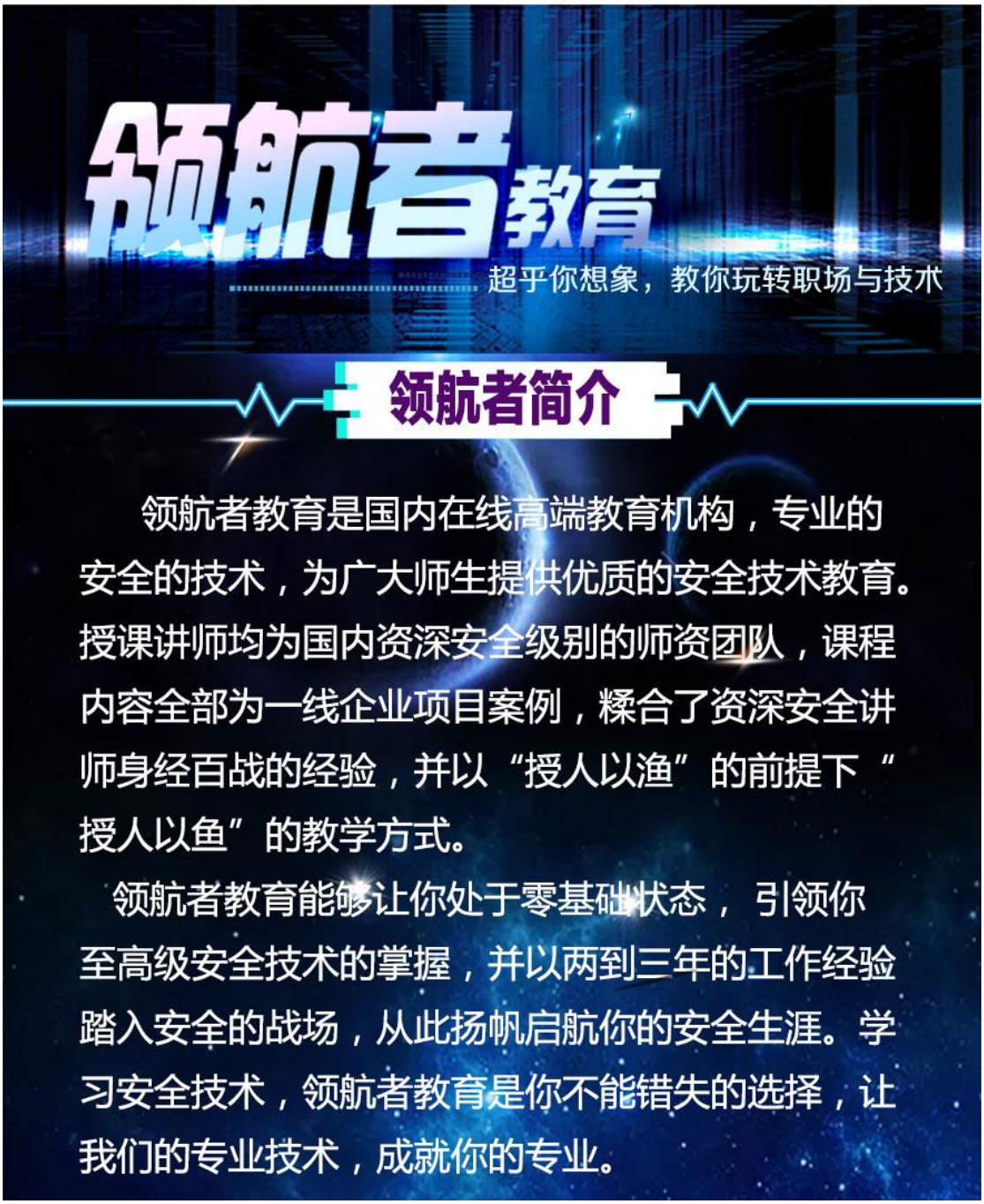


免责声明：

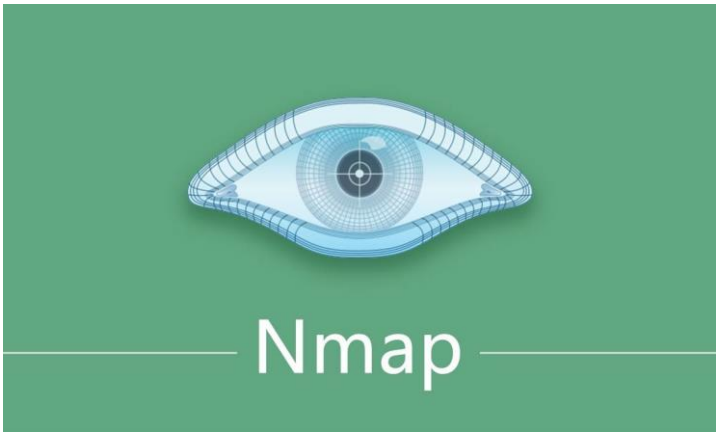
为了共同创建文明、和谐、合法网络空间，本课程内容仅限于安全教学，不得用于其他用途。所有利用本课程内容从事的违法犯罪活动，都严重违背了课程设计的初衷，均属使用者的个人行为。所有因此造成的法律问题，与领航者教育平台及讲师无关，领航者及讲师不为此承担任何法律责任。倡导网络安全，维护网络安全人人有责。

第五章-Nmap 诸神之眼

本章内容概括：

1.1 NMAP 简介
1.2 NMAP 基本参数
1.3 图形界面 zenmap 的高级使用技巧
1.4 NMAP 绕过防火墙
1.5 NMAP 脚本扫描

1.1 NMAP 简介



Nmap 是一款用于网络发现和安全审计的网络安全工具，它是自由软件。软件名字 Nmap 是 Network Mapper 的简称。通常情况下，Nmap 用于： 列举网络主机清单 管理服务升级调度 监控主机 服务运行状况 Nmap 可以检测目标主机是否在线、端口开放情况、侦测运行的服务类型及版本信息、侦测操作系统与设备类型等信息。

nmap 支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp 代理(bounce 攻击)、反向标志、ICMP、FIN、ACK 扫描、圣诞树(Xmas Tree)、SYN 扫描和 null 扫描。还可以探测操作系统类型。

总结：Nmap 是目前最流行的端口扫描类工具，开源软件，被集成于 Kali，官网 nmap.org

1. nmap 常规扫描

```
root@kali:~# nmap 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-30 11:06 CST
Nmap scan report for 192.168.1.100
Host is up (0.00043s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

3306/tcp open mysql
MAC Address: 48:5F:99:83:AB:AF (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds

2. -v 参数 #扫描服务器，显示它打开的端口及扫描详细信息
root@kali:~# nmap -v 192.168.1.106
Starting Nmap 7.70 (https://nmap.org) at 2019-10-30 11:21 CST
Initiating ARP Ping Scan at 11:21
Scanning 192.168.1.100 [1 port]
Completed ARP Ping Scan at 11:21, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:21
Completed Parallel DNS resolution of 1 host. at 11:21, 6.57s elapsed
Initiating SYN Stealth Scan at 11:21
Scanning 192.168.1.100 [1000 ports]
Discovered open port 3306/tcp on 192.168.1.100
Discovered open port 80/tcp on 192.168.1.100
Discovered open port 445/tcp on 192.168.1.100
Discovered open port 139/tcp on 192.168.1.100
Discovered open port 135/tcp on 192.168.1.100
Completed SYN Stealth Scan at 11:21, 4.73s elapsed (1000 total ports)
Nmap scan report for 192.168.1.100
Host is up (0.00042s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
MAC Address: 48:5F:99:83:AB:AF (Unknown)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.46 seconds
Raw packets sent: 1998 (87.896KB) | Rcvd: 8 (336B)

3. -p 参数，扫描服务器端口指定的一个范围： 例如端口 1-200
root@kali:~# nmap -p 1-200 192.168.1.100
Starting Nmap 7.70 (https://nmap.org) at 2019-10-30 11:27 CST
Nmap scan report for 192.168.1.100
Host is up (0.00039s latency).
Not shown: 197 filtered ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn

MAC Address: 48:5F:99:83:AB:AF (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 9.16 seconds

4. -O 参数，扫描服务器，查看此服务器的操作系统类型。
root@kali:~# nmap -O 192.168.1.106
Starting Nmap 7.70 (https://nmap.org) at 2019-10-30 11:52 CST
Nmap scan report for 192.168.1.106
Host is up (0.0010s 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
49158/tcp open unknown
MAC Address: 00:0C:29:35:53:89 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 9.36 seconds

5. -A 参数，指的是 ALL 所有信息
root@kali:~# nmap -A 192.168.1.106
Starting Nmap 7.70 (https://nmap.org) at 2019-11-17 19:05 CST
Nmap scan report for 192.168.1.106
Host is up (0.00061s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 0.7.63
|_http-server-header: nginx/0.7.63
|_http-title: DCN-WAF\xD5\xFE\xB8\xAE\xCD\xF8\xCA\xD7\xD2\xB3
3306/tcp open mysql MySQL (unauthorized)
MAC Address: 00:0C:29:35:53:89 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1

closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows 8.1 R1, 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

TRACEROUTE
HOP RTT ADDRESS
1 0.61 ms 192.168.1.106

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

扩展：traceroute 追踪路由

例 1：查找一个网段内所有机器的操作系统类型
root@kali:~# nmap -O 192.168.1.0/24

例 2：随机扫描，延时扫描，达到隐藏自己的效果
--randomize-hosts # 随机扫描
--scan-delay #延时扫描,单位秒
root@kali:~# nmap --randomize-hosts --scan-delay 5 192.168.1.100-106
Starting Nmap 7.70 (https://nmap.org) at 2019-10-30 12:11 CST
Nmap scan report for 192.168.1.100
Host is up (0.00025s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
MAC Address: 48:5F:99:83:AB:AF (Unknown)
Nmap scan report for 192.168.1.102

Host is up (0.0000040s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
Nmap done: 6 IP addresses (2 hosts up) scanned in 18.51 seconds

扩展：假如你是做安全维护工作的，用 NMAP 扫描到未知的端口打开了，你应该怎么办？
直接把端口关掉

root@piloteer101:~# lsof -i :22 #查询端口由哪个进程监听

root@piloteer101:~# ps aux |grep sshd #可以查找相关的程序更多信息，包括进程所以在的文件路径

root@piloteer101:~# kill -9 722 #杀死进程，使用 PID 来进行杀死，-9 表示强制
或者：
root@piloteer101:~# killall sshd #killall 命令杀死所有进程包括子进程，使用时需要加入进程名称

root@piloteer101:~# which sshd #查看程序所在的路径
/usr/sbin/sshd
或者
root@piloteer101:~# find / -name sshd

1.3 图形界面 zenmap 的高级使用技巧

1.3.1zenmap 介绍

Zenmap 是经典端口漏洞扫描工具 NMap 的官方 GUI(图形界面)版本，集通过 tcp/ip 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 PING 侦测下属的主机、欺骗扫描、端口过滤探测、直接的 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述等多种功能为一体，是目前为止使用最广的端口扫描工具之一。可以检测活在网络上的主机、检测主机上开放的端口、检测到相应的端口的软件和版本以及扫描端口的安全漏洞。

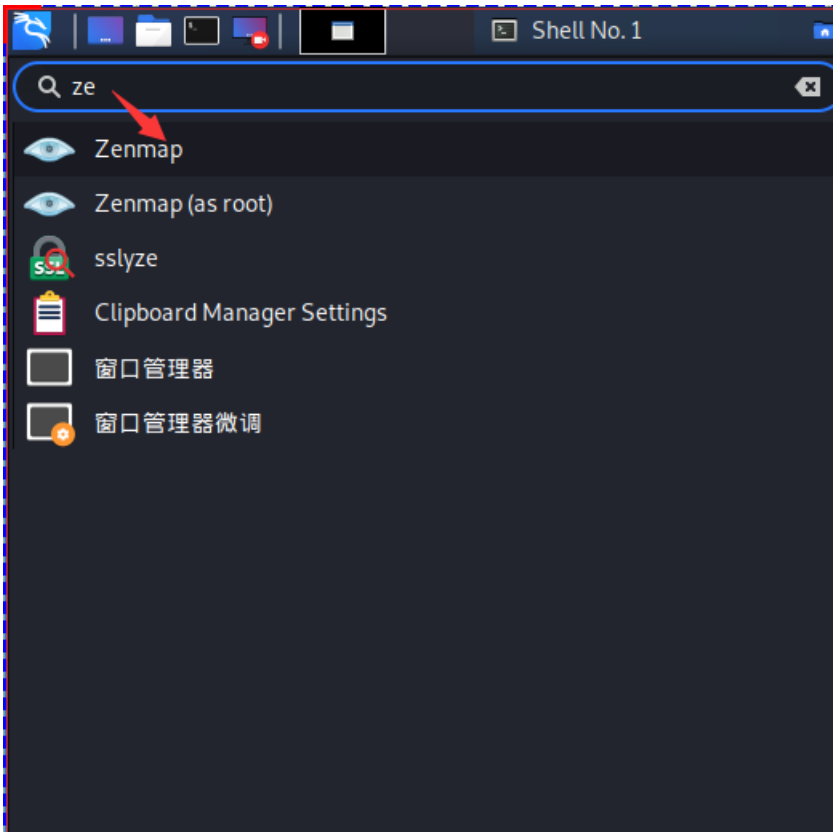
与命令行操作方式的 NMap 相比，虽然 Zenmap 的操作方式更为直观简单，但是高手们还是习惯用命令行的 NMap，当然，如果你不是大神，那么 Zenmap 更适合你。

下载 zenmap 程序，官方仅提供了 rpm 包，下载后需要转换为 deb 包
root@piloteer101:~# wget https://nmap.org/dist/zenmap-7.80-1.noarch.rpm

root@piloteer101:~# apt -y install alien #下载 deb 包转换工具

root@piloteer101:~# alien zenmap-7.80-1.noarch.rpm #把 rpm 包转为 deb
zenmap_7.80-2_all.deb generated

root@piloteer101:~# dpkg -i zenmap_7.80-2_all.deb #安装



第一种：Intense scan

(nmap -T4 -A -v)

一般来说，Intense scan 可以满足一般扫描

-T4 加快执行速度， 范围(0-5) (higher is faster)

-A 操作系统及版本探测

-v 显示详细的输出

第二种：Intense scan plus UDP
(nmap -sS -sU -T4 -A -v)
即 UDP 扫描
-sS TCP SYN 扫描
-sU UDP 扫描

第三种：Intense scan,all TCP ports
(nmap -p 1-65536 -T4 -A -v)
扫描所有端口，范围在 1-65535，试图扫描所有端口的开放情况，速度比较慢。
-p 指定端口扫描范围

第四种：Intense scan,no ping
(nmap -T4 -A -v -Pn)
非 ping 扫描
-Pn 非 ping 扫描

第五种：Ping scan
(nmap -sn)
Ping 扫描
优点：速度快。
缺点：容易被防火墙屏蔽，导致无扫描结果
-sn ping 扫描

第六种：Quick scan
(nmap -T4 -F)
快速的扫描
-F 快速模式

第七种：Quick scan plus
(nmap -sV -T4 -O -F --version-light)
快速扫描加强模式
-sV 探测端口及版本服务信息。
-O 开启服务器版本检测
--version-light 设定侦测等级为 2。

第八种：Quick traceroute
(nmap -sn --traceroute)
路由跟踪
-sn Ping 扫描，关闭端口扫描
-traceroute 显示本机到目标的路由节点。

第九种：Regular scan

常规扫描

第十种：Slow comprehensive scan
(nmap -sS -sU -T4 -A -v -PE -PP -PS80,443,-PA3389,PU40125 -PY -g 53 --script all)
慢速全面扫描

-PY 简单的控制传输协议
-g 指定源端口号

1.4 NMAP 防火墙

端口的状态：
open，端口开放；
filtered，端口被防火墙或安全软件阻止了，也可能是网络堵塞；
closed，端口关闭。

-PS 选项来实施 TCP SYN ping 可绕过防火墙
-PA 这种类型的扫描将只会扫描 ACK 包，可绕过防火墙
-PU 扫描只会对目标进行 udp ping 扫描。这种类型的扫描会发送 UDP 包来获取一个响应，可绕过防火墙
-PP 选项进行一个 ICMP 时间戳 ping 扫描，可绕过防火墙
-PE 参数进行一个 IEMP(Internet 控制报文协议)在指定的系统上输出 ping，可绕防火墙
-Pn 不采用 ping 方式进行扫描，可绕过防火墙。
-sA 用于发现防火墙规则，比如扫到的端口是过滤的，那么可以使用这个参数进行绕过。

可以在 windows 或者 linux 系统上启动防火墙，把某个端口禁止，然后再使用 nmap 进行测试

1.5 Nmap 脚本渗透测试

在 Nmap 安装目录下的 scripts 文件夹里存放了许多以“.nse”后缀结尾的文本文件，这些就是 Nmap 自带的脚本引擎。使用 Nmap Script 时，需要添加参数“--script=脚本名称”。

Nmap 脚本路径：root@kali:cd /usr/share/nmap/scripts/

```
root@kali:/usr/share/nmap/scripts# ls
acarsd-info.nse                         ip-forwarding.nse
address-info.nse                        ip-geolocation-geoplugin.nse
afp-brute.nse                           ip-geolocation-ipinfodb.nse
afp-ls.nse                              ip-geolocation-map-bing.nse
afp-path-vuln.nse                       ip-geolocation-map-google.nse
afp-serverinfo.nse                      ip-geolocation-map-kml.nse
afp-showmount.nse                       ip-geolocation-maxmind.nse
ajp-auth.nse                            ip-https-discover.nse
ajp-brute.nse                           ipidseq.nse
ajp-headers.nse                         ipmi-brute.nse
ajp-methods.nse                         ipmi-cipher-zero.nse
ajp-request.nse                         ipmi-version.nse
allseeingeye-info.nse                   ipv6-multicast-mld-list.nse
amqp-info.nse                           ipv6-node-info.nse
asn-query.nse                           ipv6-ra-flood.nse
auth-owners.nse                         irc-botnet-channels.nse
auth-spoof.nse                          irc-brute.nse
backorifice-brute.nse                   irc-info.nse
backorifice-info.nse                    irc-sasl-brute.nse
bacnet-info.nse                         irc-unrealircd-backdoor.nse
banner.nse                              iscsi-brute.nse
bitcoin-getaddr.nse                     iscsi-info.nse
bitcoin-info.nse                        isns-info.nse
```

IP 地址信息收集：

root@kali:~# nmap --script ip-geolocation-* ke.qq.com

DNS 信息收集：

root@kali:~# nmap --script dns-brute ke.qq.com

检索系统信息：

root@kali:~# nmap --script membase-http-info.nse ke.qq.com

系统常见漏洞扫描：

root@kali:~# nmap --script smb- vuln-* ke.qq.com

web 常见漏洞扫描：

http-sql-injection.nse 脚本扫描注入漏洞

http-vuln-cve2017-8917.nse 脚本 cms 注入漏洞

root@kali:~# nmap --script http-vuln-* ke.qq.com

mysql 数据库渗透测试：

mysql-brute.nse 脚本暴力破解 mysql

mysql-info.nse 脚本 mysql 详细信息

root@kali:~# nmap -p 3306 --script mysql-info.nse 192.168.1.206

课后作业：

使用 nmap 脚本扫描任意一台主机是否存在 CVE-2014-0160 漏洞