NMAP

nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 fingerprinting）。它是网络管理员必用的软件之一，以及用以评估网络系统安全。
正如大多数被用于网络安全的工具，nmap 也是不少黑客及骇客（又称脚本小子）爱用的工具 。系统管理员可以利用nmap来探测工作环境中未经批准使用的服务器，但是黑客会利用nmap来搜集目标电脑的网络设定，从而计划攻击的方法。
Nmap 常被跟评估系统漏洞软件Nessus混为一谈。Nmap 以隐秘的手法，避开闯入检测系统的监视，并尽可能不影响目标系统的日常操作。

发现
namp 192.168.0.1 -sn
使用arping192.168.0.1

nmap -iL ip.txt -sn
对ip.txt的IP进行arping握手

扫描系统
nmap -O 192.168.79.146
查询192.168.79.146的系统

nmap 192.168.79.146 -p1 -100 -Sv
扫描192.168.79.146 100个端口中的服务信息

扫描服务
nmap 192.168.79.146 -p1 -100 -sV
扫描192.168.79.146,，是否可以成为自己的僵尸机

```
C:\root> nmap 192.168.79.146 -p1 -100 -sV
nmap: unrecognized option '-100'
See the output of nmap -h for a summary of options.
C:\root> nmap 192.168.79.146 -p1- 100 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 01:26 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00017s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:96:09:B8 (VMware)
Service Info: Host: WIN-EQB7A0K4NRR; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 93.09 seconds
```

nmap 192.168.79.128 -sI 192.168.79.146 -Pn -p 0-100

利用僵尸机扫描192.168.79.128 中的 0 ~100个端口信息

```
C:\root> nmap 192.168.79.128 -sI 192.168.79.146 -Pn -p 0-100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 01:40 EDT
Skipping Idle Scan against 192.168.79.128 -- you can't idle scan your own machine (localhost)
Nmap scan report for 192.168.79.128
Host is up.

PORT    STATE   SERVICE
0/tcp   unknown unknown
1/tcp   unknown tcpmux
2/tcp   unknown compressnet
3/tcp   unknown compressnet
4/tcp   unknown unknown
5/tcp   unknown rje
6/tcp   unknown unknown
7/tcp   unknown echo
8/tcp   unknown unknown
9/tcp   unknown discard
10/tcp  unknown unknown
11/tcp  unknown systat
12/tcp  unknown unknown
13/tcp  unknown daytime
14/tcp  unknown unknown
```

nmap -iR 10 -p445

随机选择10个ip对445端口进行扫描

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 02:47 EDT
Nmap scan report for 11.37.168.128
Host is up (0.00012s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap scan report for ppp108-61.static.internode.on.net (59.167.108.61)
Host is up (0.0015s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap scan report for 6.58.89.158
Host is up (0.00012s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
```

nmap 192.168.79.0/24 --exclude 192.168.79.1- 2

对192.168.79.0/24网段进行扫描，但排除1~2

nmap sogo.com --traceroute -p80

显示sogo且指定80端口查看经过的路由位置

```
C:\root> nmap sogo.com --traceroute -p80
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:10 EDT
Nmap scan report for sogo.com (49.7.20.53)
Host is up (0.0019s latency).
Other addresses for sogo.com (not scanned): 36.110.164.37 36.110.170.48 36.110.165.43 106.39.246.42

PORT   STATE SERVICE
80/tcp open  http

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.07 ms 192.168.79.2
2   0.07 ms 49.7.20.53

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
C:\root>
```

nmap -p U:445 192.168.79.146

仅对192.168.79.146进行UDP扫描（把u换成t就成为了仅扫描TCP）

```
C:\root> nmap -p U:445 192.168.79.146
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:24 EDT
WARNING: a TCP scan type was requested, but no tcp ports were specified.  Skipping this scan type.
Nmap scan report for 192.168.79.146
Host is up (0.00028s latency).
0 ports scanned on 192.168.79.146
MAC Address: 00:0C:29:96:09:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
C:\root> nmap -p T:445 192.168.79.146
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:24 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00033s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:96:09:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
C:\root>
```

nmap 192.168.79.146 --top-ports 6

仅对192.168.79.146扫描6个端口

```
C:\root> nmap 192.168.79.146 --top-ports 6
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:28 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00037s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
443/tcp closed https
MAC Address: 00:0C:29:96:09:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
C:\root>
```

nmap -p445 192.168.79.146 -sV --version-intensity 9

针对192.168.79.146 445端口使用版本探测探测报文的深度为0~9之间，其中9是最高等级

```
C:\root> nmap -p445 192.168.79.146 -sV --version-intensity 9
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:33 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00039s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:96:09:B8 (VMware)
Service Info: Host: WIN-EQB7A0K4NRR; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.68 seconds
```

nmap --script-help=http-vuln-cve2017-8917.nse

查看http-vuln-cve2017-8917.nse模块的详细信息（使用ls /usr/share/nmap/scripts/ 查看所在目录）

```
C:\root> nmap --script-help=http-vuln-cve2017-8917.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:40 EDT

http-vuln-cve2017-8917
Categories: vuln intrusive
https://nmap.org/nsedoc/scripts/http-vuln-cve2017-8917.html
  An SQL Injection vulnerability affecting Joomla! 3.7.x before 3.7.1 allows for
  unauthenticated users to execute arbitrary SQL commands. This vulnerability was
  caused by a new component, <code>com_fields</code>, which was introduced in
  version 3.7. This component is publicly accessible, which means this can be
  exploited by any malicious individual visiting the site.

  The script attempts to inject an SQL statement that runs the <code>user()</code>
  information function on the target website. A successful injection will return
  the current MySQL user name and host name in the extra_info table.

  This script is based on a Python script written by brianwrf.

  References:
  * https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html
```

map -p445 192.168.79.146 --scan-delay 20s

20秒之后针对192.168.79.146 445端口进行扫描

```
C:\root> nmap -p445 192.168.79.146 --scan-delay 20s
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:48 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00044s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:96:09:B8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 40.18 seconds
```

nmap -D 192.168.79.131,192.168.79.132,192.168.79.133,192.168.79.128

使用192.168.79.131，192.168.79.132,192.168.79.133等诱饵对192.168.79.128进行隐蔽扫描（注意，诱饵主机必须在工作状态，否则将会导致目标主机受到来自于你的SYN洪水攻击）

```
C:\root> nmap -D 192.168.79.131,192.168.79.132,192.168.79.133,192.168.79.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:58 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
C:\root> nmap -D 192.168.79.131,192.168.79.132,192.168.79.133 192.168.79.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 03:59 EDT
Nmap scan report for 192.168.79.128
Host is up (0.000060s latency).
All 1000 scanned ports on 192.168.79.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 15.57 seconds
```

nmap -S 192.168.79.131 -e eth0 192.168.79.146

使用192.168.79.131进行原地址欺骗目标192.168.79.146

```
C:\root> nmap -S 192.168.79.131 -e eth0 192.168.79.146
WARNING: If -S is being used to fake your source address, you may also have to use -e <interface> and -
n .  If you are using it to specify your real source address, you can ignore this warning.
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 04:04 EDT
NSOCK ERROR [0.1270s] mksock_bind_addr(): Bind to 192.168.79.131:0 failed (IOD #1): Cannot assign reque
ted address (99)
Nmap scan report for 192.168.79.146
Host is up (0.00040s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

nmap -g100 192.168.79.146

使用100端口对192.168.79.146进行扫描

```
C:\root> nmap -g100 192.168.79.146
Starting Nmap 7.80 ( https://nmap.
Nmap scan report for 192.168.79.14
Host is up (0.00032s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
```

nmap -p22 192.168.79.146 --data=ABCDEF

针对192.168.79.146 22端口并在数据包中加入数据包中。

```
SSH Protocol
[Malformed Packet: SSH]
  [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]

0000  00 0c 29 96 09 b8 00 0c  29 03 a7 24 08 00 45 00   ··)····· )··$··E·
0010  00 2f cc f8 00 00 32 06  9b 6d c0 a8 4f 80 c0 a8   ·/····2· ·m··O···
0020  4f 92 c9 fe 00 16 7d a3  fe a7 00 00 00 00 60 02   O·····}· ......`·
0030  04 00 92 91 00 00 02 04  05 b4 ab cd ef            ····· ····· ·····
```

查找漏洞模块

cd /usr/share/nmap/scripts/

进入usr/share/nmap/scripts目录

cat script.db

查看script.db文件信息

nmap -p445 --script=smb-enum-shares.nse--script- args=smbuser=admin, smbpassword=pass 192.168.79.146

利用shares.nsc，对192.168.79.146进行攻击或扫描

```
C:\root> nmap -p445 --script=smb-enum-shares.nse  192.168.79.146
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-16 07:11 EDT
Nmap scan report for 192.168.79.146
Host is up (0.00052s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:96:09:B8 (VMware)

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.79.146\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.79.146\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.79.146\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
C:\root>
```

Shell No. 1