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

Анастасия Тарасова

30 марта 2015 г.

1 Цель работы

2 Ход работы

Определить набор и версии сервисов запущенных на компьютере в диапазоне адресов.

2.1 Поиск активных хостов

`db_nmap -sN 100.0.0/24` - поиск активных хостов

Вывод:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-29 18:01 EDT
Nmap scan report for 100.0.0.24
Host is up (0.00020s latency).
Not shown: 977 closed ports
PORT     STATE          SERVICE
21/tcp   open|filtered  ftp
22/tcp   open|filtered  ssh
23/tcp   open|filtered  telnet
25/tcp   open|filtered  smtp
53/tcp   open|filtered  domain
80/tcp   open|filtered  http
111/tcp  open|filtered  rpcbind
139/tcp  open|filtered  netbios-ssn
445/tcp  open|filtered  microsoft-ds
512/tcp  open|filtered  exec
513/tcp  open|filtered  login
514/tcp  open|filtered  shell
1099/tcp open|filtered  rmiregistry
1524/tcp open|filtered  ingreslock
2049/tcp open|filtered  nfs
2121/tcp open|filtered  ccproxy-ftp
3306/tcp open|filtered  mysql
5432/tcp open|filtered  postgresql
5900/tcp open|filtered  vnc
6000/tcp open|filtered  X11
6667/tcp open|filtered  irc
8009/tcp open|filtered  ajp13
8180/tcp open|filtered  unknown
MAC Address: 08:00:27:D4:D7:99 (Cadmus Computer Systems)

Nmap scan report for 100.0.0.23
Host is up (0.0000050s latency).
All 1000 scanned ports on 100.0.0.23 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 31.31 seconds
```

2.2 Определить открытые порты

`db_nmap -sS 100.0.0/24` - просмотр активных портов

Вывод:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-29 18:33 EDT
Nmap scan report for 100.0.0.24
Host is up (0.00011s 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:D4:D7:99 (Cadmus Computer Systems)

Nmap scan report for 100.0.0.23
Host is up (0.0000050s latency).
All 1000 scanned ports on 100.0.0.23 are closed

Nmap done: 256 IP addresses (2 hosts up) scanned in 29.82 seconds
```

2.3 Определить версии сервисов

`db_nmap -sV 100.0.0/24` - показать версии сервисов

Вывод:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-29 18:51 EDT
Nmap scan report for 100.0.0.24
Host is up (0.00015s 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 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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
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=6.47%I=7%D=3/29%Time=551881FD%P=i686-pc-linux-
gnu%r(NULL,
SF:33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name
\x20resolutio
```

```
SF:n\n");
MAC Address: 08:00:27:D4:D7:99 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:
linux_kernel

Nmap scan report for 100.0.0.23
Host is up (0.0000050s latency).
All 1000 scanned ports on 100.0.0.23 are closed

Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 39.96 seconds
```

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

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

(для этого создать минимальный tcp server, добиться, чтобы прискани-ровании nmap указывал для него название и версию)

2.6 Сохранить вывод утилиты в формате xml

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

`Просканировать виртуальную машину Metasploitable2 используя nmap_db 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 Выводы

Для поиска активных хостов испольховался ключ **-sN**, –**sS**