Отчет по лабораторной работе №4 Nmap + Metasploit

джомбо яшо

14 июня 2015 г.

1 NMAP

1.1 Цель работы

Научиться пользоваться утлитой nmap.

1.2 Ход работы

1.2.1 Подготовка

Скачаны дистрибутивы Kali linux и Metasploitable2, развернуты на virtualbox, тип сетевого поделючения - сетевой мост.

1.2.2 Поиск активных хостов

Поиск активных хостов путем ICMP ping. Данный способ может не сработать в реальных условиях, т.к. в большинстве корпоротивных сетей блокируется из соображений безопасности.

```
root@debian:~# nmap --version

Nmap version 6.47 ( http://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: nmap-liblua-5.2.3 openssl-1.0.1e libpcre-8.30 libpcap-1.3.0 nmap-libdnet-1.
Compiled without:
Available nsock engines: epoll poll select
root@debian:~# nmap -sn 192.168.0.*

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-11 01:15 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0079s latency).
MAC Address: E8:94:F6:FA:47:16 (Tp-link Technologies Co.)
Nmap scan report for 192.168.0.2
Host is up (0.054s latency).
MAC Address: B8:C6:8E:A2:E3:38 (Samsung Electronics Co.)
Nmap scan report for 192.168.0.150
Host is up (0.0021s latency).
MAC Address: 30:10:B3:0C:BB:B4 (Liteon Technology)
Nmap scan report for 192.168.0.151
Host is up (0.00083s latency).
MAC Address: 08:00:27:FF:A2:B1 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.152
Host is up (0.0060s latency).
MAC Address: B8:C6:8E:A2:E3:38 (Samsung Electronics Co.)
Nmap scan report for 192.168.0.153
Host is up (0.024s latency).
MAC Address: C0:D9:62:7D:50:25 (Askey Computer)
Nmap scan report for 192.168.0.154
Host is up (0.0022s latency).
MAC Address: 08:00:27:1A:CA:E6 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.156
```

```
Host is up (0.0010s latency).
MAC Address: 08:00:27:D6:48:F3 (Cadmus Computer Systems)
Nmap scan report for 192.168.0.155
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.65 seconds
root@debian:~#
```

итого id Metasploit able 2

- 192.168.0.156 Metasploit able 2

Полученые результаты соответствуют действительности.

1.2.3 Поиск открытых портов

Для этих целей будем использовать уязвиную машину Metaspoitable 2.

```
root@debian:~# nmap 192.168.0.156

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-11 01:21 EDT
Nmap scan report for 192.168.0.156
Host is up (0.0011s latency).
Not shown: 976 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
50003/tcp open  unknown
MAC Address: 08:00:27:D6:48:F3 (Cadmus Computer Systems)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@debian:~#
```

1.2.4 Определение версии сервисов

```
root@debian:~# nmap 192.168.0.156 -sV

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-11 01:27 EDT
Nmap scan report for 192.168.0.156
Host is up (0.00059s latency).
Not shown: 976 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  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
50003/tcp open  unknown
MAC Address: 08:00:27:D6:48:F3 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs:

Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 167.96 seconds
root@debian:~#
```

1.2.5 Сохраняем вывод утлиты в Xml

```
root@debian:~# nmap 192.168.0.156 -sV -oX /home/nmapOutput.txt
Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-11 01:33 EDT
Nmap scan report for 192.168.0.156
Host is up (0.00072s latency).
Not shown: 976 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  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
50003/tcp open  unknown
MAC Address: 08:00:27:D6:48:F3 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs:

Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 167.45 seconds
root@debian:~#
```

Полученный файл находится в репозитории.

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

Данные файлы находятся в репозитории.

- nmap-services Представляет собой таблицу в которой содержатся информация о сервисах, типу и номеру порта, и частоте появления.
- nmap-os-db Содержит информацию о сигнатурах рахличных ОС.

  Пример записи:

```
# 2-Wire 2701HG-G Gateway Software:  5.29.133.27
Fingerprint 2Wire 2701HG-G wireless ADSL modem
Class 2Wire | embedded || WAP
CPE cpe:/h:2wire:2701hg-g
SEQ(SP=7B-85%GCD=1-6%ISR=95-9F%TI=I%II=I%SS=S%TS=A)
OPS(O1=M5B4NNSW0NNNT11%O2=M578NNSW0NNNT11%O3=M280W0NNNT11%O4=M218NNSW0NNNT11%O5=M218N
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=Y%DF=Y%T=FA-104%TG=FF%W=8000%S=O%A=S+%F=AS%O=M109NNSW0NNNT11%RD=0%Q=)
T4(R=N)
T5(R=Y%DF=Y%T=FA-104%TG=FF%W=0%S=Z%A=S+%F=AR%O=%RD=BD1AB510%Q=)
T6(R=N)
T7(R=N)
U1(DF=Y%T=FA-104%TG=FF%IPL=70%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=Y%T=FA-104%TG=FF%CD=S)
```

- nmap-service-probes Содержит скрипт для определения сервиса, запущенного на данном порте.

  Пример записи:

```
Probe TCP NessusTPv10 q|< NTP/1.0 >\n|
rarity 8
ports 1241
sslports 1241

match http-proxy m|^HTTP/1\.0 400 Bad Request\r\nServer: squid/([\w._+-]+)\r\n| p/Squ

match nessus m|^< NTP/1.0 >\n| p/Nessus Daemon/ i/NTP v1.0/ cpe:/a:tenable:nessus/
match zabbix m|^NOT OK\n$| p/Zabbix Monitoring System/ cpe:/a:zabbix:zabbix/
```

1.2.7 Добавление своей сигнатуры

В качестве сервера была использована утлита netcat:

```
root@kali:~# (echo -e "HelloWorld\nVersion 1.2.3.4";) | nc -vv -l -p 5000
```

Сигнатура:

```
Probe TCP SimpleServer q|Any text|

match simple tcp m|HelloWorld\nVersion ([0-9.]*)|
p/Simple Server/ v/$P(1)/
```

Из ответа извлекается версия и возвращается в качестве ответа.

```
root@debian:~# nmap 192.168.0.155 -p 5000 -sV
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-11 02:48 EDT
Nmap scan report for 192.168.0.155
Host is up (0.00034s latency).
PORT     STATE  SERVICE VERSION
5000/tcp closed upnp

Service detection performed. Please report any incorrect results at http://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
root@debian:~#
```

1.2.8 Исследование различных способов сканирования с помощью утлиты WireShark

Исследовались следующие варианты сканирования портов для машины-цели с адресом 192.168.0.153

Wireshark является программой-анализатором сетевых пакетов с исходным кодом. Без какого-либо специального оборудования или перенастройки эта программа может перехватывать входящие и исходящие данные на любом сетевом интерфейсе компьютера: Ethernet, WiFi, PPP, loopback и даже USB. Обычно Wireshark применяется для выявления проблем в сети, таких, как перегруженность, слишком долгое время ожидания или ошибки протоколов. Но для того, чтобы изучить Wireshark, совсем не нужно ждать, когда произойдет какая-либо поломка. Давайте приступим к обзору этой программы.

Перехват трафика

Запуск новой сессии перехвата производится в окне программы из меню "Capture". Чтобы увидеть весь список сетевых интерфейсов, которые смогла обнаружить Wireshark, перейдите по пути в меню "Capture > Interfaces". Появится диалоговое окно, в котором, помимо физических устройств, будет присутствовать псевдо-устройство "any которое перехватывает данные со всех других устройств этого списка. Перед началом можно задать некоторые опции, с которыми будет запускаться перехват. Перейдя по "Capture > Options достаточно выбрать:

- фильтры для выборочного анализа трафика (например, по определенному протоколу или диапазону адресов); - автоматически остановить перехват по достижении указанного в настройках времени; - отсортировать полученные данные по указанному размеру или дате.

Первое, что вы увидите при запуске новой сессии - окно лога, где будет показываться основная информация о выполняемом программой процессе: источник, приемник, протокол, время и т.п. Вся информация организована в виде таблицы с заголовками. Для большей удобочитаемости Wireshark выполняет цветовое выделение фрагментов текста, изменение цвета фона или пометку наиболее "интересных"пакетов с помощью флагов.

1.3 Выводы

работы были изучены основные возможности nmap. Определение активных хостов, сканирование портов, определение версий сервисов, дополнение

определения версий сервисов, были рассмотрены основные файлы используемые для определения версий сервисов и ОС.