

Отчет по лабораторным работам 4-5:  
"Утилита для исследования сети и сканер  
портов Nmap, Инструмент тестов на  
проникновение Metasploit"  
по дисциплине  
"Методы и средства защиты информации"

Певцов Игорь, гр.53501/3

1 июня 2015 г.

## Содержание

<b>1</b>	<b>Утилита для исследования сети и сканер портов Nmap.</b>	<b>3</b>
1.1	Цель работы . . . . .	3
1.2	Ход работы . . . . .	3
1.2.1	Определение набора и версии сервисов, запущенных на компьютере в диапазоне адресов. . . . .	3
1.2.2	Сканирование виртуальной машины Metasploitable2 с использованием db_nmap из состава metasploitframework. . . . .	10
1.2.3	Выбрать 5 записей из файла nmap-service-probes и описать их работу. . . . .	10
1.2.4	Выбрать один скрипт из состава Nmap и описать его работу. . . . .	10
1.3	Выводы . . . . .	10
<b>2</b>	<b>Инструмент тестов на проникновение Metasploit.</b>	<b>10</b>
2.1	Цель работы . . . . .	10
2.2	Ход работы . . . . .	11
2.2.1	Изучение . . . . .	11
2.2.2	Подключение к VNC-серверу, получение доступа к консоли . . . . .	11
2.2.3	Получение списка директорий в общем доступе по протоколу SMB . . . . .	11
2.2.4	Получение консоли с использованием уязвимости в vsftpd . . . . .	11
2.2.5	Получение консоли с использованием уязвимости в irc . . . . .	11
2.2.6	Armitage Nail Mary . . . . .	11
2.3	Выводы . . . . .	11

# 1 Утилита для исследования сети и сканер портов Nmap.

## 1.1 Цель работы

Изучение принципов работы утилиты Nmap на примере локальной сети

## 1.2 Ход работы

Работа выполнялась в домашней локальной сети с адресами 192.168.1.0/24

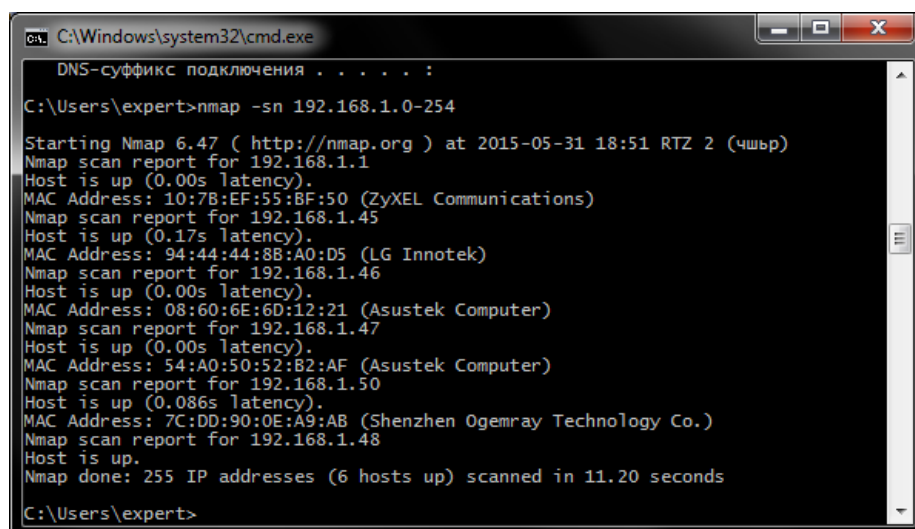
### 1.2.1 Определение набора и версии сервисов, запущенных на компьютере в диапазоне адресов.

#### Сканирование хостов

Проводим поиск активных хостов. Для этого необходимо ввести команду

```
nmap -sn 192.168.1.0-254
```

Ключ -sn служит для "быстрого" сканирования, когда не сканируются порты. Результат выполнения команды:



```
C:\Windows\system32\cmd.exe
DNS-суффикс подключения . . . . . :
C:\Users\expert>nmap -sn 192.168.1.0-254
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 18:51 RTZ 2 (чшьр)
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
MAC Address: 10:7B:EF:55:BF:50 (ZyXEL Communications)
Nmap scan report for 192.168.1.45
Host is up (0.17s latency).
MAC Address: 94:44:44:8B:A0:D5 (LG Innotek)
Nmap scan report for 192.168.1.46
Host is up (0.00s latency).
MAC Address: 08:60:6E:6D:12:21 (Asustek Computer)
Nmap scan report for 192.168.1.47
Host is up (0.00s latency).
MAC Address: 54:A0:50:52:B2:AF (Asustek Computer)
Nmap scan report for 192.168.1.50
Host is up (0.086s latency).
MAC Address: 7C:DD:90:0E:A9:AB (Shenzhen Ogemray Technology Co.)
Nmap scan report for 192.168.1.48
Host is up.
Nmap done: 255 IP addresses (6 hosts up) scanned in 11.20 seconds
C:\Users\expert>
```

Рис. 1: Сканирование хостов.

## Сканирование портов

Чтобы просканировать порты используем команду

```
nmap --top-ports 10 192.168.1.0-254
```

Ключ `-top-ports 10` используется для вывода информации о 10 наиболее активных портах в заданном диапазоне адресов. Результат выполнения команды:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 18:56 RTZ 2
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    open  telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   open  netbios-ssn
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  closed ms-wbt-server
MAC Address: 10:7B:EF:55:BF:50 (ZyXEL Communications)

Nmap scan report for 192.168.1.43
Host is up (0.12s latency).
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    filtered http
110/tcp   filtered pop3
139/tcp   filtered netbios-ssn
443/tcp   filtered https
445/tcp   filtered microsoft-ds
3389/tcp  filtered ms-wbt-server
MAC Address: 04:DB:56:2D:82:76 (Apple)

Nmap scan report for 192.168.1.45
Host is up (0.028s latency).
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
```

443/tcp closed https  
445/tcp closed microsoft-ds  
3389/tcp closed ms-wbt-server  
MAC Address: 94:44:44:8B:A0:D5 (LG Innotek)

Nmap scan report for 192.168.1.46  
Host is up (0.0040s latency).  
PORT STATE SERVICE  
21/tcp filtered ftp  
22/tcp filtered ssh  
23/tcp filtered telnet  
25/tcp filtered smtp  
80/tcp open http  
110/tcp filtered pop3  
139/tcp filtered netbios-ssn  
443/tcp open https  
445/tcp filtered microsoft-ds  
3389/tcp filtered ms-wbt-server  
MAC Address: 08:60:6E:6D:12:21 (Asustek Computer)

Nmap scan report for 192.168.1.47  
Host is up (0.0032s latency).  
PORT STATE SERVICE  
21/tcp filtered ftp  
22/tcp filtered ssh  
23/tcp filtered telnet  
25/tcp filtered smtp  
80/tcp filtered http  
110/tcp filtered pop3  
139/tcp open netbios-ssn  
443/tcp filtered https  
445/tcp open microsoft-ds  
3389/tcp filtered ms-wbt-server  
MAC Address: 54:A0:50:52:B2:AF (Asustek Computer)

Nmap scan report for 192.168.1.50  
Host is up (0.026s latency).  
PORT STATE SERVICE  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet  
25/tcp closed smtp  
80/tcp open http  
110/tcp closed pop3  
139/tcp open netbios-ssn  
443/tcp closed https  
445/tcp closed microsoft-ds  
3389/tcp closed ms-wbt-server  
MAC Address: 7C:DD:90:0E:A9:AB (Shenzhen Ogemray Technology Co.)

```

Skipping SYN Stealth Scan against 192.168.1.48 because Windows does not support
scanning your own machine (localhost) this way.
Nmap scan report for 192.168.1.48
Host is up.
PORT      STATE      SERVICE
21/tcp    unknown   ftp
22/tcp    unknown   ssh
23/tcp    unknown   telnet
25/tcp    unknown   smtp
80/tcp    unknown   http
110/tcp   unknown   pop3
139/tcp   unknown   netbios-ssn
443/tcp   unknown   https
445/tcp   unknown   microsoft-ds
3389/tcp  unknown   ms-wbt-server

Nmap done: 255 IP addresses (7 hosts up) scanned in 12.46 seconds

```

### Сканирование портов с запросом версий сервисов

Сканируем порты с использованием ключа -V для определени версий

```

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-01 00:50 RTZ 2
Nmap scan report for 192.168.1.46
Host is up (0.045s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  skype2  Skype
443/tcp    open  skype2  Skype
MAC Address: 08:60:6E:6D:12:21 (Asustek Computer)

Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 3 IP addresses (2 hosts up) scanned in 188.57 seconds

```

Из листинга исключен хост 192.168.1.48 поскольку он является локальной машиной и не может исследоваться подобным образом.

### Служебные файлы

Файл **nmap-services** представляет собой базу портов и протоколов. В данном файле можно найти описание назначения портов, причем не только стандартных, но и используемых вредоносным ПО. Отрывок из файла.

```

\# 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

Файл **nmap-os-db** является базой данных примеров(fingerprint) поведения различных операционных систем при воздействии на них с помощью Nmap. Пример fingerprint'a из файла **nmap-os-db**.

```

\# 2.6.38.7-desktop-1mnb2
\# Mandriva 2011 (free) Kernel: Linux 2.6.38.7
Fingerprint Linux 2.6.38
Class Linux | Linux | 2.6.X | general purpose
CPE cpe:/o:linux:linux\_kernel:2.6 auto
SEQ(SP=CO-CA%GCD=1-6%ISR=C7-D1%TI=Z%CI=Z%TS=A)
OPS(O1=M5B4ST11NW5|M5B4ST11NW6|M5B4ST11NW7|M5B4ST11NW8|M5B4ST11NW9%O2=M5B4ST11NW5|M5B4ST11NW6|M5B4ST11NW7|M5B4ST11NW8|M5B4ST11NW9%O3=M5B4NNT11NW5|M5B4NNT11NW6|M5B4NNT11NW7|M5B4NNT11NW8|M5B4NNT11NW9%O4=M5B4ST11NW5|M5B4ST11NW6|M5B4ST11NW7|M5B4ST11NW8|M5B4ST11NW9%O5=M5B4ST11NW5|M5B4ST11NW6|M5B4ST11NW7|M5B4ST11NW8|M5B4ST11NW9%O6=M5B4ST11)
WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)
ECN(R=Y%DF=Y%T=3B-45%TG=40%W=3908%O=M5B4NNSNW5|M5B4NNSNW6|M5B4NNSNW7|M5B4NNSNW8|M5B4NNSNW9%CC=N)
T1(R=Y%DF=Y%T=3B-45%TG=40%S=0%A=S+%F=AS%RD=0)
T2(R=N)
T3(R=Y%DF=Y%T=3B-45%TG=40%W=3890%S=0%A=S+%F=AS%O=M5B4ST11NW5|M5B4ST11NW6|M5B4ST11NW7|M5B4ST11NW8|M5B4ST11NW9)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%RD=0)
T5(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%RD=0)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%RD=0)
T7(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%RD=0)
U1(DF=N%T=3B-45%TG=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G)
IE(DFI=N%T=3B-45%TG=40%CD=S)

```

Файл **nmap-service-probes** является базой данных примеров поведения различных сервисов при воздействии на них с помощью Nmap.

Для добавления сигнатуры в файл nmap-service-probes создадим простой tcp-сервер. Исходный код сервера:

Листинг 1: Пример простого TCP-сервера

```
1  /* Name: Simple TCP server */
2  /* Version: 1.2 */
3
4  #include <sys/socket.h>
5  #include <netinet/in.h>
6  #include <stdio.h>
7  #include <string.h>
8
9  int main(int argc, char**argv)
10 {
11     int listenfd;
12     int connfd;
13     int msgsize;
14
15     struct    sockaddr_in servaddr;
16     struct    sockaddr_in cliaddr;
17
18     socklen_t clilen;
19     pid_t     childpid;
20     char      msg[1000];
21
22     listenfd = socket(AF_INET, SOCK_STREAM, 0);
23     bzero(&servaddr, sizeof(servaddr));
24
25     servaddr.sin_family = AF_INET;
26     servaddr.sin_addr.s_addr = htonl(INADDR_ANY);           /* ADDR:
27     ANY! */
28     servaddr.sin_port = htons(3000);                        /* PORT:
29     3000 */
30     bind(listenfd, (struct sockaddr *)&servaddr, sizeof(servaddr));
31
32     listen(listenfd, 1024);
33
34     for (;;)
35     {
36         clilen = sizeof(cliaddr);
37         connfd = accept(listenfd, (struct sockaddr *)&cliaddr, &clilen)
38         ;
39
40         if ((childpid = fork()) == 0)
41         {
42             close(listenfd);
43
44             for (;;)
45             {
46                 msgsize = recvfrom(connfd, msg, 1000, 0, (struct sockaddr
47                 *)&cliaddr, &clilen);
48                 if (!strncmp(msg, "version", 7))
49                 {
50                     strcpy(msg, "1.0.0\n");
51                     msgsize = strlen(msg);
52                 }
53                 sendto(connfd, msg, msgsize, 0, (struct sockaddr *)&
54                 cliaddr, sizeof(cliaddr));
55             }
56         }
57     }
58 }
```



```

54 |     close(connfd);
55 | }
56 | }

```

Сервер запущен, запускаем Nmap:

```

nmap -sV -p 3000 192.168.1.48

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 18:56 RTZ 2
Nmap scan report for 192.168.1.48
Host is up (0.0038s latency).
PORT      STATE SERVICE VERSION
3000/tcp  open  echo

Service detection performed.
Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.28 seconds

```

Nmap распознал, что сервер является эхо-сервисом, однако не смог узнать версию сервиса. Попробуем подредактировать файл `nmap-service-probes`, добавив следующий текст:

```

#####NEXT PROBE#####
# Simple TSP server.
Probe TCP simple-tcp-server-ver q|version\\r\\n|
rarity 9
ports 3000
match stcps m|^1\\.0\\.0$| p/Simple TCP Server/ v/1.2/

```

Повторное сканирование:

```

$ nmap -sV -p 3000 192.168.1.48
Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 18:56 RTZ 2
Nmap scan report for 192.168.1.48
Host is up (0.0035s latency).
PORT      STATE SERVICE VERSION
3000/tcp  open  stcps   Simple TCP Server 1.2
Service detection performed.
Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.21 seconds

```

Версия сервиса определена верно.

### Сохранение вывода программы в формате xml

Для сохранения в формате xml используем команду:

```

nmap -sV -p 3000 -oX - scanme.nmap.org 192.168.1.48

```

Результат выполнения команды:

```

<?xml version="1.0"?>
<?xml-stylesheet href="file:///usr/bin/../../share/nmap/nmap.xsl"
                    type="text/xsl"?>
<!-- Nmap 6.47 scan initiated Sun May 31 23:47:51 2015
      as: nmap -sV -p 3000 -oX - scanme.nmap.org 192.168.1.48 -->
<nmaprun scanner="nmap" args="nmap -sV -p 3000 -oX - scanme.nmap.org
192.168.1.48" start="1431910071" startstr="Sun May 31 23:47:51
2015" version="6.47" xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1" services="3000"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1431910071" endtime="1431910079"><status state="up"
      reason="conn-refused" reason_ttl="0"/>
<address addr="192.168.1.48" addrtype="ipv4"/>
<hostnames>
</hostnames>
<ports><port protocol="tcp" portid="3000"><state state="open"
      reason="syn-ack" reason_ttl="0"/><service name="stcps" product=
      "Simple TCP Server" version="1.2" method="probed" conf="10"/>
</port>
</ports>
<times srtt="4122" rttvar="2991" to="100000"/>
</host>
<runstats><finished time="1431910079" timestr="Sun May 31 23:47:51 2015"
elapsed="7.40" summary="Nmap done at Sun May 31 23:47:51 2015;
2 IP addresses (1 host up) scanned in 7.40 seconds"
exit="success"/><hosts up="1" down="1" total="2"/>
</runstats>
</nmaprun>

```

1.2.2 Сканирование виртуальной машины Metasploitable2 с использованием db\_nmap из состава metasploitframework.

1.2.3 Выбрать 5 записей из файла nmap-service-probes и описать их работу.

1.2.4 Выбрать один скрипт из состава Nmap и описать его работу.

## 1.3 Выводы

# 2 Инструмент тестов на проникновение Metasploit.

## 2.1 Цель работы

Изучение принципов работы инструментария тестов на проникновения Metasploit.

## **2.2   Ход работы**

### **2.2.1   Изучение**

### **2.2.2   Подключение к VNC-серверу, получение доступа к консоли**

### **2.2.3   Получение списка директорий в общем доступе по протоколу SMB**

### **2.2.4   Получение консоли с использованием уязвимости в vsftpd**

### **2.2.5   Получение консоли с использованием уязвимости в irc**

### **2.2.6   Armitage Nail Mary**

## **2.3   Выводы**