Лабораторные работы №4
Курс: Защита информации

Воробьев Олег

5 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 12
1.7 Сохранить вывод утилиты в XML 12
1.8 Исследовать работу nmap с применением WIRESHARK 13

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).

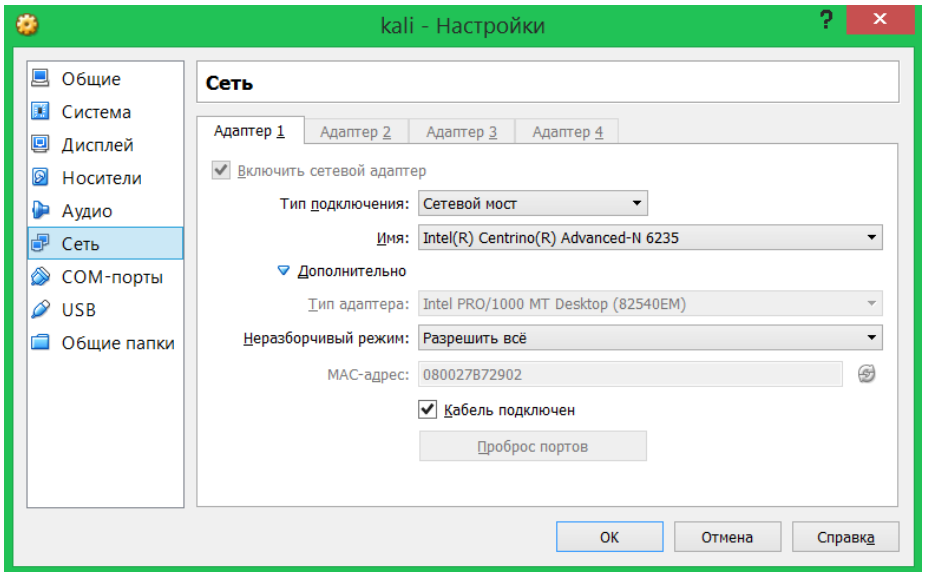

Рис. 1: Настройки сети.

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).

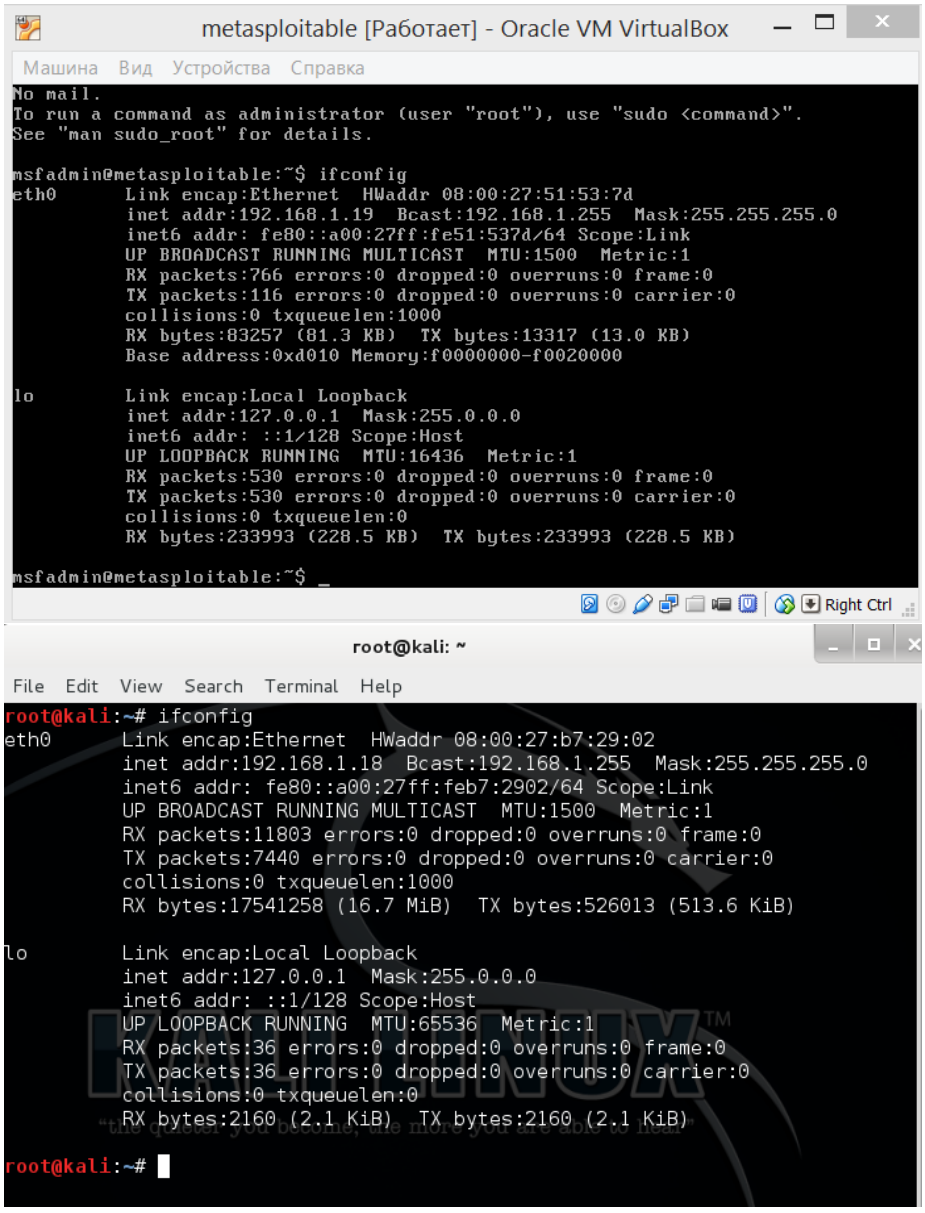

Рис. 2: IP адреса машин.

1.2 Поиск активных портов

Поиск активных хостов осушествляется 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.

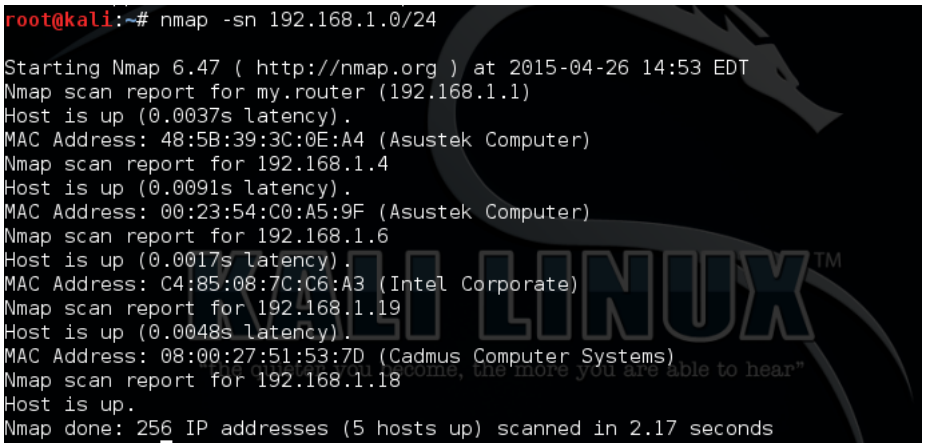

Рис. 3: Список активных хостов.

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 осушествляется 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.

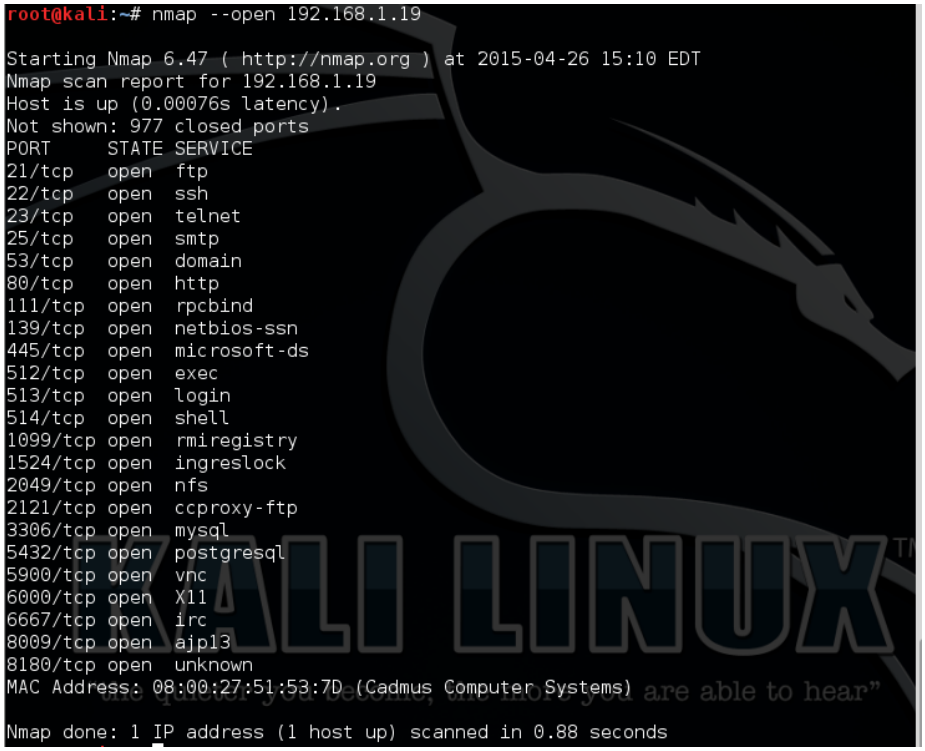

Рис. 4: Список всех открытых портов по данному IP адресу.

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.

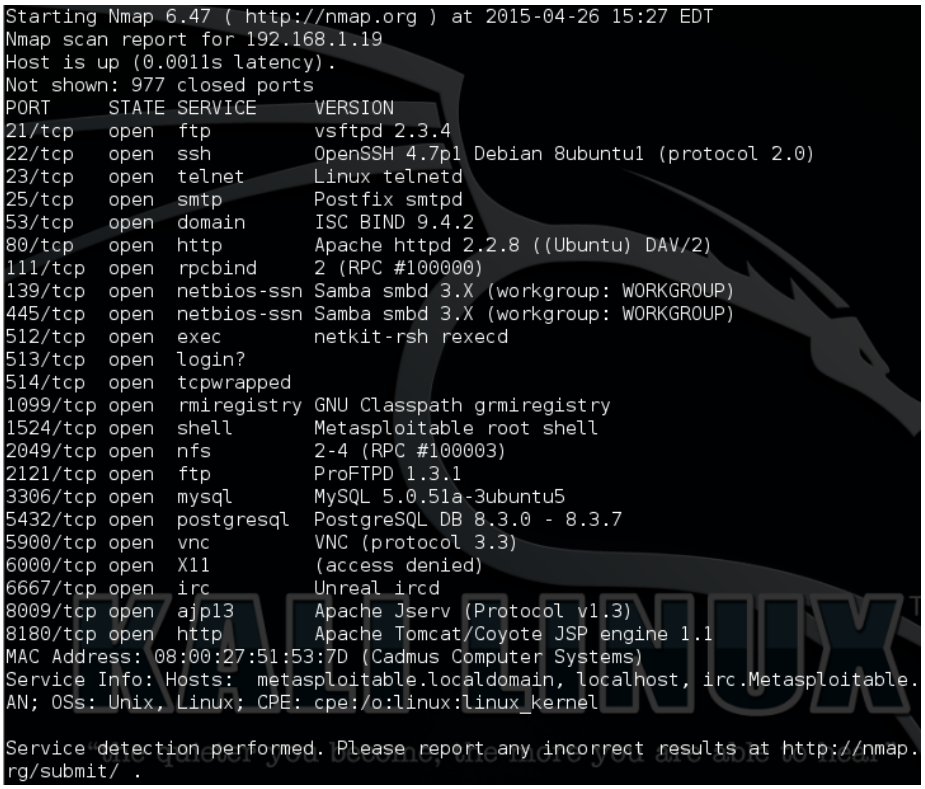

Рис. 5: Список открытых портов с версиями сервисов.

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 потем, 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
ariel1  419/tcp 0.000138
ariel1  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
```

Рис. 6: Содержимое файла nmap-servives.

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

```
nmap -F 192.168.1.19
```

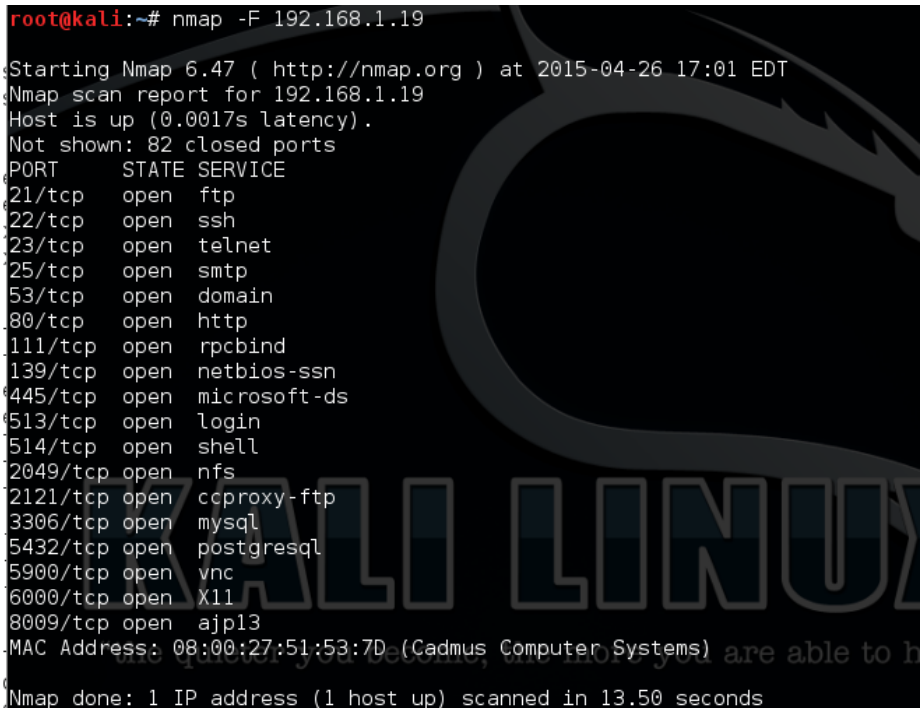

Рис. 7: Результат работы nmap с опцией -F.

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=O%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=O|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=O%F=AR%O=WANM109T10S%RD=0%Q=)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%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%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=WFNM109T10S%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 задействования 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.

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.

```
match amanda m|^220 ([-.\w]+) AMANDA index server \((\d[-.\w ]+)\) ready\.\r\n| p/Amanda backup system
 index server/ v/$2/ o/Unix/ h/$1/
match amanda m|^501 Could not read config file [^!\r\n]+!\r\n220 ([-.\w]+) AMANDA index server \(([-\w
_.]+)\) ready\.\r\n| p/Amanda backup system index server/ v/$2/ i/broken: config file not found/ h/$1/
match amanda m|^ld\.so\.1: amandad: fatal: (libsunmath\.so\.1): open failed: No such file or directory
\n$| p/Amanda backup system index server/ i/broken: $1 not found/

match AndroMouse m|^AMServer$|s p/AndroMouse Android remote mouse server/

match antivir m|^220 Symantec AntiVirus Scan Engine ready\.\r\n| p/Symantec AntiVirus Scan Engine/ cpe
:/a:symantec:antivirus/
match antivir m|^200 NOD32SS ([\d.]+) \((\d+)\)\r\n| p/NOD32 AntiVirus/ v/$1 ($2)/ cpe:/a:eset:nod32_a
ntivirus:$1/

match anyremote m|^Set\(icons,M,6,forward,7,prev,8,stop,9,next,\*,question,0,pause,#,no\);Set\(font,sm
all\);Set\(menu,replace,Playlist,Toggle Shuffle,Toggle Repeat\);Set\(icons,MPD,1,vol_down,2,mute,3,vol
_up,4,rewind,5,play,6,forward,7,prev,8,stop,9,next,\*,question,0,pause,#,no\);Set\(font,small\);Set\(m
enu,replace,Playlist,Toggle Shuffle,Toggle Repeat\);$| p/anyRemote remote control daemon/

match aperio-aaf m|^<aafMessage><aafInitRequest></aafInitRequest></aafMessage>| p/Aperio Algorithm Fra
mework/

match aplus m|^\x01\xff\0\xff\x01\x1d\0\xfd\0\n\x03\x05A\+ API \(([\d.]+)\) - CCS \(([\d.]+)\)\0| p/Cl
eo A+/ i/API $1; CSS $2/
match app m|^\0\x01\0\x08\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\x01\0\0\0\x02$| p/Cisco Application Pe
ering Protocol/ d/load balancer/

# http://www.qosient.com/argus/
match argus m|^\x80\x01\0\x80\0\x80\0\0\xe5az\xcb\0\0\0\0J...............\x02\0\x01\0\0<\x01,.......\0
...\0\0\0\0\x01\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\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\xff\xff\xff\xff\x01\x04\0.\0\x80\x08|s p/Argus netwo
rk analyzer/ v/3.0/

match arkeia m|^\0`\0\x04\0\0\0\x1810\x000\x000\x00852224\0\0\0\0\0\0\0\0\0\0\0$| p/Arkeia Network Bac
kup/
# arkstats (part of arkeia-light 5.1.12 Backup server) on Linux 2.4.20
match arkstats m|^\0`\0\x03\0\0\0\x1810\x000\x000\x00852224\0\0\0\0\0\0\0\0\0\0\0| p/Arkeia arkstats/
                                                                                  73,1           0%
```

Рис. 10: Содержимое файла nmap-service-probes.

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 даный порт с помошью nmap мы увидим что его поле сервиса не заполнено.

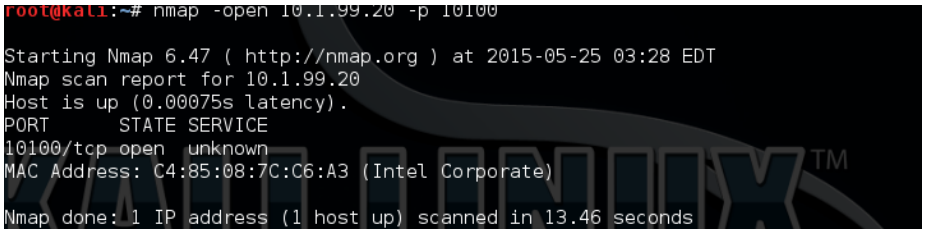

Рис. 11: Сканирование порта 10100 без изменения файла.

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 тереь 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
```

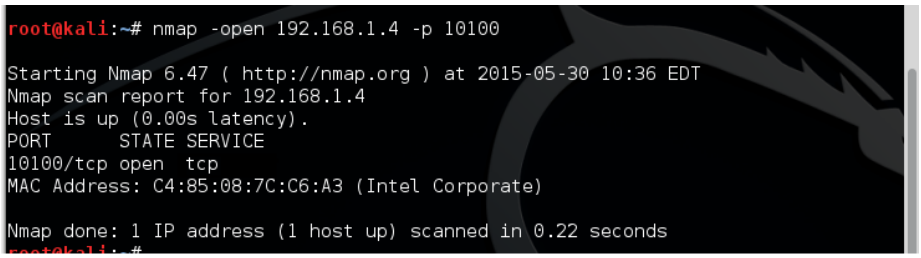

Рис. 13: Обновленный вывод утилиты.

1.8 Исследовать работу nmap с применением WIRESHARK

Проанализируем с помошью wireshark каким путем nmap работает с компьютером.

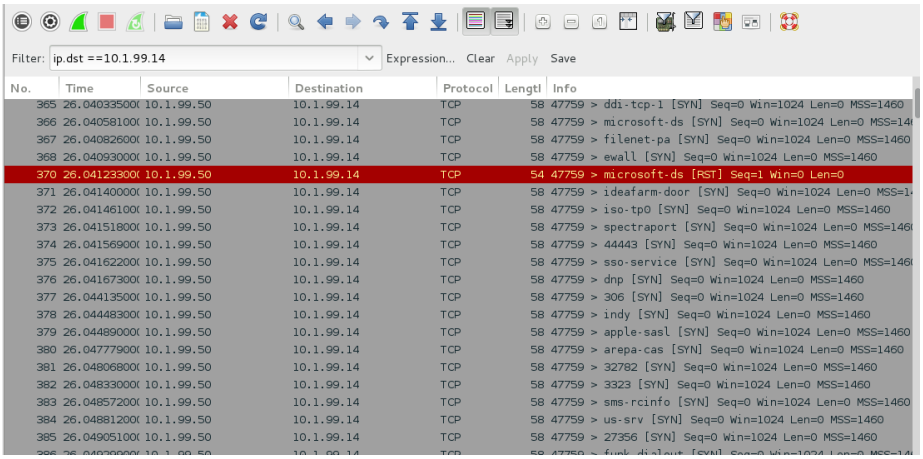

Рис. 14: Демонстрация работы nmap в Wireshark.

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