实验 1　网络侦察&网络扫描

- 实验目的
  - 熟悉网络侦察的几种常用方法和作用。
  - 掌握常见扫描技术（主机扫描、端口扫描、操作系统检测）
- 实验分组
  - 独立完成
- 实验报告：每次实验需提交1份报告
  - 命名：'201530561010-陈梓仪-LAB1

实验内容一：网络侦察

- 练习搜索基本命令和技巧
- https://ahrefs.com/blog/google-advanced-search-operators/

Notation	Find result	Example
term1 term2	with both *term1* and *term2*	[carry-on luggage]
term1 OR *term2* *term1* | *term2*	with either *term1* or *term2* or both	[Tahiti OR Hawaii] [Tahiti | Hawaii]
"*term*"	with *term* (Put quotation marks around terms that are stop words — that is, words Google would otherwise ignore — or when you want Google to return only pages that match your search terms exactly.)	["i" spy]
-*term*	without *term*	[twins minnesota -baseball]
~*term*	with *term* or one of its synonyms (currently supported on Web and Directory search)	[google ~guide]
number1..*number2*	with a number in the specified range	[recumbent bicycle $250..$1000]
"*terms1* * *terms2*"	with the phrase (enclosed in quotes) and * replaced by one or more words	["Google * my life"]
"*phrase*"	with the exact *phrase*, a proper name, or a set of words in a specific order	["I have a dream"] ["Rio de Janeiro"]

Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

实验内容一：网络侦察

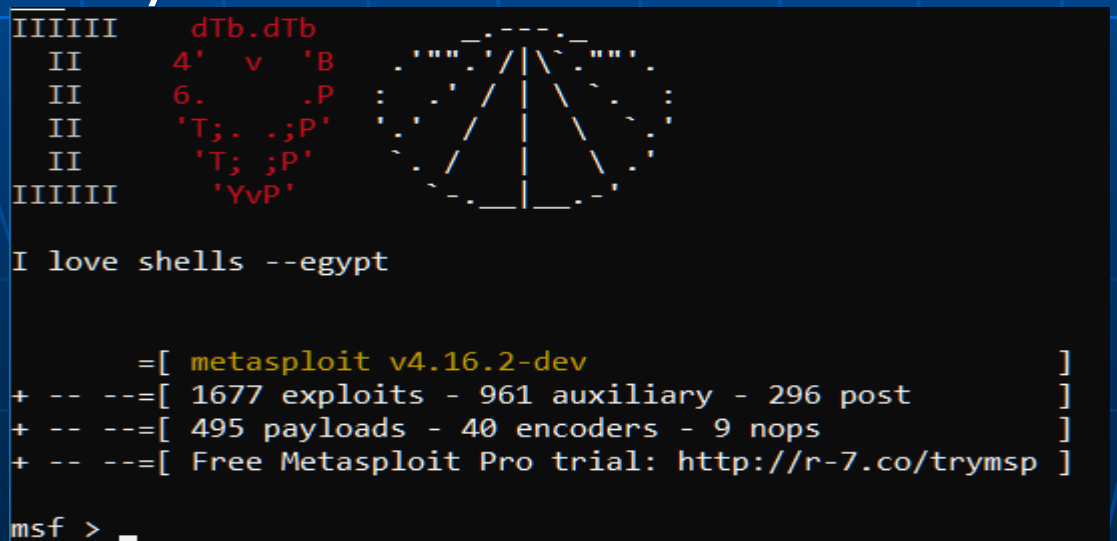
- 利用搜索引擎搜索<自选目标>
  1. 获取目标公司或网站的域名或网站地址
  2. 获取目标网络相关信息
     - 网络拓扑图
     - IP分配表
     - 网络设备
     - 安全设施
     - ……
  3. 搜索密码文件、搜索管理员后台URL、搜索CGI漏洞、搜索黑客留下的后门……

实验内容一：网络侦察

- 利用WHOIS数据库查询<自选目标>
  1. 查询目标域名的注册机构
  2. 查询目标域名详细的注册资料
     - 已注册域名的拥有者信息
     - 域名登记人信息
     - 联系方式
     - 域名注册时间和更新时间
     - 权威DNS的IP地址
     - ……
  3. 查询IP地址分配和拥有机构

实验内容二：网络扫描

- Nmap
  - **Nmap** (*Network Mapper*) is a security scanner used to discover hosts and services on a computer network, thus building a "map" of the network。
- Metasploit-framework
  - Far more than just a collection of exploits. It's an infrastructure that you can build upon and utilize for your custom needs.



Nmap default scan

nmap scanme.nmap.org

```
root@kali:~# nmap scanme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 09:19 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (3.0s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
4444/tcp  filtered krb524
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 278.69 seconds
```

Nmap service version scans

nmap –sV scanme.nmap.org

```
root@kali:~# nmap -sV canme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 09:25 EDT
Nmap scan report for canme.nmap.org (45.33.49.119)
Host is up (0.036s latency).
Other addresses for canme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe98:ff4e
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 994 filtered ports
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 6.6.1 (protocol 2.0)
25/tcp    open   smtp       Postfix smtpd
80/tcp    open   tcpwrapped
113/tcp   closed ident
443/tcp   open   ssl/ssl    Apache httpd (SSL-only mode)
31337/tcp closed Elite
Service Info: Host:  ack.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 69.05 seconds
```

Nmap specified scan ranges

- By default, Nmap will only scan the top 1,000 ports that are usually open.
- It's possible to specify a specific port range by using the -p flag
  - -p80,443
  - -p1-1024
  - -p-
- specify multiple IP addresses or hostnames
  - 192.168.1.0/24
  - 1.2.3.4,1.2.3.5,1.2.3.6
  - -iL targets.txt

Understanding the reason flag

nmap -sV --reason scanme.nmap.org

```
root@kali:~# nmap -sV --reason scanme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 09:49 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 255 (1.6s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
Reason: 992 resets
PORT      STATE    SERVICE        REASON         VERSION
22/tcp    open     ssh            syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http           syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc          no-response
139/tcp   filtered netbios-ssn    no-response
445/tcp   filtered microsoft-ds   no-response
593/tcp   filtered http-rpc-epmap no-response
4444/tcp  filtered krb524         no-response
31337/tcp open     tcpwrapped     syn-ack ttl 64
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 278.22 seconds
```

HOST DISCOVERY

- -sL (List Scan)
  - Not sending any packets to the target hosts, zero packet reconnaissance
  - Useful to get reverse DNS lookups
  - Nmap –sL 202.38.193.50-60

```
root@kali:~# nmap 202.38.193.50-60 -sL

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 10:13 EDT
Nmap scan report for 202.38.193.50
Nmap scan report for scutsvr1.scut.edu.cn (202.38.193.51)
Nmap scan report for 202.38.193.52
Nmap scan report for scutsvr2.scut.edu.cn (202.38.193.53)
Nmap scan report for 202.38.193.54
Nmap scan report for dnscache.scut.edu.cn (202.38.193.55)
Nmap scan report for 202.38.193.56
Nmap scan report for mailbox.scut.edu.cn (202.38.193.57)
Nmap scan report for 202.38.193.58
Nmap scan report for scut-nc-hub3.scut.edu.cn (202.38.193.59)
Nmap scan report for scut-nc-hub4.scut.edu.cn (202.38.193.60)
Nmap done: 11 IP addresses (0 hosts up) scanned in 0.02 seconds
```

HOST DISCOVERY

- -sn (No port scan)
  - Often known as a “ping scan”, consists of an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request
  - ARP requests are used to scan targets on a local ethernet network
  - Nmap –sn –n 192.168.56.1-254

```
root@kali:~# nmap -sn -n 192.168.56.1-254

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 10:21 EDT
Nmap scan report for 192.168.56.1
Host is up (-0.10s latency).
MAC Address: 0A:00:27:00:00:03 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00063s latency).
MAC Address: 08:00:27:7A:D7:43 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency).
MAC Address: 08:00:27:C9:39:60 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 254 IP addresses (4 hosts up) scanned in 4.63 seconds
```

HOST DISCOVERY

- -Pn (No ping)
  - By default, Nmap only performs heavy probing against hosts that are found to be up
  - -Pn causes Nmap to attempt the requested scanning functions against every target IP address specified
  - Nmap –Pn –n mmsec.science

```
root@kali:~# nmap -Pn -n mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 10:30 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (1.0s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 52.77 seconds
```

HOST DISCOVERY

- -PS port list (TCP SYN Ping)
  - Sends an empty TCP packet with the SYN flag set.
    - default destination port is 80
  - Nmap –sn –PS mmsec.science

```
root@kali:~# nmap -sn -PS mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:02 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (0.013s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

```
root@kali:~# nmap -sn -PS8080 mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:03 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (1.0s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

HOST DISCOVERY

- -PA port list (TCP ACK Ping)
  - Sends an empty TCP packet with the ACK flag set.
    - default destination port is 80
  - Nmap –sn –PA mmsec.science

```
root@kali:~# nmap -sn -PA mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:05 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (0.00018s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
root@kali:~# nmap -sn -PA8080 mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:06 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (0.00024s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

HOST DISCOVERY

- -PU port list (UDP Ping)
  - Sends a UDP packet to the given ports.
    - default destination port is 40125
  - Nmap –sn –PU mmsec.science

```
root@kali:~# nmap -sn -PU mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:17 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.16 seconds
```

```
root@kali:~# nmap -sn -PU53 mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:17 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (0.0055s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

HOST DISCOVERY

- -PE; -PP; -PM (ICMP Ping Types)
  - Send an ICMP echo request packet
  - ICMP timestamp reply (-PP)
  - and address mark reply (-PM)
- Nmap –sn –PE mmsec.science

```
root@kali:~# nmap -sn -PE mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:22 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.08 seconds
```

```
root@kali:~# nmap -sn -PP mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:22 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.08 seconds
root@kali:~# nmap -sn -PM mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:22 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.09 seconds
```

HOST DISCOVERY

- -PO protocol list (IP Protocol Ping)
  - Sends IP packets with the specified protocol number
  - Default: ICMP (protocol 1), IGMP (protocol 2), and IP-in-IP (protocol 4)
  - Nmap –sn –PO –packet-trace mmsec.science

```
root@kali:~# nmap -sn -PO --packet-trace mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:28 EDT
SENT (0.0531s) ICMP [10.0.3.15 > 139.199.1.226 Echo request (type=8/code=0) id=38562 seq=0] IP [ttl=37 id=53647 iplen=28 ]
SENT (0.0535s) IGMP (2) 10.0.3.15 > 139.199.1.226: ttl=37 id=55517 iplen=28
SENT (0.0538s) IP (4) 10.0.3.15 > 139.199.1.226: ttl=43 id=5879 iplen=20
SENT (2.0551s) IP (4) 10.0.3.15 > 139.199.1.226: ttl=48 id=11817 iplen=20
SENT (2.0557s) IGMP (2) 10.0.3.15 > 139.199.1.226: ttl=54 id=34556 iplen=28
SENT (2.0560s) ICMP [10.0.3.15 > 139.199.1.226 Echo request (type=8/code=0) id=9614 seq=0] IP [ttl=58 id=16962 iplen=28 ]
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
```

HOST DISCOVERY

- -PR (ARP Ping)
  - scan an ethernet LAN
  - Nmap –sn –PR –packet-trace mmsec.science

```
root@kali:~# nmap -sn -PR --packet-trace 192.168.56.102

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-07 01:31 EDT
SENT (0.0426s) ARP who-has 192.168.56.102 tell 192.168.56.101
RCVD (0.0430s) ARP reply 192.168.56.102 is-at 08:00:27:C9:39:60
NSOCK INFO [0.2620s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.2620s] nsock_connect_udp(): UDP connection requested to 139.199.1.226:53 (IOD #1) EID 8
NSOCK INFO [0.2630s] nsock_read(): Read request from IOD #1 [139.199.1.226:53] (timeout: -1ms) EID 18
NSOCK INFO [0.2630s] nsock_write(): Write request for 45 bytes to IOD #1 EID 27 [139.199.1.226:53]
NSOCK INFO [0.2630s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [139.199.1.226:53]
NSOCK INFO [0.2630s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [139.199.1.226:53]
NSOCK INFO [0.2710s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [139.199.1.226:53] (104 bytes)
NSOCK INFO [0.2720s] nsock_read(): Read request from IOD #1 [139.199.1.226:53] (timeout: -1ms) EID 34
NSOCK INFO [0.2720s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.2720s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.56.102
Host is up (0.00040s latency).
MAC Address: 08:00:27:C9:39:60 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

PORT SCANNING

- -sU (UDP scans)
  - If an ICMP port unreachable error (type 3, code 3) is returned, the port is closed.
  - scanning UDP services is generally slower and less reliable, many hosts rate limit ICMP port unreachable messages by default.
    - Linux 2.4.20 kernel limits destination unreachable messages to one per second

```
root@kali:~# nmap -sU -p53 mmsec.science --reason

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 10:44 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up, received reset ttl 255 (0.0022s latency).

PORT   STATE SERVICE REASON
53/udp open  domain  udp-response ttl 64

Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

PORT SCANNING

- Special TCP scans
  - -sS (TCP SYN scan)
  - -sT (TCP connect scan)
  - -sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)
  - -sA (TCP ACK scan)
  - --scanflags (Custom TCP scan)
  - -sI zombie host[:probeport] (idle scan)

OS DETECTION

- -O (Enable OS detection)
  - remote OS detection using TCP/IP stack fingerprinting
  - Nmap -O mmsec.science

```
root@kali:~# nmap -O mmsec.science

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-06 11:05 EDT
Nmap scan report for mmsec.science (139.199.1.226)
Host is up (0.011s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
8080/tcp closed http-proxy
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 21.31 seconds
```

Metasploit scanner

- Discovery

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/discovery# ll
total 64
drwxr-xr-x  2 root root  4096 Sep  5 09:14 ./
drwxr-xr-x 76 root root  4096 Sep  5 09:14 ../
-rw-r--r--  1 root root  3393 Aug 25 11:09 arp_sweep.rb
-rw-r--r--  1 root root  1247 Aug 25 11:09 empty_udp.rb
-rw-r--r--  1 root root  4080 Aug 25 11:09 ipv6_multicast_ping.rb
-rw-r--r--  1 root root  5763 Aug 25 11:09 ipv6_neighbor.rb
-rw-r--r--  1 root root  5747 Aug 25 11:09 ipv6_neighbor_router_advertisement.rb
-rw-r--r--  1 root root 12986 Aug 25 11:09 udp_probe.rb
-rw-r--r--  1 root root 11957 Aug 25 11:09 udp_sweep.rb
```

- Portscan

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary/scanner/portscan# ll
total 28
drwxr-xr-x  2 root root 4096 Sep  5 09:14 ./
drwxr-xr-x 76 root root 4096 Sep  5 09:14 ../
-rw-r--r--  1 root root 3949 Aug 25 11:09 ack.rb
-rw-r--r--  1 root root 2661 Aug 25 11:09 ftpbounce.rb
-rw-r--r--  1 root root 3787 Aug 25 11:09 syn.rb
-rw-r--r--  1 root root 3268 Aug 25 11:09 tcp.rb
-rw-r--r--  1 root root 3980 Aug 25 11:09 xmas.rb
```

Metasploitable 3

- 对靶机Metasploitable 3进行扫描
  - 防火墙关闭
    - 端口
    - OS
    - 漏洞
  - 防火墙打开
    - 端口
    - OS
    - 漏洞
  - 总结分析扫描结果


Thank You!