Санкт-Петербургский Политехнический Университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Методы и средства защиты информации

Отчет по лабораторной работе №2
Утилита для исследования сети и сканер портов Nmap

Работу выполнил:
Косолапов С.А.
Группа: 53501/3
Преподаватель:
Вылегжанина К.Д.

Санкт-Петербург
2016

Содержание

1 Цель работы

Изучить способы и особенности применения утилиты nmap. Определить набор и версии сервисов запущенных на компьютере в диапазоне адресов

2 Программа работы

1. Провести поиск активных хостов
2. Определить открытые порты
3. Определить версии сервисов
4. Изучить файлы nmap-services, nmap-os-db, nmap-service-probes
5. Добавить новую сигнатуру службы в файл nmap-service-probes (для этого создать минимальный tcp server, добиться, чтобы при сканировании nmap указывал для него название и версию)
6. Сохранить вывод утилиты в формате xml
7. Исследовать различные этапы и режимы работы nmap с использованием утилиты Wireshark

Просканировать виртуальную машину Metasploitable2 используя db_nmap из состава metasploit-framework
Выбрать пять записей из файла nmap-service-probes и описать их работу Выбрать один скрипт из состава Nmap и описать его работу

3 Теоретическая информация

Утилита nmap является утилитой с открытым исходным кодом, позволяющей производить сканирование сети и обнаруживать уязвимости в исследуемых узлах (открытые порты). Данная утилита использует "сырые"IP-пакеты нестандартными способами для обнаружения хостов в сети, а так же установленных на них операционных систем, типы пакетных фильтров и брандмауэров, используемые службы и так далее.

4 Ход выполнения работы

В работе используются две сконфигурированные виртуальные машины - Kali Linux 1.0.6 (последняя версия, увы, не заработала в супервизоре) и metasploitable2 в качестве машины для сканирования и поведения атак с ip-адресами 10.0.0.1 и 10.0.0.2 соответственно.

Установка привязка адресов к интерфейсам и проверка производились следующим образом:

```
root@kali:~# ifconfig eth0 10.0.0.1
root@kali:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_req=1 ttl=64 time=4.51 ms
64 bytes from 10.0.0.2: icmp_req=2 ttl=64 time=2.03 ms
64 bytes from 10.0.0.2: icmp_req=3 ttl=64 time=1.17 ms
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 1.172/2.572/4.511/1.415 ms
root@kali:~#
```

4.1 Провести поиск активных хостов

В новых версиях nmap это делается с опцией -sn. В предыдущих версиях Nmap опция -sn выглядит, как -sP.

Вот некоторые другие варианты сканирования:

- -sL - вырожденное сканирование всех подряд хостов, без посылки пакетов хостам
- -sn | -sP - пинг-сканирование
- -Pn - не использовать пинг-сканирование

- -PS <list of ports> - TCP SYN сканирование. Позволяет определить, открыт ли порт (в зависимости от ответа на посланный SYN).
- -PA <list of ports> - TCP ACK сканирование. Позволяет определить существование порта. В ответ прослушиваемый порт будет отдавать RST.
- ...
- -n не производить разрешение DNS имён
- –traceroute - отслеживать путь

```
root@kali:~# nmap -sn 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-19 19:30 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@kali:~#
```

Таким образом, видим, что nmap обнаружил имеющийся хост.

4.2 Определить открытые порты

Такую операцию выполняет утилита без опций, либо можно указать, например, опции -PS или -PA.

```
root@kali:~# nmap 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-19 19:43 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.0023s latency).
Not shown: 979 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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: 08:00:27:67:80:33 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

```
root@kali:~# nmap -PS 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-19 19:44 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.0053s 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: 08:00:27:67:80:33 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
root@kali:~#
```

Результаты в целом совпадают, однако, по непонятным причинам, в первом случае 53 DNS-порт оказался закрыт, а во втором он открылся. При повторе эксперимента с -PS порт указан, как открытый.

4.3 Определить версии сервисов

Это можно сделать с помощью опции -sV.

Результат определения версий:

```
root@kali:~# nmap -sV 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-19 19:58 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.036s 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 rexecd
513/tcp   open  login?
514/tcp   open  shell?
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
1 service unrecognized despite returning data. If you know the service/version, please submit
    ↪ the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port514-TCP:V=6.40%I=7%D=6/19%Time=5766F976%P=i686-pc-linux-gnu%r(NULL,
SF:33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20resolutio
SF:n\n")%r(GetRequest,33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x
SF:20name\x20resolution\n")%r(RPCCheck,33,"\x01getnameinfo:\x20Temporary\x
SF:20failure\x20in\x20name\x20resolution\n")%r(DNSStatusRequest,33,"\x01ge
SF:tnameinfo:\x20Temporary\x20failure\x20in\x20name\x20resolution\n")%r(Ge
SF:nericLines,33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x
SF:20resolution\n")%r(HTTPOptions,33,"\x01getnameinfo:\x20Temporary\x20fai
SF:lure\x20in\x20name\x20resolution\n")%r(kumo-server,33,"\x01getnameinfo:
```

```
SF:\x20Temporary\x20failure\x20in\x20name\x20resolution\n");
MAC Address: 08:00:27:67:80:33 (Cadmus Computer Systems)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix
    ↪ , Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.28 seconds
root@kali:~#
```

Судя по всему, из-за более старой версии nmap, чем metasploitable2, nmap не сумел определить приложение на порте 8180. На этом порте располагается сервис Apache Tomcat.

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

Эти файлы являются служебными и располагаются в директории /usr/share/nmap.

```
root@kali:/usr/share/nmap# ls -l
total 6503
-rw-r--r-- 1 root root   10546 Dec  6  2013 nmap.dtd
-rw-r--r-- 1 root root  455371 Dec  6  2013 nmap-mac-prefixes
-rw-r--r-- 1 root root 3694559 Dec  6  2013 nmap-os-db
-rw-r--r-- 1 root root   11749 Dec  6  2013 nmap-payloads
-rw-r--r-- 1 root root    6631 Dec  6  2013 nmap-protocols
-rw-r--r-- 1 root root   49243 Dec  6  2013 nmap-rpc
-rw-r--r-- 1 root root 1727204 Dec  6  2013 nmap-service-probes
-rw-r--r-- 1 root root  622039 Dec  6  2013 nmap-services
-rw-r--r-- 1 root root   31935 Dec  6  2013 nmap.xsl
drwxr-xr-x 3 root root    1761 Jan  8  2014 nselib
-rw-r--r-- 1 root root   47190 Dec  6  2013 nse_main.lua
drwxr-xr-x 2 root root   12216 Jan  8  2014 scripts
```

4.4.1 Файл nmap-services

Файл содержит описание привязки портов и протоколов к сервисам.

```
root@kali:/usr/share/nmap# head -n 100 nmap-services
# THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT.
# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD.
# Well known service port numbers -*- mode: fundamental; -*-
# From the Nmap Security Scanner ( http://nmap.org )
#
# $Id: nmap-services 31220 2013-07-03 04:30:43Z david $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2011 by Insecure.Com
# LLC.  It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatable open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
# Fields in this file are: Service name, portnum/protocol, open-frequency, optional comments
#
tcpmux  1/tcp 0.001995  # TCP Port Service Multiplexer [rfc-1078]
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]
ftp-data  20/udp  0.001878  # File Transfer [Default Data]
ftp 21/sctp 0.000000  # File Transfer [Control]
ftp 21/tcp  0.197667  # File Transfer [Control]
ftp 21/udp  0.004844  # File Transfer [Control]
ssh 22/sctp 0.000000  # Secure Shell Login
ssh 22/tcp  0.182286  # Secure Shell Login
ssh 22/udp  0.003905  # Secure Shell Login
telnet  23/tcp  0.221265
telnet  23/udp  0.006211
priv-mail 24/tcp  0.001154  # any private mail system
priv-mail 24/udp  0.000329  # any private mail system
smtp  25/tcp  0.131314  # Simple Mail Transfer
smtp  25/udp  0.001285  # Simple Mail Transfer
rsftp 26/tcp  0.007991  # RSFTP
nsw-fe  27/tcp  0.000138  # NSW User System FE
nsw-fe  27/udp  0.000395  # NSW User System FE
unknown 28/tcp  0.000050
msg-icp 29/tcp  0.000025  # MSG ICP
msg-icp 29/udp  0.000560  # MSG ICP
unknown 30/tcp  0.000527
msg-auth  31/tcp  0.000025  # MSG Authentication
msg-auth  31/udp  0.000939  # MSG Authentication
unknown 32/tcp  0.000339
dsp 33/tcp  0.001016  # Display Support Protocol
dsp 33/udp  0.000560  # Display Support Protocol
unknown 34/tcp  0.000025
priv-print  35/tcp  0.000038  # any private printer server
priv-print  35/udp  0.000708  # any private printer server
time  37/tcp  0.003161  # timserver
time  37/udp  0.006458  # timserver
rap 38/tcp  0.000025  # Route Access Protocol
rap 38/udp  0.002043  # Route Access Protocol
rlp 39/udp  0.000478  # Resource Location Protocol
unknown 40/tcp  0.000038
graphics  41/udp  0.000445
nameserver  42/tcp  0.000803  # Host Name Server
nameserver  42/udp  0.005288  # Host Name Server
whois 43/tcp  0.000314  # nicname
whois 43/udp  0.000313  # nicname
```

Как видим, каждая строка файла описана в следующем формате:

```
1 service-name port/protocol
```

Как видим, для большинства сервисов определены различные протоколы и порты.

4.4.2 Файл nmaposdb

Nmap позволяет определить сигнатуры (отпечатки, fingerprints) ответов на запросы к различным протоколам и портам, за счёт чего и производится определение ОС атакуемого. Дело в том, что различные ОС по-разному реализуют многие аспекты таких протоколов, как TCP, UDP, ICMP и т.д. Исходя из того, что, в зависимости от ОС, поля могут быть по-разному заполнены, а время ответа может варьироваться, можно с большой вероятностью установить, какая это операционная система. Правда nmap в случае, если не может по отпечаткам точно идентифицировать систему, не использует вероятностный подход, а пишет, что система не распознана.

Сигнатуры таких параметров как раз и представлены в файле nmap-os-db:

```
root@kali:/usr/share/nmap# head -n 100 nmap-os-db
```

```
# Nmap OS Fingerprinting 2nd Generation DB. -*- mode: fundamental; -*-
# $Id: nmap-os-db 31567 2013-07-29 00:03:01Z david $
#
# Contributions to this database are welcome.  If Nmap obtains a new
# fingerprint (and test conditions are favorable), it will print out a
# URL you can use to submit the fingerprint.  If Nmap guesses wrong,
# please see http://nmap.org/submit/ .
#
# By submitting fingerprints you are transfering any and all copyright
# interest in the data to Insecure.Com LLC so it can modified,
# incorporated into Nmap, relicensed, etc.
#
# This collection of fingerprint data is (C) 1996-2010 by Insecure.Com
# LLC.  It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatable open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
# For a complete description of Nmap OS detection and the format of
# fingerprints in this file, see http://nmap.org/book/osdetect.html.

# This first element provides the number of points every fingerprint
# test is worth.  Tests like TTL or Don't fragment are worth less
# (individually) because there are so many of them and the values are
# often correlated with each other.  Meanwhile, elements such as TS
# (TCP timestamp) which are only used once, get more points.  Points
# are used when there are no perfect matches to determine which OS
# fingerprint matches a target machine most closely.
MatchPoints
SEQ(SP=25%GCD=75%ISR=25%TI=100%CI=50%II=100%SS=80%TS=100)
OPS(O1=20%O2=20%O3=20%O4=20%O5=20%O6=20)
WIN(W1=15%W2=15%W3=15%W4=15%W5=15%W6=15)
ECN(R=100%DF=20%T=15%TG=15%W=15%O=15%CC=100%Q=20)
T1(R=100%DF=20%T=15%TG=15%S=20%A=20%F=30%RD=20%Q=20)
T2(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T3(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T4(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T5(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T6(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T7(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
U1(R=50%DF=20%T=15%TG=15%IPL=100%UN=100%RIPL=100%RID=100%RIPCK=100%RUCK=100%RUD=100)
IE(R=50%DFI=40%T=15%TG=15%CD=100)

# 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|ST10WAL%O5=M218|
    ↪ M218ST10WAL%O6=M109|M109ST10)
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
Fingerprint 2N Helios IP VoIP doorbell
Class 2N | embedded || specialized
CPE cpe:/h:2n:helios
SEQ(SP=0-5%GCD=51E80C|A3D018|F5B824|147A030|199883C%ISR=C8-D2%TI=I|RD%CI=I%II=RI%SS=S%TS=U)
OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)
WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)
```

```
ECN(R=Y%DF=N%T=FA-104%TG=FF%W=8000%O=M5B4%CC=N%Q=)
T1(R=Y%DF=N%T=FA-104%TG=FF%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=N%T=FA-104%TG=FF%W=8000%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)
T4(R=Y%DF=N%T=FA-104%TG=FF%W=8000%S=A+%A=S%F=AR%O=%RD=0%Q=)
T5(R=Y%DF=N%T=FA-104%TG=FF%W=8000%S=A%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=N%T=FA-104%TG=FF%W=8000%S=A%A=S%F=AR%O=%RD=0%Q=)
T7(R=Y%DF=N%T=FA-104%TG=FF%W=8000%S=A%A=S+%F=AR%O=%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)

# BT2700HGV DSL Router version 5.29.107.19
Fingerprint 2Wire BT2700HG-V ADSL modem
Class 2Wire | embedded || broadband router
CPE cpe:/h:2wire:bt2700hg-v
SEQ(SP=6A-BE%GCD=1-6%ISR=96-A0%TI=I%CI=I%II=I%SS=S%TS=A)
OPS(O1=M5B4NNSW0NNNT11%O2=M578NNSW0NNNT11%O3=M280W0NNNT11%O4=M218NNSW0NNNT11%O5=
    ↪ M218NNSW0NNNT11%O6=M109NNSNNT11)
WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)
ECN(R=Y%DF=Y%T=FA-104%TG=FF%W=8000%O=M5B4NNSW0N%CC=N%Q=)
T1(R=Y%DF=Y%T=FA-104%TG=FF%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=FA-104%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=E44A4E43%Q=)
T5(R=Y%DF=Y%T=FA-104%TG=FF%W=0%S=Z%A=S+%F=AR%O=%RD=1F59B3D4%Q=)
T6(R=Y%DF=Y%T=FA-104%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=1F59B3D4%Q=)
```

Проверить ОС атакуемого можно следующим образом:

```
root@kali:/usr/share/nmap# nmap -O -sn 10.0.0.2
WARNING: OS Scan is unreliable without a port scan. You need to use a scan type along with it
    ↪ , such as -sS, -sT, -sF, etc instead of -sn
QUITTING!
root@kali:/usr/share/nmap# nmap -O 10.0.0.2

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-20 05:26 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.0011s 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: 08:00:27:67:80:33 (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

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
root@kali:/usr/share/nmap#
```

Первый эксперимент показывает, что при запрете сканирования портов нет никакой возможности установить тип и версию ОС. Дальнейший эксперимент показывает, что metasploitable2 построена на

ядре Linux 2.6.x. Знание типа и версии ОС является одним из фундаментов для построения атаки.

4.4.3 Файл nmap-service-probes

При сканировании, в первую очередь, nmap полагается на информацию, описанную в файле nmap-services, где описано стандартное использование портов. Вместе с тем, вполне возможно, что назначение стандартного порта было переопределено, что, казалось бы, может добавить сложности при проведении атаки. Однако nmap анализирует также и отклик служб на описанные запросы. Как раз такие описания и содержит в себе файл nmapserviceprobes. Вот некоторые директивы, которые можно описать в этом файле:

- probe

  ```
  Probe <protocol> <probename> <probestring>
  ```

  Описывает строку, которую nmap будет посылать атакуемому серверу.

- match

  ```
  match <service> <pattern> [<versioninfo>]
  ```

  Позволяет описать, как распознать ответ атакуемого сервера на посылку, описанную в probe, на основе чего можно сделать заключение о том, что это за сервис и его версии.

- ports и sslports

  ```
  ports <portlist>
  ```

  Позволяет определить, какие порты обычно обнаруживаются. Строка ports/sslports должна быть одна на каждую probe-секцию.

- exclude

  ```
  Exclude <port specification>
  ```

  Директива исключает порты из сканирования версий.

```
root@kali:/usr/share/nmap# head nmap-service-probes -n 100
# Nmap service detection probe list -*- mode: fundamental; -*-
# $Id: nmap-service-probes 31402 2013-07-18 03:38:37Z david $
#
# This is a database of custom probes and expected responses that the
# Nmap Security Scanner ( http://nmap.org ) uses to
# identify what services (eg http, smtp, dns, etc.) are listening on
# open ports.  Contributions to this database are welcome.  We hope to
# create an automated submission system (as with OS fingerprints), but
# for now you can email fyodor any new probes you develop so that he
# can include them in the main Nmap distributon.  By sending new
# probe/matches to Fyodor or one the insecure.org development mailing
# lists, it is assumed that you are transfering any and all copyright
# interest in the data to Fyodor so that he can modify it, relicense
# it, incorporate it into programs, etc. This is important because the
# inability to relicense code has caused devastating problems for
# other Free Software projects (such as KDE and NASM).  Nmap will
# always be available Open Source.  If you wish to specify special
# license conditions of your contributions, just say so when you send
# them.
#
# This collection of probe data is (C) 1998-2010 by Insecure.Com
# LLC.  It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatable open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
```

```
# For details on how Nmap version detection works, why it was added,
# the grammar of this file, and how to detect and contribute new
# services, see http://nmap.org/book/vscan.html.

# The Exclude directive takes a comma separated list of ports.
# The format is exactly the same as the -p switch.
Exclude T:9100-9107

# This is the NULL probe that just compares any banners given to us
##############################NEXT PROBE##############################
Probe TCP NULL q||
# Wait for at least 6 seconds for data.  It used to be 5, but some
# smtp services have lately been instituting an artificial pause (see
# FEATURE('greet_pause') in Sendmail, for example)
totalwaitms 6000

match 1c-server m|^S\xf5\xc6\x1a{| 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\0\0\0\0
    ↪ $|s 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\x1b\0\0\0\0\0\0\0acarsd\t([\w._-]+)\tAPI-([\w._-]+)\)\0\0\0\x06\x05
    ↪ \0\0\0\0\0\0<\?xml | p/acarsd/ v/$1/ i/API $2/ cpe:/a:acarsd:$1/
match acmp m|^ACMP Server Version ([\w._-]+)\r\n| p/Aagon ACMP Inventory/ v/$1/
match activemq m|^\0\0\0.\x01ActiveMQ\0\0\0|s p/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|^.\0\x01\0[^\0]\0[^\0]\0[^\0]\0[^\0]\0[^\0]\0.*\0\0\0$|s p/Microsoft
    ↪ ActiveSync/ o/Windows/ cpe:/a:microsoft:activesync/ cpe:/o:microsoft:windows/a
match activesync m|^\(\0\0\0\x02\0\0\0\x03\0\0\0\+\0\0\x003\0\0\0\0\0\0\0\x04\0\0`\x01\0\0\xff
    ↪ \0\0\0\0\0\0\0\0\0\0\0$|s 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/

match adobe-crossdomain m|^<cross-domain-policy><allow-access-from domain='([^']*)' to-ports
    ↪ ='([^']*)' /></cross-domain-policy>\0$| p/Adobe cross-domain policy/ i/domain: $1; ports
    ↪ : $2/
# Missing trailing \0? Was like that in the submission.
match adobe-crossdomain m|^<cross-domain-policy><allow-access-from domain=\"([^\"]*)\"␣to-
    ↪ ports=\"([^\"]*)\"/></cross-domain-policy>$| p/Adobe cross-domain policy/ i/domain: $1;
    ↪ ports: $2/

match afsmain m|^\+Welcome to Ability FTP Server \(Admin\)\. \[20500\]\r\n| p/Code-Crafters
    ↪ Ability FTP Server afsmain admin/ o/Windows/ cpe:/o:microsoft:windows/a

match altiris-agent m|^<\0r\0e\0s\0p\0o\0n\0s\0e\0>\0C\0o\0n\0n\0e\0c\0t\0e\0d\0 \0t\0o\0 [\0\
    ↪ d.]*<\0/\0r\0e\0s\0p\0o\0n\0s\0e\0>\0$| p/Altiris remote monitoring agent/

# AMANDA index server 2.4.2p2 on Linux 2.4
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 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_antivirus:$1/

match anyremote m|^Set\(icons,M,6,forward,7,prev,8,stop,9,next,\*,question,0,pause,#,no\);Set
    ↪ \(font,small\);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\(menu,replace,Playlist,Toggle Shuffle,Toggle
    ↪ Repeat\);$| p/anyRemote remote control daemon/

match aperio-aaf m|^<aafMessage><aafInitRequest></aafInitRequest></aafMessage>| p/Aperio
    ↪ Algorithm Framework/
```

```
match aplus m|^\x01\xff\0\xff\x01\x1d\0\xfd\0\n\x03\x05A\+ API \(([\d.]+)\) - CCS \(([\d.]+)\)
    ↪ \0| p/Cleo A+/ i/API $1; CSS $2/
match app m|^\0\x01\0\x08\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\x01\0\0\0\x02$| p/Cisco
    ↪ Application Peering 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\
    ↪ xff\xff\xff\xff\x01\x04\0.\0\x80\x08|s p/Argus network 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$| p/Arkeia
    ↪ Network Backup/
# 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| p/Arkeia
    ↪ arkstats/
match artsd m|^MCOP\0\0\0.\0\0\0\x01\0\0\0\x10aRts/MCOP-([\d.]+)\0\0\0\0|s p/artsd/ i/MCOP $1/

# Asterisk call manager - port 5038
match asterisk m|^Asterisk Call Manager/([\d.]+)\r\n| p/Asterisk Call Manager/ v/$1/ cpe:/a:
    ↪ digium:asterisk:$1/
match asterisk-proxy m|^Response: Follows\r\nPrivilege: Command\r\n--END COMMAND--\r\n| p/
    ↪ Asterisk Call Manager Proxy/ cpe:/a:digium:asterisk/

match audit m|^Visionsoft Audit on Demand Service\r\nVersion: ([\d.]+)\r\n\r\n| p/Visionsoft
    ↪ Audit on Demand Service/ v/$1/ o/Windows/ cpe:/o:microsoft:windows/a
match autosys m|^([\w._-]+)\nListener for [\w._-]+ AutoSysAdapter\nEOS\nExit Code = 1001\nIP
    ↪ <[\d.]+> is not authorized for this request\. Please contact your Web Administrator\.\
    ↪ nEOS\n| p/CA AutoSys RCS Listener/ v/$1/ i/not authorized/
root@kali:/usr/share/nmap#
```

4.5 Добавить новую сигнатуру службы в файл nmap-service-probes (для этого создать минимальный tcp server, добиться, чтобы при сканировании nmap указывал для него название и версию)

Для исследования использовался простейший сервер:

```c
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <stdio.h>

#include <string.h>

#define BUFFER_SIZE 255

int main() {
  char buffer[BUFFER_SIZE];
  char *rec_srt="Greeting (SomeServer 2.4)\n";

  int listen_fd, comm_fd;
  struct sockaddr_in servaddr;

  listen_fd = socket(AF_INET, SOCK_STREAM, 0);

  bzero(&servaddr, sizeof(servaddr));

  servaddr.sin_family = AF_INET;
  servaddr.sin_addr.s_addr = htons(INADDR_ANY);
  servaddr.sin_port = htons(10000);

  bind(listen_fd, (struct sockaddr *) &servaddr, sizeof(servaddr));

  listen(listen_fd, 10);

  comm_fd = accept(listen_fd, (struct sockaddr*) NULL, NULL);

  while(1) {
    bzero(buffer, BUFFER_SIZE);
    read(comm_fd,buffer, BUFFER_SIZE);
    printf("You wrote: %s", buffer);
    write(comm_fd, rec_srt, strlen(rec_srt)+1);
  }
}
```

Листинг 1: Код сервера

Для того, чтобы сервис определился, необходимо прописать в файле nmap-service-probes информацию, позволяющую его идентифицировать. В регулярном выражении в директиве match необходимо специфицировать ответ сервера, в котором можно выделить версию.

```
Exclude T:9100-9106

Probe TCP SomeServer q|x02Hi|
rarity 1
ports 9107
match someServer m/^Greeting \((\w*) ([\d.]*)\)/ p/$1/ v/$2/
```

В результате, можем идентифицировать работающий на сканируемой машине сервер:

```
root@kali:~# nmap 10.0.0.2 -p 9107 -sV

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-20 07:53 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.0017s latency).
PORT     STATE SERVICE    VERSION
9107/tcp open  someServer SomeServer 2.4
MAC Address: 08:00:27:67:80:33 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds
```

4.6 Сохранить вывод утилиты в формате xml

Вывод в xml осуществляется с помощью опции -X, в сочетании с которой можно вывести в файл. Ниже представлен пример вызова nmap с сохранением в xml.

```
root@kali:~/Desktop# nmap 10.0.0.2 -sV -p 1-2000 -oX output.xml

Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-20 08:10 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
    ↪ system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.2
Host is up (0.0011s latency).
Not shown: 1986 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 rexecd
513/tcp  open  login
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
1 service unrecognized despite returning data. If you know the service/version, please submit
    ↪ the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port514-TCP:V=6.40%I=7%D=6/20%Time=5767A507%P=i686-pc-linux-gnu%r(NULL,
SF:33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20resolutio
SF:n\n");
MAC Address: 08:00:27:67:80:33 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost; OSs: Unix, Linux; CPE: cpe:/o:
    ↪ linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
```

Вывод будет осуществлён в файл output.xml:

```
<?xml version="1.0"?>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
```

```
<!-- Nmap 6.40 scan initiated Mon Jun 20 08:10:44 2016 as: nmap -sV -p 1-2000 -oX output.xml 10.0.0.2 -->
<nmaprun scanner="nmap" args="nmap -sV -p 1-2000 -oX output.xml 10.0.0.2" start="1466410244" startstr="Mon Jun 20 08:10:44 2016" version="6.40" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="2000" services="1-2000"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1466410244" endtime="1466410258"><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="10.0.0.2" addrtype="ipv4"/>
<address addr="08:00:27:67:80:33" addrtype="mac" vendor="Cadmus Computer Systems"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="1986">
<extrareasons reason="resets" count="1986"/>
</extraports>
<port protocol="tcp" portid="21"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ftp" product="vsftpd" version="2.3.4" ostype="Unix" method="probed" conf="10"><cpe>cpe:/a:vsftpd:vsftpd:2.3.4</cpe></service></port>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" product="OpenSSH" version="4.7p1 Debian 8ubuntu1" extrainfo="protocol 2.0" ostype="Linux" method="probed" conf="10"><cpe>cpe:/a:openbsd:openssh:4.7p1</cpe><cpe>cpe:/o:linux:linux_kernel</cpe></service></port>
<port protocol="tcp" portid="23"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="telnet" product="Linux telnetd" ostype="Linux" method="probed" conf="10"><cpe>cpe:/o:linux:linux_kernel</cpe></service></port>
<port protocol="tcp" portid="25"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="smtp" product="Postfix smtpd" hostname="metasploitable.localdomain" method="probed" conf="10"><cpe>cpe:/a:postfix:postfix</cpe></service></port>
<port protocol="tcp" portid="53"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="domain" product="ISC BIND" version="9.4.2" method="probed" conf="10"><cpe>cpe:/a:isc:bind:9.4.2</cpe></service></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" product="Apache httpd" version="2.2.8" extrainfo="(Ubuntu) DAV/2" method="probed" conf="10"><cpe>cpe:/a:apache:http_server:2.2.8</cpe></service></port>
<port protocol="tcp" portid="111"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="rpcbind" version="2" extrainfo="RPC #100000" method="probed" conf="10"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="netbios-ssn" product="Samba smbd" version="3.X" extrainfo="workgroup: WORKGROUP" method="probed" conf="10"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="netbios-ssn" product="Samba smbd" version="3.X" extrainfo="workgroup: WORKGROUP" method="probed" conf="10"/></port>
<port protocol="tcp" portid="512"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="exec" product="netkit-rsh rexecd" ostype="Linux" method="probed" conf="10"><cpe>cpe:/o:linux:linux_kernel</cpe></service></port>
<port protocol="tcp" portid="513"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="login" method="probed" conf="10"/></port>
<port protocol="tcp" portid="514"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="shell" servicefp="SF-Port514-TCP:V=6.40%I=7%D=6/20%Time=5767A507%P=i686-pc-linux-gnu%r(NULL,33,&quot;\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20resolution\n&quot;);" method="table" conf="3"/></port>
<port protocol="tcp" portid="1099"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="rmiregistry" product="GNU Classpath grmiregistry" hostname="localhost" method="probed" conf="10"/></port>
<port protocol="tcp" portid="1524"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="shell" product="Metasploitable root shell" method="probed" conf="10"/></port>
</ports>
<times srtt="1132" rttvar="545" to="100000"/>
</host>
<runstats><finished time="1466410258" timestr="Mon Jun 20 08:10:58 2016" elapsed="14.37" summary="Nmap done at Mon Jun 20 08:10:58 2016; 1 IP address (1 host up) scanned in 14.37 seconds" exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun>
```

Листинг 2: Выходной xml-файл

4.7 Исследовать различные этапы и режимы работы nmap с использованием утилиты Wireshark

При анализе metasploitable2 с помощью nmap без параметров (кроме адреса) суммарно уходят и приходят порядка 2000 пакетов.

Изначально для сервисов на сканируемой машине посылаются TCP SYN-запросы. Они составляют подавляющее количество исходящих пакетов. Также среди исходящих встречаются TCP RST-пакеты - для тех сервисов, которые ответили на SYN-запросы. Таких посылок 23. Однако определённых сервисов - 22. Таким образом, один сервис, судя по всему, не проходит дополнительную фильтрацию.

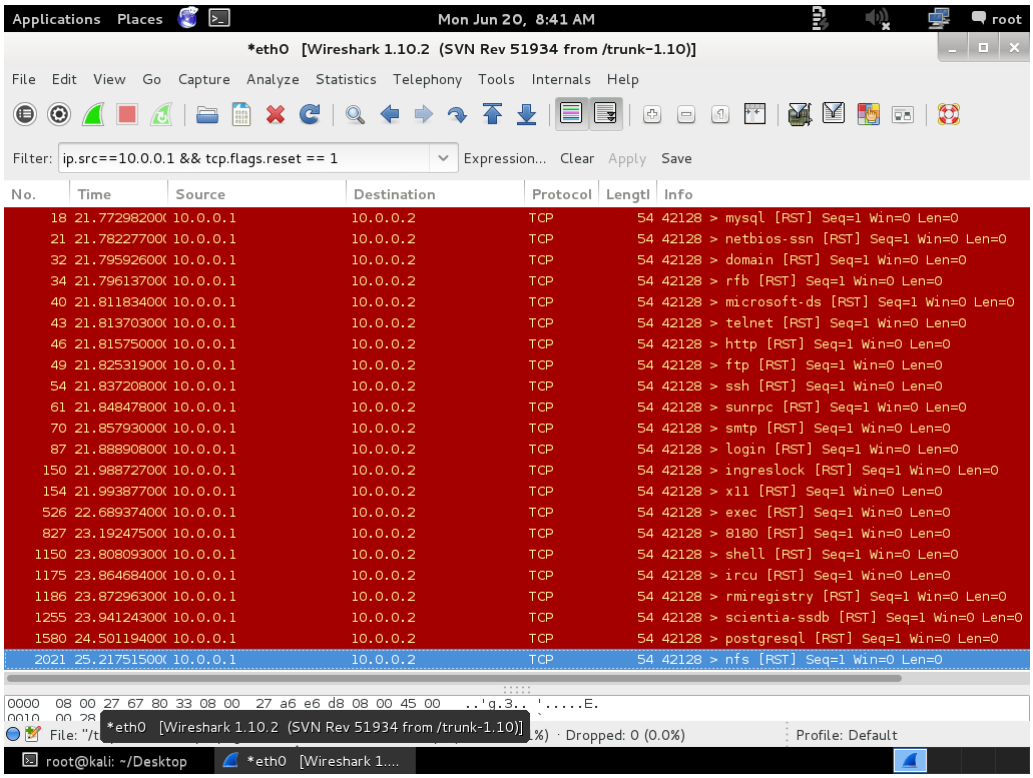

Рис. 1: Демонстрация исходящих RST-пакетов

В случае, если всё хорошо и порт прослушивается, в ответ приходит пакет с флагами (SYN, ACK), в ответ на который посылается RST:

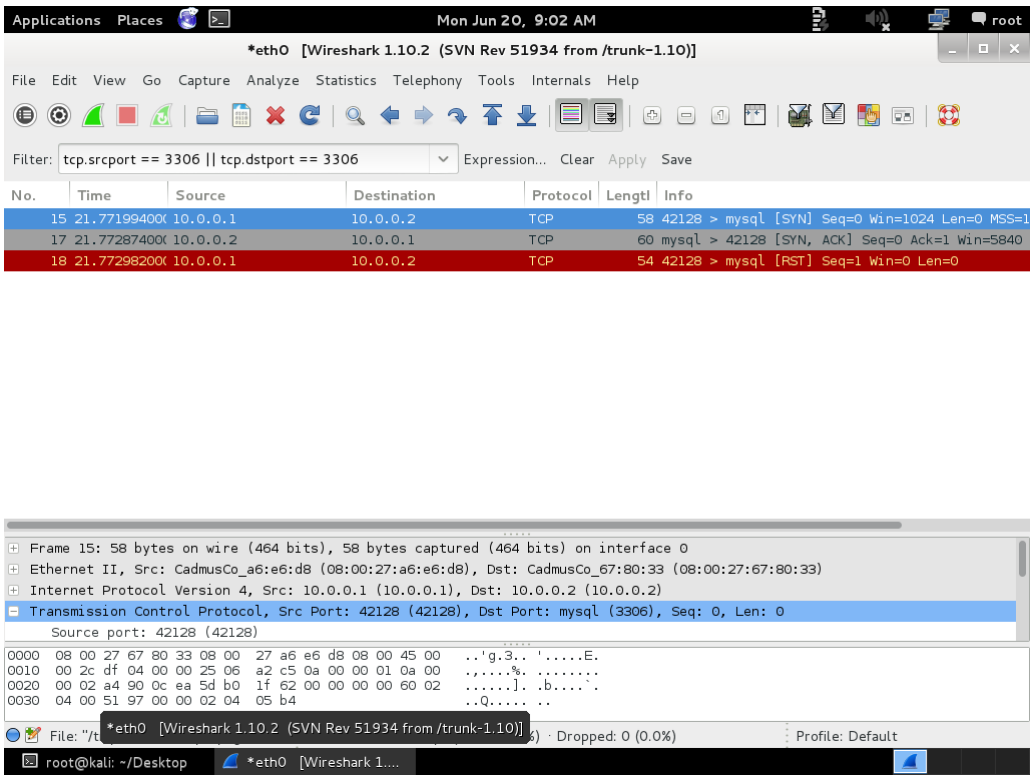

Рис. 2: Демонстрация определения прослушиваемого порта

В случае же, если порт не прослушивается сервисами на стороне сканируемой машины, в ответ приходит пакет с флагами (RST, ACK).

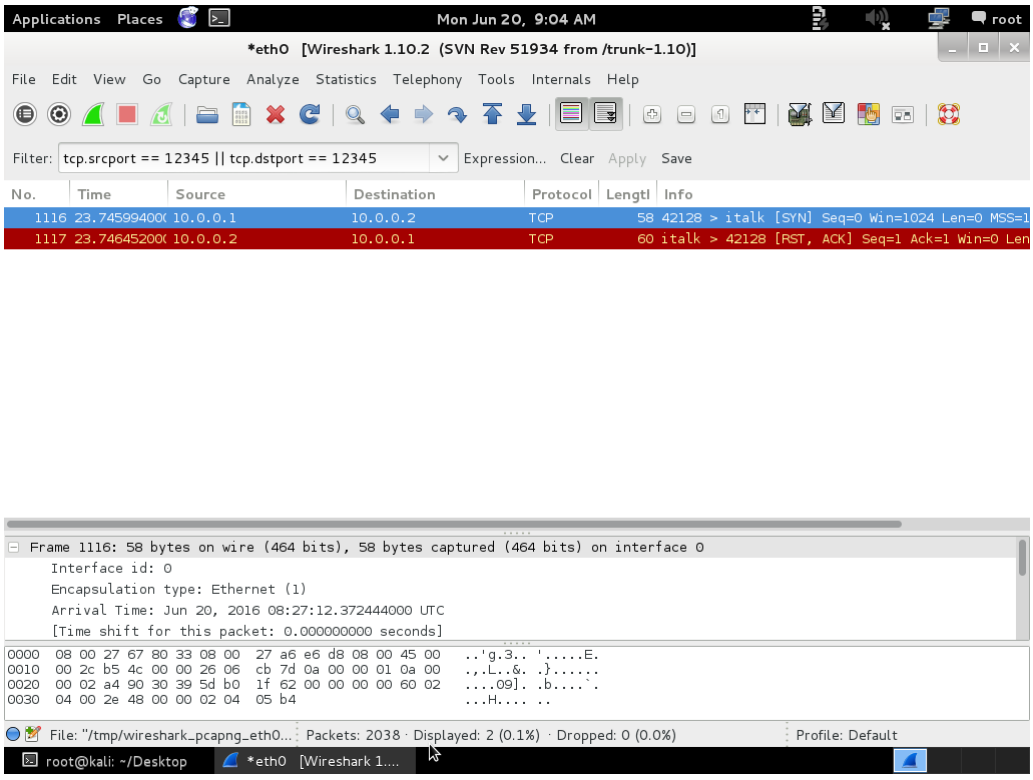

Рис. 3: Демонстрация определения непрослушиваемого порта

4.8 Просканировать виртуальную машину Metasploitable2 используя db_nmap из состава metasploit-framework

Начальным этапом служит настройка фреймворка. До Kali2.0 использовался Metasploit вместо metasploit framework, и детали настройки несколько отличаются. В частности, отсутствует утилита msfdb, с помощью которой производится инициализация базы данных в последующих релизах. Инициализация производится при старте msfconsole.

```
root@kali:~# /etc/init.d/postgresql start
[....] Starting PostgreSQL 9.1 database server: main
. ok
root@kali:~# service metasploit start
Configuring Metasploit...
Creating metasploit database user 'msf3'...
Creating metasploit database 'msf3'...
insserv: warning: current start runlevel(s) (empty) of script `metasploit' overrides LSB
    ↪ defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `metasploit' overrides
    ↪ LSB defaults (0 1 6).
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~# msfconsole
NOTICE:  CREATE TABLE will create implicit sequence "hosts_id_seq" for serial column "hosts.id
    ↪ "
<...>
NOTICE:  CREATE TABLE / PRIMARY KEY will create implicit index "task_sessions_pkey" for table
    ↪ "task_sessions"
[*] The initial module cache will be built in the background, this can take 2-5 minutes...

 _
/ \     /\          __                                  _    __   /_/ __
| |\   / | _____    \ \                ___    _____  | |  /  \  _    \ \
| | \/| | | ___\ |- -|    /\     /  __\  | -__/  |  || |  || | |- -|
|_|   | | | _|__   | |_   / -\ __\ \     | |     | | \__/| |   | |_
      |/  |_____/  \___\/ /\ \\___/    \/      \__|     |_\   \___\


Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops
msf >
```

Далее можно сделать сканирование с помощью nmap, но уже внутри msfconsole. В данном случае результат совпадает с представленным выше.

```
msf > db_nmap 10.0.0.2
[*] Nmap: Starting Nmap 6.40 ( http://nmap.org ) at 2016-06-20 09:45 UTC
[*] Nmap: 'mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
    ↪ Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: Nmap scan report for 10.0.0.2
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 978 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 21/tcp   open  ftp
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 23/tcp   open  telnet
[*] Nmap: 25/tcp   open  smtp
[*] Nmap: 53/tcp   open  domain
[*] Nmap: 80/tcp   open  http
[*] Nmap: 111/tcp  open  rpcbind
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 512/tcp  open  exec
[*] Nmap: 513/tcp  open  login
[*] Nmap: 514/tcp  open  shell
[*] Nmap: 1099/tcp open  rmiregistry
[*] Nmap: 1524/tcp open  ingreslock
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 2121/tcp open  ccproxy-ftp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: 6000/tcp open  X11
```

```
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8180/tcp open  unknown
[*] Nmap: MAC Address: 08:00:27:67:80:33 (Cadmus Computer Systems)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 5.15 seconds
msf >
```

4.9 Выбрать один скрипт из состава Nmap и описать его работу

Nmap поддерживает скрипты, описанные на языке Lua (в рамках NSE - nmap scripting engine). Найти скрипты можно по адресу: https://nmap.org/nsedoc/.

Был взят один из размещённых там скриптов.

Главной функцией в скриптах является функция action(host, port). Перед ней следуют блоки description, присваиваются значения переменным author, license, categories (категории, к которым можно определить скрипт). Ниже представлен вариант скрипта, реализующий вывод информации о формате amqp, используемого в RabbitMQ.

```
1  local amqp = require "amqp"
2  local nmap = require "nmap"
3  local shortport = require "shortport"
4  local stdnse = require "stdnse"
5
6  description = [[
7  Gathers information (a list of all server properties) from an AMQP (advanced message queuing
       ↪ protocol) server.
8
9  See http://www.rabbitmq.com/extensions.html for details on the
10 <code>server-properties</code> field.
11 ]]
12
13 ---
14 -- @usage
15 -- nmap --script amqp-info -p5672 <target>
16 ---
17 -- @args amqp.version Can be used to specify the client version to use (currently, 0-8, 0-9 or
       ↪ 0-9-1)
18 --
19 -- @output
20 -- 5672/tcp open  amqp
21 -- | amqp-info:
22 -- |   capabilities:
23 -- |     publisher_confirms: YES
24 -- |     exchange_exchange_bindings: YES
25 -- |     basic.nack: YES
26 -- |     consumer_cancel_notify: YES
27 -- |   copyright: Copyright (C) 2007-2011 VMware, Inc.
28 -- |   information: Licensed under the MPL.  See http://www.rabbitmq.com/
29 -- |   platform: Erlang/OTP
30 -- |   product: RabbitMQ
31 -- |   version: 2.4.0
32 -- |   mechanisms: PLAIN AMQPLAIN
33 -- |_  locales: en_US
34
35 author = "Sebastian Dragomir"
36
37 license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
38
39 categories = {"default", "discovery", "safe", "version"}
40
41
42 portrule = shortport.version_port_or_service(5672, "amqp", "tcp", "open")
43
44 action = function(host, port)
45   -- создаём новый клиент
46   local cli = amqp.AMQP:new( host, port )
47
48   -- подключаем клиент и проверяем корректность подключения
49   local status, data = cli:connect()
50   if not status then return "Unable to open connection: " .. data end
51
52   -- пытаемся осуществить handshake
53   status, data = cli:handshake()
54   if not status then return data end
55
```

```
56    -- разрываем соединение
57    cli:disconnect()
58
59    -- записываем характеристики в порт
60    port.version.name = "amqp"
61    port.version.product = cli:getServerProduct()
62    port.version.extrainfo = cli:getProtocolVersion()
63    port.version.version = cli:getServerVersion()
64    nmap.set_port_version(host, port)
65
66    return stdnse.format_output(status, cli:getServerProperties())
67  end
```

Этот скрипт позволяет подготовиться к атаке при использовании amqp. Создаётся клиент, устанавливается соединение, извлекаются параметры (имя, название продукта и т.д.). Затем полученные параметры записываются в объект port, переданный в функцию.

4.10 Выбрать пять записей из файла nmap-service-probes и описать их работу

1. ```
   match asterisk m|^Asterisk Call Manager/([\d.]+)\r\n| p/Asterisk Call Manager/ v/$1/ cpe:
       ↪ a:digium:asterisk:$1/
   ```

   Сначала должно быть описание приложения - Asterisk Call Manager, затем ищет числа, разделённые точкой. Далее указано выводимое описание - название продукта (p), версия (v), которая парсится описанным ранее регулярным выражением, далее идёт описание CPE (стандартный формат наименования программных продуктов).

2. ```
   Exclude T:9100-9107
   ```

   Исключить порты с 9100 по 9107.

3. ```
   Probe TCP NULL q||
   ```

   Задаётся имя и формат посылки. В данном случае - для TCP, имя NULL, далее описывается посылаемое сообщение - в данном случае оно пустое. Т.е. далее в директивах match описываются сигнатуры реакций сервисов на данный запрос.

4. ```
   match someServer m/^Greeting \((\w*) ([\d.]*)\)/ p/$1/ v/$2/
   ```

   Описывается представленный выше сервер. Сначала ожидается слово Greeting, далее в скобках - сначала слово, а затем версия, заданные регулярными выражениями. Далее описывается имя продукта - слово, распарсенное из первого регулярного выражения, а затем версия продукта - число из второго регулярного выражения.

5. ```
   match asterisk-proxy m|^Response: Follows\r\nPrivilege: Command\r\n--END COMMAND--\r\n| p
       ↪ /Asterisk Call Manager Proxy/ cpe:/a:digium:asterisk/
   ```

   В ответе должна содержаться строка, указанная между ^и CPE. Далее описывается CPE.

5 Выводы

В работе рассмотрена утилита nmap. Она позволяет сканировать удалённые хосты на наличие открытых портов, а следовательно, искать уязвимости в них. С её помощью можно определить наименование и версию операционной системы, названия и версии используемых сервисов, привязанных к определённых портам. Можно произвести анализ соответствия сервиса, привязанного к определённому порту, стандартному назначению порта. Также можно редактировать и добавлять свои сигнатуры в файлы, используемые утилитой nmap, тонко настраивать порты сканирования и параметры отображения. Утилита входит в состав пакетов Metasploit и Fetasploit Framework. Также утилита nmap имеет свой скриптовой движок и позволяет использовать готовые или писать свои скрипты. Nmap является одним из фундаментов при подготовке и проведении атаки на удалённый хост.
   ```