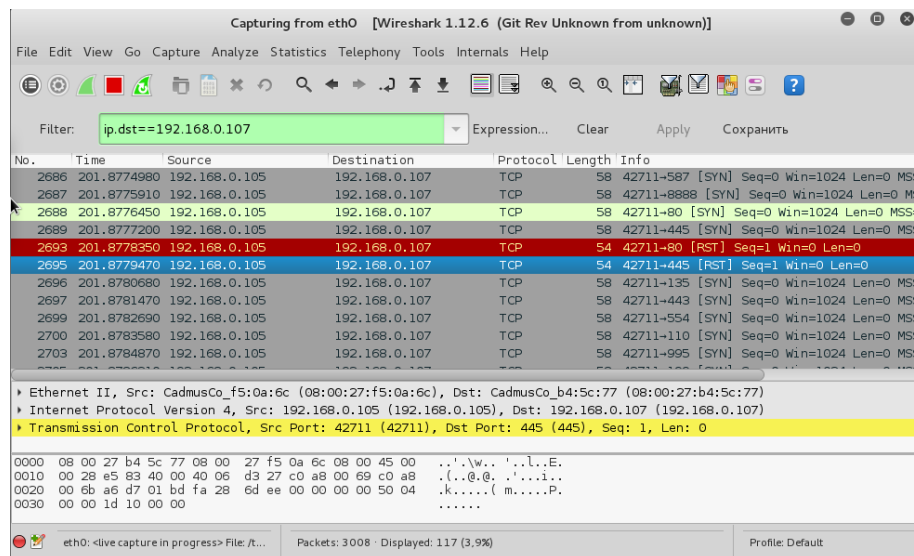


Рис. 12: Демонстрация работы nmap в Wireshark.

Как видно из скриншота утилита устанавливает TCP соединения со всеми портами и анализирует ответы на эти запросы.

Рассмотрите один скрипт из состава NMAP
Рассмотрим скрипт auth-spoof.nse

```
local comm = require "comm"
local shortport = require "shortport"

description = [[
Checks for an identd (auth) server which is spoofing its replies.

Tests whether an identd (auth) server responds with an answer before
we even send the query. This sort of identd spoofing can be a sign of
malware infection, though it can also be used for legitimate privacy
reasons.
]]

---
-- @output
-- PORT      STATE SERVICE REASON
-- 113/tcp   open  auth    syn-ack
-- |_auth-spoof: Spoofed reply: 0, 0 : USERID : UNIX : OGJdvM

author = "Diman Todorov"

license = "Same as Nmap--See http://nmap.org/book/man-legal.html"

categories = {"malware", "safe"}

portrule = shortport.port_or_service(113, "auth")

action = function(host, port)
local status, owner = comm.get_banner(host, port, {lines=1})

if not status then
return
end

return "Spoofed reply: " .. owner
end
```

Сначала объявляются переменные.

```
local comm = require "comm"
local shortport = require "shortport"
```

Затем следует описание скрипта.

```

description = [[
Checks for an identd (auth) server which is spoofing its replies.

Tests whether an identd (auth) server responds with an answer before
we even send the query. This sort of identd spoofing can be a sign of
malware infection, though it can also be used for legitimate privacy
reasons.
]]

```

Затем идет правило порта. Эта функция возвращает true если ответ совпал с правилом и false если нет.

```

portrule = shortport.port_or_service(113, "auth")

```

Затем описано действие.

```

action = function(host, port)
local status, owner = comm.get_banner(host, port, {lines=1})

if not status then
return
end

```

Данный скрипт просто проверяет отклик порта, перед началом работы с ним.

2 Вывод

В ходе данной работы были изучены основные возможности nmap. Определение активных хостов, сканирование портов, определение версий сервисов, дополнение определения версий сервисов, были рассмотрены основные файлы используемые для определения версий сервисов и ОС.

Инструмент nmap является мощным и гибким инструментом для сбора информации.