

Лабораторные работы №4
Курс: Защита информации

Воробьев Олег

6 июня 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	13
1.7	Сохранить вывод утилиты в XML	13
1.8	Исследовать работу nmap с применением WIRESHARK	14

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(Рис 1).

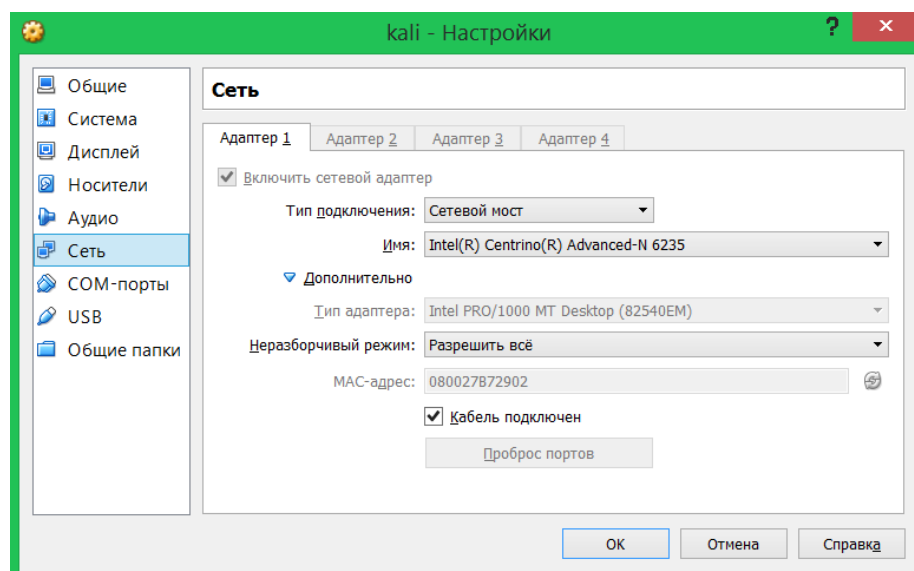


Рис. 1: Настройки сети.

Благодаря таким настройкам, две виртуальные машины могут видеть друг друга в локальной сети. Это обезопасит дальнейшую работу с ними. С помощью команды `ifconfig` можно удостовериться что машины получили свои `ip` адреса для дальнейшей работы с ними(Рис 2).

```
metasploitable [Работаer] - Oracle VM VirtualBox
Машина Вид 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 08:00:27:51:53:7d
          inet addr:192.168.1.19  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe51:537d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:766 errors:0 dropped:0 overruns:0 frame:0
          TX packets:116 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:83257 (81.3 KB)  TX bytes:13317 (13.0 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:530 errors:0 dropped:0 overruns:0 frame:0
          TX packets:530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:233993 (228.5 KB)  TX bytes:233993 (228.5 KB)

msfadmin@metasploitable:~$ _

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b7:29:02
          inet addr:192.168.1.18  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb7:2902/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11803 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7440 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17541258 (16.7 MiB)  TX bytes:526013 (513.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2160 (2.1 KiB)  TX bytes:2160 (2.1 KiB)

root@kali:~#
```

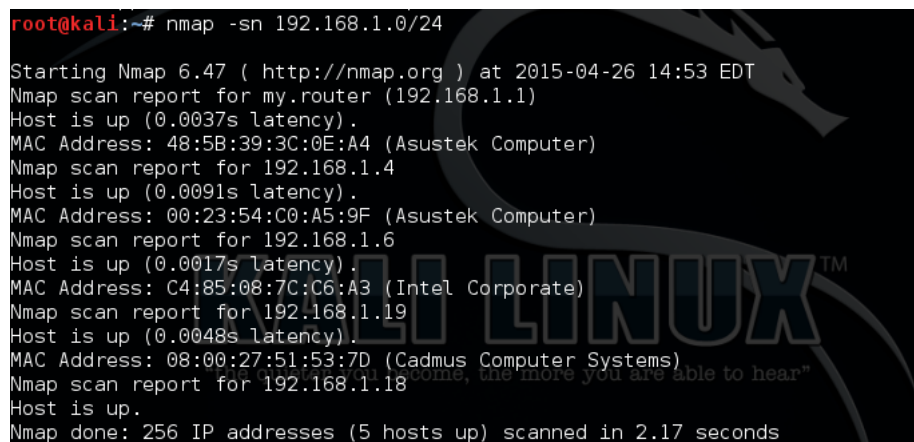
Рис. 2: IP адреса машин.

1.2 Поиск активных портов

Поиск активных хостов осуществляется с помощью следующей команды.

```
nmap -sn 192.168.1.0/24
```

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 192.168.1.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-26 14:53 EDT
Nmap scan report for my.router (192.168.1.1)
Host is up (0.0037s latency).
MAC Address: 48:5B:39:3C:0E:A4 (Asustek Computer)
Nmap scan report for 192.168.1.4
Host is up (0.0091s latency).
MAC Address: 00:23:54:C0:A5:9F (Asustek Computer)
Nmap scan report for 192.168.1.6
Host is up (0.0017s latency).
MAC Address: C4:85:08:7C:C6:A3 (Intel Corporate)
Nmap scan report for 192.168.1.19
Host is up (0.0048s latency).
MAC Address: 08:00:27:51:53:7D (Cadmus Computer Systems)
Nmap scan report for 192.168.1.18
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.17 seconds
```

Рис. 3: Список активных хостов.

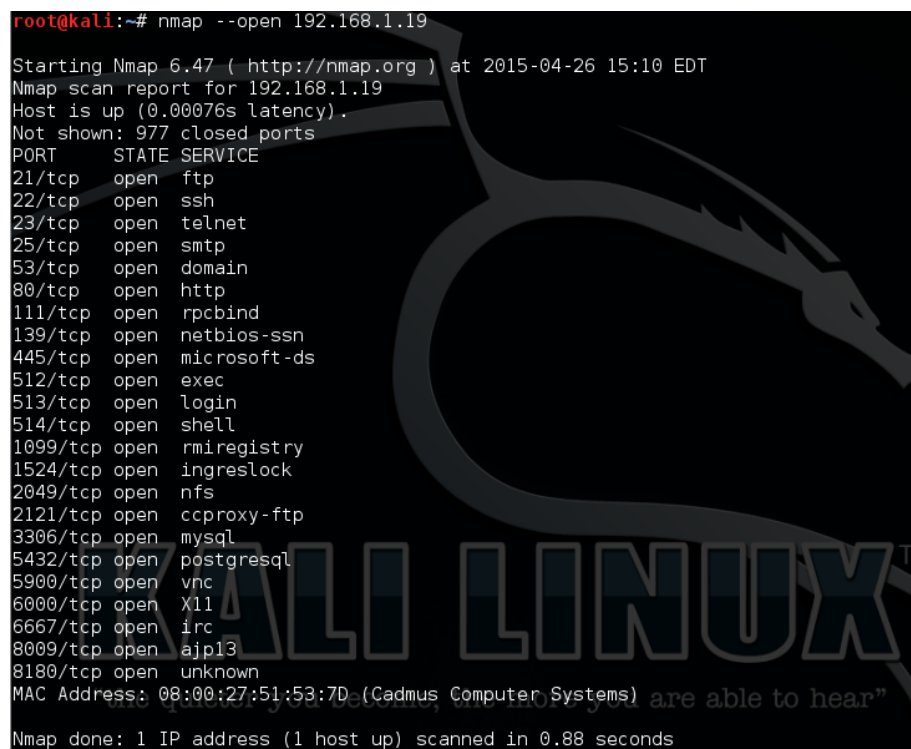
Последние 2 адреса - это адреса виртуальных машин запущенных на данном компьютере. Адрес 192.168.1.19 это адрес metasploitable к которому мы будем обращаться в течении работы.

1.3 Определить открытые порты

Поиск открытых портов осуществляется с помощью следующей команды.

```
nmap -open 192.168.1.19
```

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



```
root@kali:~# nmap --open 192.168.1.19

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-26 15:10 EDT
Nmap scan report for 192.168.1.19
Host is up (0.00076s latency).
Not shown: 977 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
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:51:53:7D (Cadmus Computer Systems) are able to hear"
Nmap done: 1 IP address (1 host up) scanned in 0.88 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 192.158.1.19
```

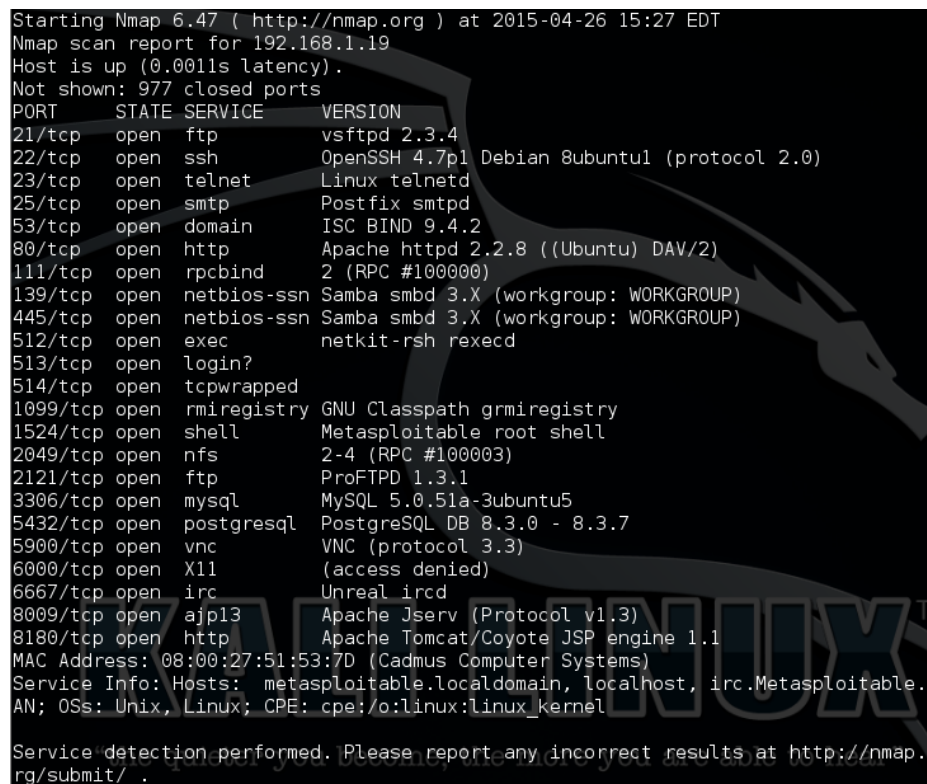
Обработка такого запроса анимает гораздо больше времени, чем предыдущего, так как программа обращается ко всем возможным портам по данному IP адресу.

1.4 Определить версии портов

Отображение версий портов осуществляется следующей командой.

```
nmap -sV 192.168.1.19
```

Результат обработки такого запроса представлен на рисунке 5.



```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-26 15:27 EDT
Nmap scan report for 192.168.1.19
Host is up (0.0011s latency).
Not shown: 977 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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:51:53:7D (Cadmus Computer Systems)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.
AN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.
rg/submit/ .
```

Рис. 5: Список открытых портов с версиями сервисов.

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

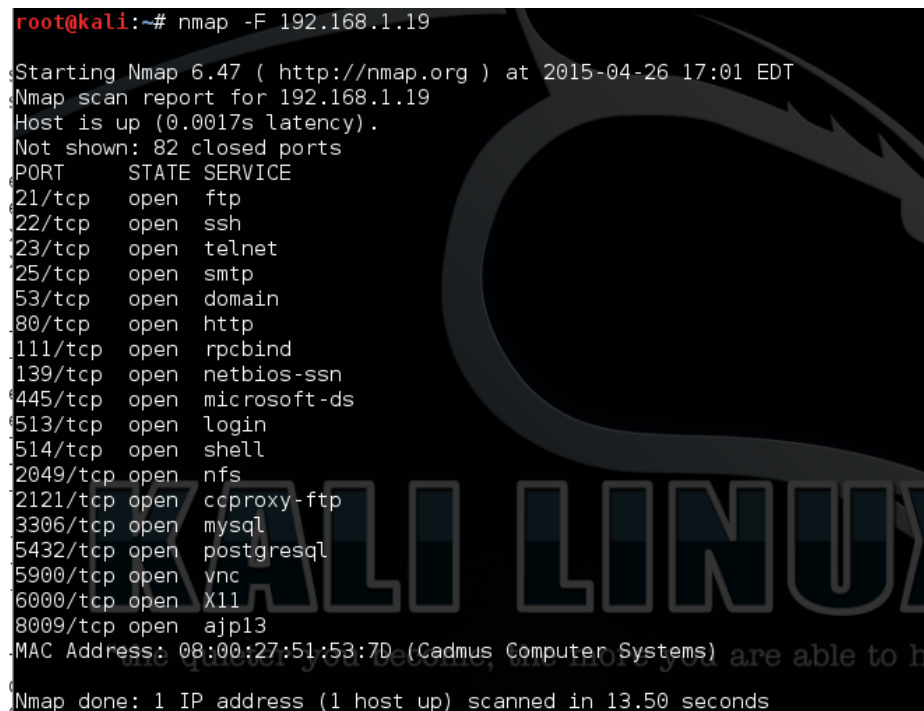
Файл nmap-services содержит набор наиболее часто используемых портов и сервисов на них. Подключение этого файла к процессу сканирования позволяет ускорить обработку команды, так как опрос будет проводиться не по всем 65536 портам а только по тем, которые указаны в файле. Содержимое файла представлено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

```
synoptics-trap 412/udp 0.000511      # Trap Convention Port
smsp 413/tcp 0.000013
smsp 413/udp 0.000395
infoseek 414/tcp 0.000013
infoseek 414/udp 0.000346
bnet 415/tcp 0.000025
bnet 415/udp 0.000445
silverplatter 416/tcp 0.000201
silverplatter 416/udp 0.000675
onmux 417/tcp 0.000226      # Meeting maker
onmux 417/udp 0.000774      # Meeting maker
hyper-g 418/tcp 0.000025
hyper-g 418/udp 0.000544
ariell 419/tcp 0.000138
ariell 419/udp 0.000544
smpte 420/tcp 0.000013
smpte 420/udp 0.000511
ariel2 421/udp 0.000428
ariel3 422/tcp 0.000025
ariel3 422/udp 0.000346
opc-job-start 423/tcp 0.000013      # IBM Operations Planning
opc-job-start 423/udp 0.000000      # IBM Operations Planning
```

Рис. 6: Содержимое файла nmap-services.

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

```
nmap -F 192.168.1.19
```

```
root@kali:~# nmap -F 192.168.1.19
Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-26 17:01 EDT
Nmap scan report for 192.168.1.19
Host is up (0.0017s latency).
Not shown: 82 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
8009/tcp  open  ajp13
MAC Address: 08:00:27:51:53:7D (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 13.50 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.

```
# 4-port GSM-SIP gateway PORTech MV-374
# 2FXS VoIP gateway K-3288W
Fingerprint 2FXS K-3288W or PORTech MV-374 GSM-SIP VoIP adapter
Class 2FXS | embedded || VoIP adapter
Class PORTech | embedded || VoIP adapter
CPE cpe:/h:portech:mv-374
SEQ(SP=0-5%GCD=61A8|C350|124F8|186A0|1E848%ISR=8A-94%TI=I%II=RI%SS=0%TS=U)
OPS(O1=M5B4|WANM5B4T10S%O2=M578|M578W0ST10L%O3=M280|T10NNW5NM280%O4=M5B4|ST1
WIN(W1=0|3180%W2=0|3180%W3=0|3180%W4=0|3180%W5=0|3180%W6=0|3180)
ECN(R=Y%DF=N%T=3B-45%TG=40%W=0%O=WANM5B4SNN%CC=N%Q=R)
T1(R=Y%DF=N%T=3B-45%TG=40%S=0|Z%A=S+%F=AR|AS%RD=0%Q=)
T2(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S%F=AR%O=WANM109T10S%RD=0%Q=)
T3(R=Y%DF=N%T=3B-45%TG=40%W=0%S=Z%A=0%F=AR%O=WANM109T10S%RD=0%Q=)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%Z%F=R%O=WANM109T10S%RD=0%Q=)
T5(R=Y%DF=N%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=WANM109T10S%RD=0%Q=)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%Z%F=R%O=WANM109T10S%RD=0%Q=)
T7(R=Y%DF=N%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=WANM109T10S%RD=0%Q=)
U1(DF=N%T=FA-104%TG=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=S%T=FA-104%TG=FF%CD=S)

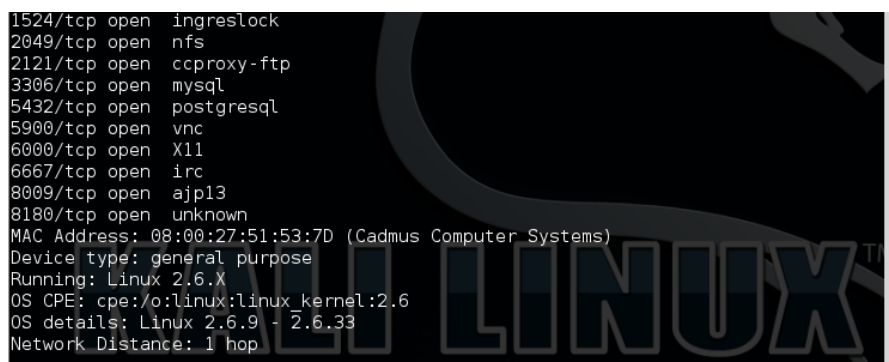
# 2N VOIP doorbell
```

Рис. 8: Содержимое файла nmap-os-db.

Для задеирования этого файла используется опция -O. Команда выглядит так

```
nmap -O 192.168.1.19
```

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



```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:51:53:7D (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
```

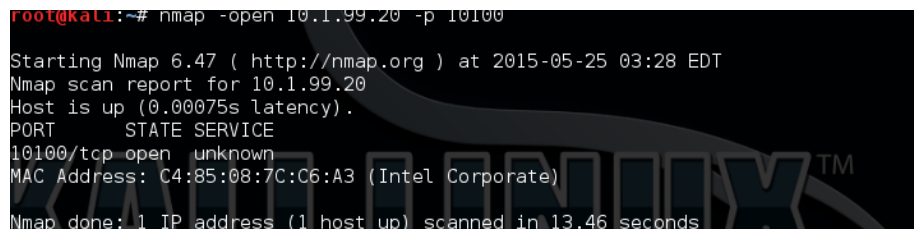
Рис. 9: Дополнительный вывод утилиты.

База данных nmap-service-probes содержит запросы для обращения к различным службам и соответствующие выражения для распознавания и анализа ответов.

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

Для наглядной демонстрации работы файла nmap service probes запустим примитивный TCP сервер на порте 10100.

Просканировав данный порт с помощью nmap мы увидим что его поле сервиса не заполнено.



```
root@kali:~# nmap -open 10.1.99.20 -p 10100
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-25 03:28 EDT
Nmap scan report for 10.1.99.20
Host is up (0.00075s latency).
PORT      STATE SERVICE
10100/tcp  open  unknown
MAC Address: C4:85:08:7C:C6:A3 (Intel Corporate)
Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

Рис. 11: Сканирование порта 10100 без изменения файла.

Теперь отредактируем файл nmap service probes. Добавим в него следующие строки:

```
# This is the NULL probe that just compares any banners given to us
#####NEXT PROBE#####
Probe TCP MYPROBE q|sample text||
ports 10100

match tcp m|^this is my server$| p/my_server/ v/1.0.0/

#####NEXT PROBE#####
```

Рис. 12: Внесенные изменения в файл nmap service probes.

Если построчно то мы делаем следующее:

- создаем новый запрос TCP MYPROBE
- прикрепляем запрос к порту 10100
- в случае если получен ответ "this is my server" то система распознает наш сервер

Теперь запустим утилиту еще раз но уже с обновленным файлом. Как видно, система распознала наш сервер и вместо сервиса unknown теперь указан tcp.

1.7 Сохранить вывод утилиты в XML

Сохранение вывода утилиты в формате xml осуществляется всего командой:

```
nmap -sV -oX -some_output 192.168.1.4
```

```
root@kali:~# nmap -open 192.168.1.4 -p 10100

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-30 10:36 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00s latency).
PORT      STATE SERVICE
10100/tcp  open  tcp
MAC Address: C4:85:08:7C:C6:A3 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

Рис. 13: Обновленный вывод утилиты.

1.8 Исследовать работу nmap с применением WIRESHARK

Проанализируем с помощью wireshark каким путем nmap работает с компьютером.

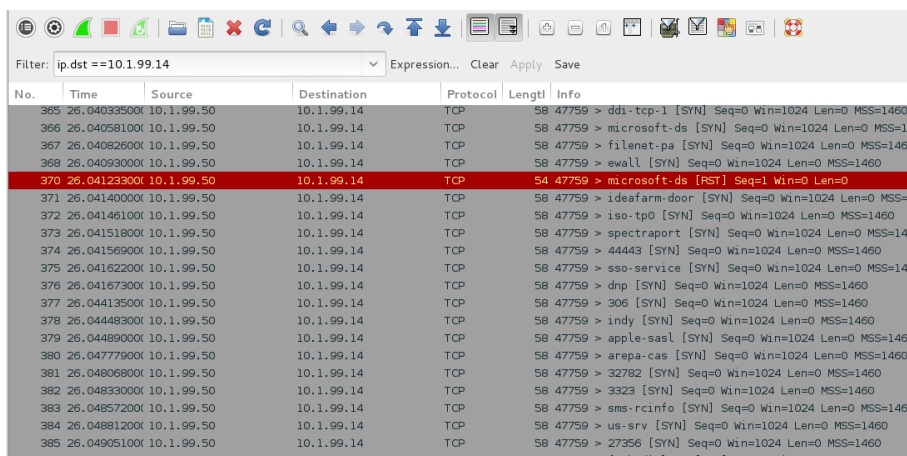


Рис. 14: Демонстрация работы nmap в Wireshark.

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

1.9 Просканировать виртуальную утилиту Metasploitable2 используя db nmap из состава metasploit framework.

Предварительно необходимо включить postgresql и metasploit

```
service postgresql start
service metasploit start
msfconsole
```

```

root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvd.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.

```

Рис. 15: Подключение.

Затем запускаем команду

```
db_nmap -v -sV 192.168.124.211
```

Результат сканирования приведен на рисунке ниже.

1.10 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 приемы работы с nmap, wireshark и metasploit. Nmap является многогранным инструментом для сбора информации о компьютере. Это может стать хорошим подспорьем в подготовке атаки или в анализе слабых мест машины.