1. DNS枚举

1.1 DNSenum

`DNSenum` 是一款非常强大的**域名信息收集工具**。它能够通过谷歌或者字典文件猜测可能存在的域名，并对一个网段进行反向查询。它不仅可以查询网站的主机地址信息、域名服务器和邮件交换记录，还可以在域名服务器上执行 `axfr` 请求，然后通过谷歌脚本得到扩展域名信息，提取子域名并查询，最后计算C类地址并执行 `whois` 查询，执行反向查询，把地址段写入文件。

- `--threads [number]`：设置用户同时运行多个进程数。
- `-r`：允许用户启用递归查询。
- `-d`：允许用户设置WHOIS请求之间时间延迟数（单位为秒）。
- `-o`：允许用户指定输出位置。
- `-w`：允许用户启用WHOIS请求。

示例：

```
> dnsenum -f /usr/share/dnsenum/dns.txt hust.edu.cn
dnsenum VERSION:1.2.6
-----   hust.edu.cn   -----
Host's addresses:
__________________
hust.edu.cn.                            4502     IN    A
 202.114.0.245

Name Servers:
______________
dns1.hust.edu.cn.                       4502     IN    A
 202.114.0.120
dns2.hust.edu.cn.                       4502     IN    A
 59.172.234.181
......
Brute forcing with /usr/share/dnsenum/dns.txt:
_____________________________________________
access.hust.edu.cn.                     4502     IN    A
 210.42.109.207
aco.hust.edu.cn.                        4502     IN    CNAME
zhanqun5.hust.edu.cn.
```

```
zhanqun5.hust.edu.cn.                    4502     IN    A
 210.42.108.5
blog.hust.edu.cn.                        4502     IN    A
 202.114.18.177
......
```

• 1.2 fierce

`fierce` 工具和 `DNSenum` 工具性质差不多，其 `fierce` 主要是**对子域名进行扫描和收集信息**的。使用 `fierce` 工具获取一个目标主机上所有IP地址和主机信息。

```
> fierce --domain baidu.com
NS: ns3.baidu.com. ns7.baidu.com. dns.baidu.com. ns4.baidu.com.
ns2.baidu.com.
SOA: dns.baidu.com. (110.242.68.134)
......
Nearby:
{'111.202.115.74': 'mx11.baidu.com.', '111.202.115.75': 'mx10.baidu.com.'}
Found: cache.baidu.com. (110.242.68.227)
Found: cafe.baidu.com. (123.125.115.189)
Found: cc.baidu.com. (112.34.111.153)
Found: cdn.baidu.com. (10.169.43.10)
......
```

• 1.3 Sublist3r

> “
> https://github.com/aboul3la/Sublist3r.git

`Sublist3r` 是一个 `python` 工具，旨在使用 `OSINT` **枚举网站的子域**。 `Sublist3r` 使用Google、Yahoo、Bing、百度和Ask等许多搜索引擎枚举子域。 `Sublist3r` 还使用Netcraft、Virustotal、ThreatCrowd、DNSdumpster和ReverseDNS来枚举子域名。

```
> python sublist3r.py -d hust.edu.cn

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|
```

```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hust.edu.cn
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 150
www.hust.edu.cn
admission.hust.edu.cn
advise.hust.edu.cn
bcf.hust.edu.cn
biophy.hust.edu.cn
blog.hust.edu.cn
byhh.hust.edu.cn
......
```

2. 测试网络范围

• 2.1 域名查询工具 `DMitry`

`DMitry` 工具是用来**查询IP或域名WHOIS信息**的。

```
> dmitry -winsepo rzchina.net
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Writing output to 'rzchina.net.txt'
HostIP:180.178.61.83
HostName:rzchina.net
......
Gathered Inic-whois information for rzchina.net
---------------------------------
   Domain Name: RZCHINA.NET
   Registry Domain ID: 965877923_DOMAIN_NET-VRSN
```

```
12      Registrar WHOIS Server: whois.bizcn.com
13      Registrar URL: http://www.bizcn.com
14      Updated Date: 2020-05-10T07:17:45Z
15      Creation Date: 2007-05-09T10:08:08Z
16      Registry Expiry Date: 2021-05-09T10:08:08Z
17      Registrar: Bizcn.com, Inc.
18      Registrar IANA ID: 471
19      Registrar Abuse Contact Email:
20      Registrar Abuse Contact Phone:
21      Domain Status: clientDeleteProhibited
    https://icann.org/epp#clientDeleteProhibited
22      Domain Status: clientTransferProhibited
    https://icann.org/epp#clientTransferProhibited
23      Name Server: DNS1.BIZMOTO.COM
24      Name Server: DNS2.BIZMOTO.COM
25      DNSSEC: unsigned
26      URL of the ICANN Whois Inaccuracy Complaint Form:
    https://www.icann.org/wicf/
27  >>> Last update of whois database: 2021-03-29T13:11:07Z <<<
28  ......
```

• 2.2 跟踪路由工具 Scapy

`Scapy` 是一款强大的交互式数据包处理工具、数据包生成器、网络扫描器、网络发现工具和包嗅探工具。它提供多种类别的交互式生成数据包或数据包集合、对数据包进行操作、发送数据包、包嗅探、应答和反馈匹配等功能。

> “
>
> 内容较多。

3. nmap

`nmap` (network mapper)是一个用于网络发现和安全审计的免费开放源码(许可证)工具。

可用于**主机发现，端口扫描，服务发现，操作系统**。

3.1 测试主机存活

```
> nmap -sP 192.168.205.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 21:22 CST
Nmap scan report for 192.168.205.3
Host is up (0.00037s latency).
MAC Address: 00:0C:29:75:81:24 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

3.2 查看打开端口

直接传入ip地址即为扫描端口。

```
> nmap 192.168.205.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 21:26 CST
Nmap scan report for 192.168.205.3
Host is up (0.0011s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:75:81:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```

`-v` ： 显示详细的扫描信息

`-sS` ： 扫描方式-sS是使用SYN半开式扫描，这种扫描方式使得扫描结果更加正确(又称半开放，或隐身扫描)

`-oN/-oX/-oS/-oG <file>` : 输出为文件normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.

`-sS/sT/sA/sW/sM` : TCP SYN/Connect()/ACK/Window/Maimon scans

`-sU` : UDP Scan

`-sN/sF/sX` : TCP Null, FIN, and Xmas scans

`-sI` <zombie host[:probeport]>: Idle scan

`-sY/sZ` : SCTP INIT/COOKIE-ECHO scans

`-sO` : IP protocol scan

`-b` : FTP bounce scan

`-p` ： 指定端口或端口范围 -p 80-445。

3.3 系统指纹识别

```
> nmap -O 192.168.205.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 21:32 CST
Nmap scan report for 192.168.205.3
Host is up (0.00083s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:75:81:24 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```

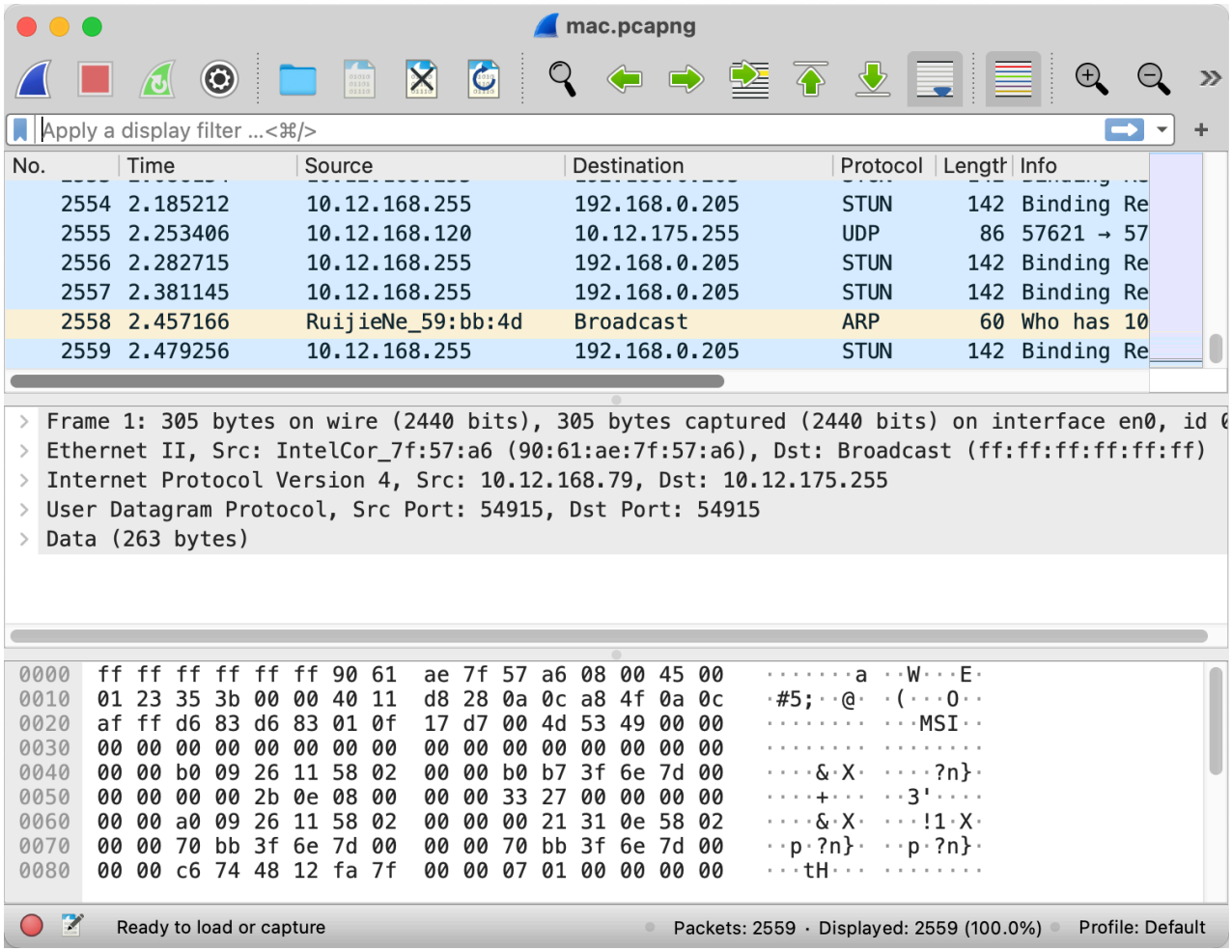
```
> nmap -O 192.168.205.6
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 19:55 CST
Nmap scan report for 192.168.205.6
Host is up (0.0016s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:74:C6:08 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```

- 指纹识别工具 `p0f`

p0f是一款**百分之百的 *被动* 指纹识别工具**。该工具通过分析目标主机发出的数据包，对主机上的操作系统进行鉴别。



```
> p0f -r ~/Desktop/mac.pcapng -o result.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Will read pcap data from file '/root/Desktop/mac.pcapng'.
[+] Default packet filtering configured [+VLAN].
[+] Log file 'result.log' opened for writing.
[+] Processing capture data.

.-[ 10.12.168.255/55108 -> 192.168.0.205/59442 (syn) ]-
|
| client   = 10.12.168.255/55108
| os       = Mac OS X
| dist     = 0
| params   = generic fuzzy
| raw_sig  = 4:64+0:0:1460:65535,6:mss,nop,ws,nop,nop,ts,sok,eol+1:id-:0
|
`----

.-[ 10.12.168.255/55108 -> 192.168.0.205/59442 (mtu) ]-
|
| client   = 10.12.168.255/55108
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

All done. Processed 2535 packets.
```

• 3.4 服务指纹识别

```
> nmap -sV 192.168.205.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 21:42 CST
Nmap scan report for 192.168.205.3
Host is up (0.00100s latency).
Not shown: 993 filtered 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)
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

```
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:75:81:24 (VMware)
Service Info: Host: WIN-96S87FOPGPF; 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 71.62 seconds
```

• 3.5 其他

```
nmap -sP 172.16.15.0/24
nmap -sP 172.16.15.*

# 列出开放了指定端口的主机列表
nmap -sT -p 80 -oG - 192.168.1.* | grep open

# 获取远程主机的系统类型及开放端口
nmap -A <target>
# 这里的 < target > 可以是单一 IP，或主机名，或域名，或子网
```

4. 其他信息收集

• 4.1 ARP侦查工具 `Netdiscover`

`Netdiscover` 是一个主动/被动的**ARP侦查工具**。使用 `Netdiscover` 工具可以在网络上扫描IP地址，检查在线主机或搜索为它们发送的ARP请求。

```
> netdiscover
 Currently scanning: 172.16.24.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120

_____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.205.1   e2:b5:5f:2f:91:64      1      60  Unknown vendor
 192.168.205.6   00:0c:29:74:c6:08      1      60  VMware, Inc.
```

• 4.2 搜索引擎工具 Shodan

Shodan是互联网上最强大的一个搜索引擎工具。该工具不是在网上搜索网址，而是直接**搜索服务器**。

> “
>
> 参考：
>
> https://tools.kali.org/tools-listing
>
> https://github.com/aboul3la/Sublist3r