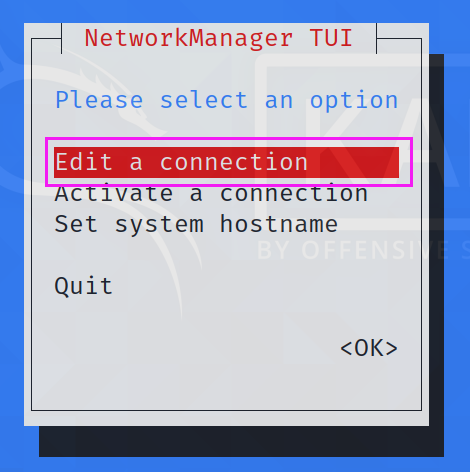
1. NMAP扫描

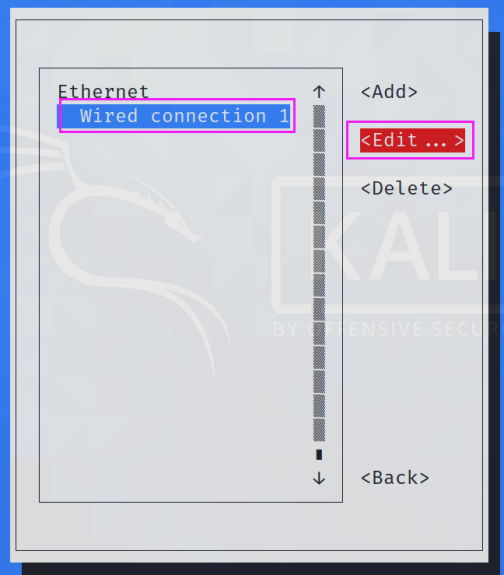
P1 配置Kali虚拟机网络

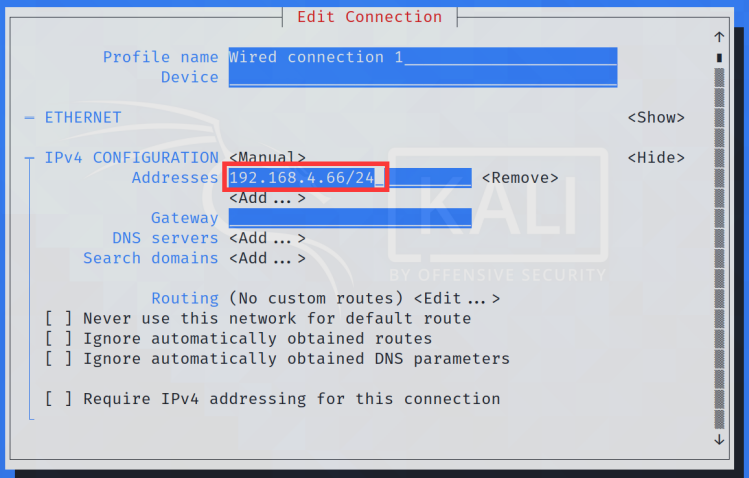
配置Kali虚拟机IP地址，建议使用nmtui命令

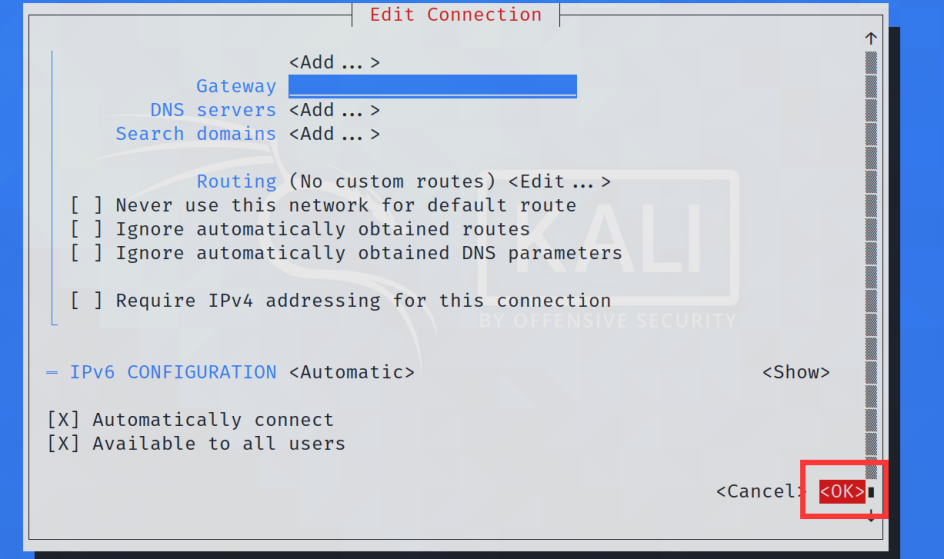
┌──(kali㉿kali)-[~]

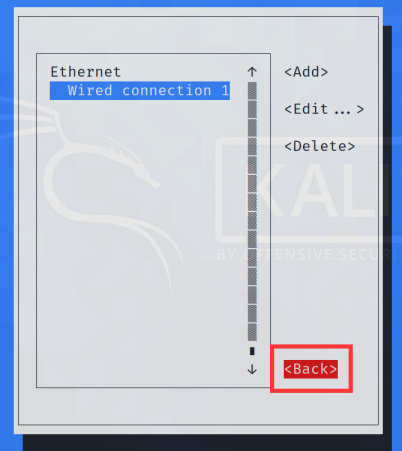
└─$ sudo nmtui

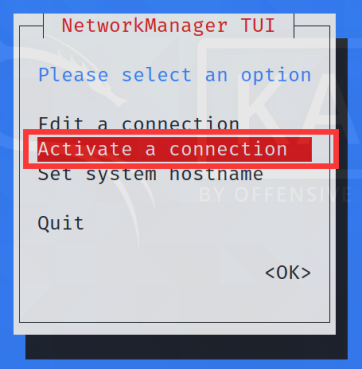




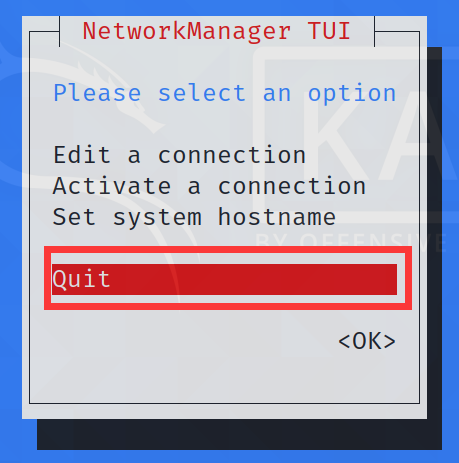


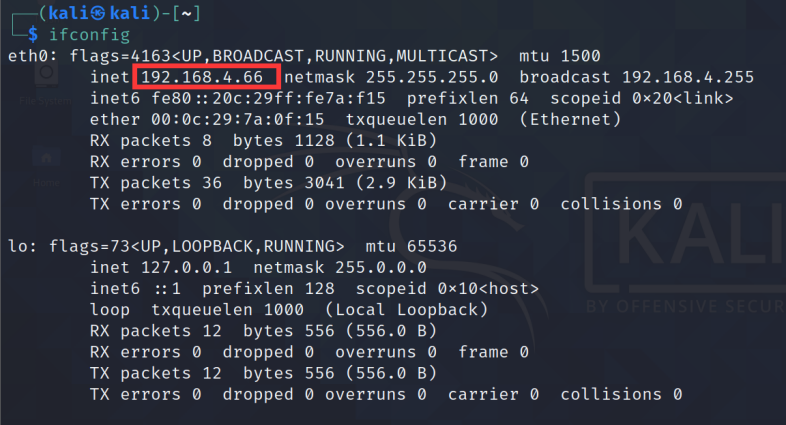


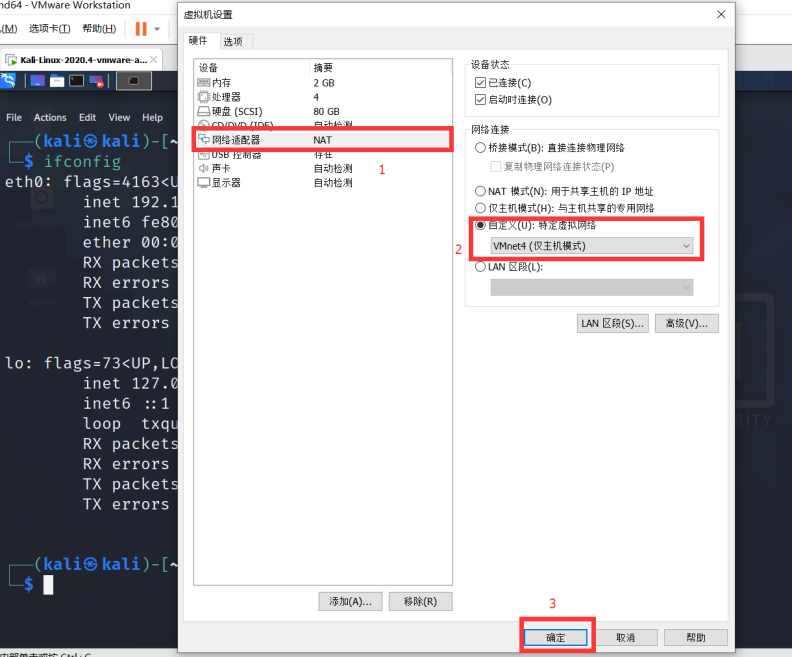


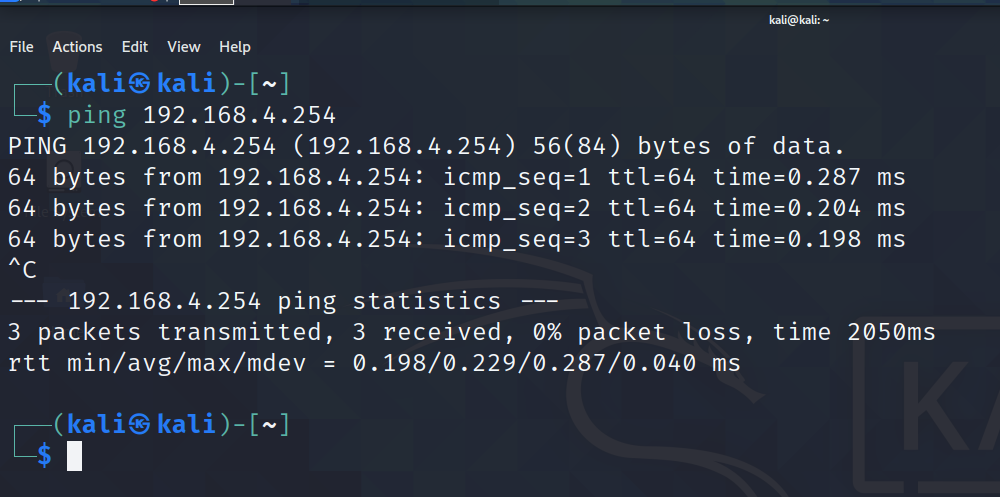












P2 使用NMAP做常规扫描

通过nmap扫描，检查指定主机开放了哪些端口，不指定使用扫描类型，默认是-sT，TCP全开扫描

┌──(kali㉿kali)-[~]

└─$ sudo nmap 192.168.4.11

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:22 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.000058s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

9100/tcp open jetdirect

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

也可以加上-sT选择，指定使用全开扫描

┌──(kali㉿kali)-[~]

└─$ sudo nmap -sT 192.168.4.11

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:25 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.0010s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

9100/tcp open jetdirect

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

使用-sS ，TCP半开扫描，最终的结果是和全开扫描是一样的，只不过工作过程不一样

┌──(kali㉿kali)-[~]

└─$ sudo nmap -sS 192.168.4.11

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:27 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.000054s latency).

Not shown: 997 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

9100/tcp open jetdirect

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

使用-sU，UDP扫描，UDP扫描是面向非链接的，很有可能我们去扫描主机，主机没有回应，或者主机断网了，那这个时候我们就会一直的去扫描，直到超时为止，才会结束扫描，所以UDP扫描是非常慢的，需要等待很长时间才可以扫描完成

┌──(kali㉿kali)-[~]

└─$ sudo nmap -sU 192.168.4.11

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:31 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 1.65% done; ETC: 12:34 (0:02:59 remaining)

Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 2.08% done; ETC: 12:35 (0:04:42 remaining)

Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 3.38% done; ETC: 12:36 (0:04:46 remaining)

Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan

UDP Scan Timing: About 4.25% done; ETC: 12:35 (0:04:30 remaining)

使用-sP，可以做ping扫描，用于检查某个机器或者某个网段的主机是否可以通信，或者是否已经开机

┌──(kali㉿kali)-[~]

└─$ sudo nmap -sP 192.168.4.0/24 130 ⨯

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:32 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.000087s latency).

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap scan report for 192.168.4.254

Host is up (0.00018s latency).

MAC Address: 00:50:56:C0:00:04 (VMware)

Nmap scan report for 192.168.4.66

Host is up.

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.99 seconds

使用-A全面扫描，可以对目标主机做全面分析，可以扫描对方服务软件的版本、系统的版本、服务上共享的数据是什么、路由跟踪等等

在这里，我们可以在node1主机上安装vsftpd软件，然后在/var/ftp目录下创建一个a.txt和b.txt，然后启动vsftpd服务，用kali系统做测试

┌──(kali㉿kali)-[~]

└─$ sudo nmap -A 192.168.4.11

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:35 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.0015s latency).

Not shown: 997 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.2

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| -rw-r--r-- 1 0 0 0 Jul 10 16:19 a.txt

| -rw-r--r-- 1 0 0 0 Jul 10 16:19 b.txt

|\_drwxr-xr-x 2 0 0 6 Aug 03 2017 pub

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.4.66

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPd 3.0.2 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 23:89:84:3a:ec:84:40:8b:a1:3e:f2:7b:35:4c:13:21 (RSA)

| 256 f0:67:85:fe:61:20:b4:3f:22:88:2a:77:e1:b6:db:70 (ECDSA)

|\_ 256 c1:17:88:d7:98:ea:03:ff:1e:a0:38:68:ef:00:76:3a (ED25519)

9100/tcp open jetdirect?

MAC Address: 00:0C:29:94:E7:9D (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: OS: Unix

TRACEROUTE

HOP RTT ADDRESS

1 1.54 ms 192.168.4.11

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 2.44 seconds

P3 使用NMAP做脚本扫描

nmap自带很多脚本，这些脚本都存放在/usr/share/nmap/scripts目录下

我们可以使用这些脚本对对目标主机做暴力破解、渗透测试、检查漏洞等等

使用nmap对目标主机的ftp服务做脚本扫描，测试FTP服务是否可以匿名访问

┌──(kali㉿kali)-[~]

└─$ sudo nmap --script=ftp-anon.nse 192.168.4.11 -p 21

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:39 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.00020s latency).

PORT STATE SERVICE

21/tcp open ftp

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| -rw-r--r-- 1 0 0 0 Jul 10 16:19 a.txt

| -rw-r--r-- 1 0 0 0 Jul 10 16:19 b.txt

|\_drwxr-xr-x 2 0 0 6 Aug 03 2017 pub

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

使用nmap脚本检查目标主机的FTP服务的软件信息

┌──(kali㉿kali)-[~]

└─$ sudo nmap -script=ftp-syst.nse 192.168.4.11 -p 21

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:45 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.00015s latency).

PORT STATE SERVICE

21/tcp open ftp

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:192.168.4.66

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPd 3.0.2 - secure, fast, stable

|\_End of status

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

使用nmap脚本检测目标主机FTP服务有没有漏洞，有没有后门

┌──(kali㉿kali)-[~]

└─$ sudo nmap -script=ftp-vsftpd-backdoor.nse 192.168.4.11 -p 21

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:46 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.00017s latency).

PORT STATE SERVICE

21/tcp open ftp

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds

如果目标主机ftp服务没有允许匿名访问，必须要有用户名才能访问，这个时候，可以使用脚本的字典进行暴力破解用户和密码，这个过程需要很长的时间，一时之间无法破解完成

┌──(kali㉿kali)-[~]

└─$ sudo nmap -script=ftp-brute.nse 192.168.4.11 -p 21

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:48 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 0.00% done

Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 0.00% done

Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 0.00% done

使用nmap脚本对ssh服务做暴力破解，因为ssh服务都是需要用户名和密码的，如果我们不知道用户名和密码，这个时候就可以使用nmap脚本通过字典文件不断的尝试和破解，我们也可以自己准备一个常见的用户字典文件或者密码字典文件，用于密码破解也是可以的

我们可以在node上创建一个用户tom，密码123456，用于测试：

┌──(kali㉿kali)-[~]

└─$ sudo nmap --script=ssh-brute.nse 192.168.4.11 -p 22 #使用nmap自身的字典文件进行暴力破解

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 12:58 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

NSE: [ssh-brute] Trying username/password pair: root:root

NSE: [ssh-brute] Trying username/password pair: admin:admin

NSE: [ssh-brute] Trying username/password pair: administrator:administrator

NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin

NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin

NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin

NSE: [ssh-brute] Trying username/password pair: guest:guest

NSE: [ssh-brute] Trying username/password pair: user:user

NSE: [ssh-brute] Trying username/password pair: web:web

NSE: [ssh-brute] Trying username/password pair: test:test

NSE: [ssh-brute] Trying username/password pair: root:

NSE: [ssh-brute] Trying username/password pair: admin:

┌──(kali㉿kali)-[~]

└─$ sudo vim /tmp/users.lst #自定义用户字典文件

root

tom

┌──(kali㉿kali)-[~]

└─$ vim /tmp/pass.lst #自定义密码字典文件

123456

654321

┌──(kali㉿kali)-[~]

└─$ sudo nmap --script=ssh-brute.nse --script-args userdb=/tmp/users.lst,passdb=/tmp/pass.lst 192.168.4.11 -p 22 #使用自定义的字典文件暴力破解

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 13:05 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

NSE: [ssh-brute] Trying username/password pair: root:root

NSE: [ssh-brute] Trying username/password pair: tom:tom

NSE: [ssh-brute] Trying username/password pair: root:123456

NSE: [ssh-brute] Trying username/password pair: tom:123456

NSE: [ssh-brute] Trying username/password pair: root:654321

Nmap scan report for 192.168.4.11

Host is up (0.00015s latency).

PORT STATE SERVICE

22/tcp open ssh

| ssh-brute:

| Accounts:

| tom:123456 - Valid credentials

|\_ Statistics: Performed 5 guesses in 2 seconds, average tps: 2.5

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds

在访问网站的时候，我们给web服务器发送请求，可以有很多访问的方法，在这里我们可以用nmap去扫描检测web服务器支持的的访问方法有哪些

我们可以在node1上安装httpd软件，创建/var/www/html/index.html首页，网页内容是 “hello world”，然后启动httpd服务，用nmap测试

┌──(kali㉿kali)-[~]

└─$ sudo nmap --script=http-methods.nse 192.168.4.11 -p 80 #扫描web服务支持哪些请求方法

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 13:12 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.00016s latency).

PORT STATE SERVICE

80/tcp open http

| http-methods:

| Supported Methods: GET HEAD POST OPTIONS TRACE

|\_ Potentially risky methods: TRACE

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

使用nmap检测web服务器是否有SQL注入的风险，一般静态页面无法SQL注入，但是如果是动态页面，就需要注意动态页面中的代码是否合理，是否有漏洞，是否有bug，如果有，就有可能被SQL注入，攻击我们的服务器

┌──(kali㉿kali)-[~]

└─$ sudo nmap --script=http-sql-injection.nse 192.168.4.11 -p 80

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-10 13:13 EDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.4.11

Host is up (0.00013s latency).

PORT STATE SERVICE

80/tcp open http

MAC Address: 00:0C:29:94:E7:9D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

使用john工具根据已知的密文反向破解成明文数据，默认john也会有自己的字典文件，去傻瓜式破解密文，但如果密文特别复杂，字典文件可能无法破解，这个时候我们也可以让john进行暴力破解，我们也可以自己创建一个字典文件，用于破解

┌──(kali㉿kali)-[~]

└─$ sudo john --single /etc/shadow #使用自带的字典文件傻瓜式破解

Using default input encoding: UTF-8

Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])

Cost 1 (iteration count) is 5000 for all loaded hashes

Will run 4 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status

kali (kali)

1g 0:00:00:00 DONE (2021-07-10 13:18) 100.0g/s 800.0p/s 800.0c/s 800.0C/s kali..kali99

Use the "--show" option to display all of the cracked passwords reliably

Session completed

┌──(kali㉿kali)-[~]

└─$ sudo john --show /etc/shadow #破解以后，可以使用--show查看破解的结果

kali:kali:18583:0:99999:7:::

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]

└─$ sudo john /etc/shadow #暴力破解

Using default input encoding: UTF-8

Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])

No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]

└─$ sudo vim /a.txt

kali

12345

root

┌──(kali㉿kali)-[~]

└─$ sudo john --wordlist=/a.txt /etc/shadow #使用自己编写的字典文件破解

Using default input encoding: UTF-8

Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])

No password hashes left to crack (see FAQ)

二、tcpdump数据抓包

P1 抓取FTP服务数据包

数据抓包，抓取ftp用户名和密码

node1搭建FTP服务器

[root@node1 ~]# yum -y install vsftpd

[root@node1 ~]# useradd jerry

[root@node1 ~]# echo 123456 | passwd --stdin jerry

[root@node1 ~]# echo AAA > /home/jerry/hello.txt

[root@node1 ~]# echo BBB > /home/jerry/world.txt

[root@node1 ~]# systemctl restart vsftpd

使用kali系统进行抓包

┌──(kali㉿kali)-[~]

└─$ sudo tcpdump -A host 192.168.4.11 and tcp port 21

在kali系统上再开一个终端，使用jerry用户访问node1的ftp服务，然后在kali抓包界面上验证查看，可以看到明文的密码

┌──(kali㉿kali)-[~]

└─$ sudo ftp 192.168.4.11

Connected to 192.168.4.11.

220 (vsFTPd 3.0.2)

Name (192.168.4.11:kali): jerry #用户名

331 Please specify the password.

Password: #密码

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls #可以看到jerry用户家目录下的内容

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

-rw-r--r-- 1 0 0 4 Jul 10 18:14 hello.txt

-rw-r--r-- 1 0 0 4 Jul 10 18:14 world.txt

226 Directory send OK.

P2 抓取Nginx服务数据包

抓取Nginx web服务器用户名和密码

在node1源码安装nginx，增加用户认证，访问用户名jerry，密码654321

[root@node1 ~]# tar -xf lnmp\_soft.tar.gz

[root@node1 ~]# cd lnmp\_soft/

[root@node1 lnmp\_soft]# tar -xf nginx-1.16.1.tar.gz

[root@node1 lnmp\_soft]# cd nginx-1.16.1

[root@node1 nginx-1.16.1]# yum -y install gcc pcre-devel openssl-devel

[root@node1 nginx-1.16.1]# ./configure

[root@node1 nginx-1.16.1]# make && make install

[root@node1 nginx-1.16.1]# vim /usr/local/nginx/conf/nginx.conf

server {

listen 80;

server\_name localhost;

auth\_basic "message";

auth\_basic\_user\_file "/usr/local/nginx/pass";

[root@node1 nginx-1.16.1]# /usr/local/nginx/sbin/nginx

[root@node1 nginx-1.16.1]# yum -y install httpd-tools

[root@node1 nginx-1.16.1]# htpasswd -c /usr/local/nginx/pass jerry

在kali系统上抓取访问数据包并保存在文件中

真机浏览器访问4.11 nginx的网页，并输入用户名密码

┌──(kali㉿kali)-[~]

└─$ sudo tcpdump -A -w web.cap host 192.168.4.11 and tcp port 80

真机浏览器访问并输入用户名密码

http:// 192.168.4.11

在kali系统上查看抓取的数据包文件，可以获取到编码的用户名和密码，我们解码就可以看到用户和密码的内容

┌──(kali㉿kali)-[~]

└─$ sudo cat web.cap #找到Authorization: Basic字样

使用base64进行解码

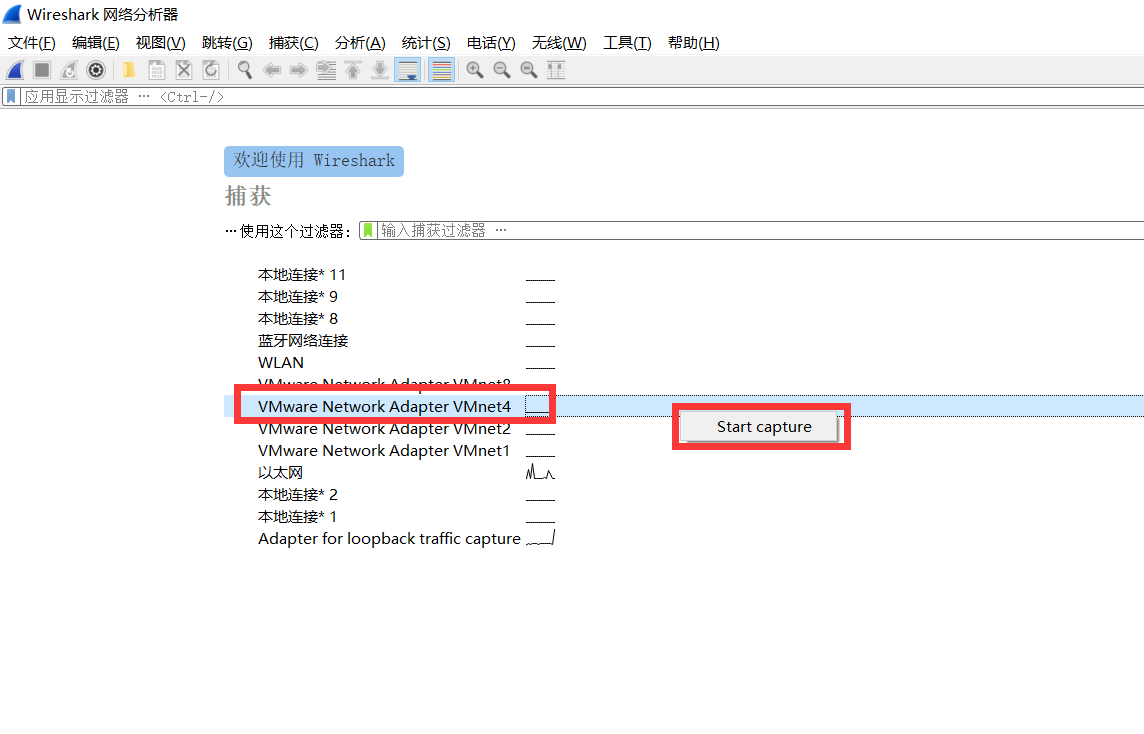
┌──(kali㉿kali)-[~]

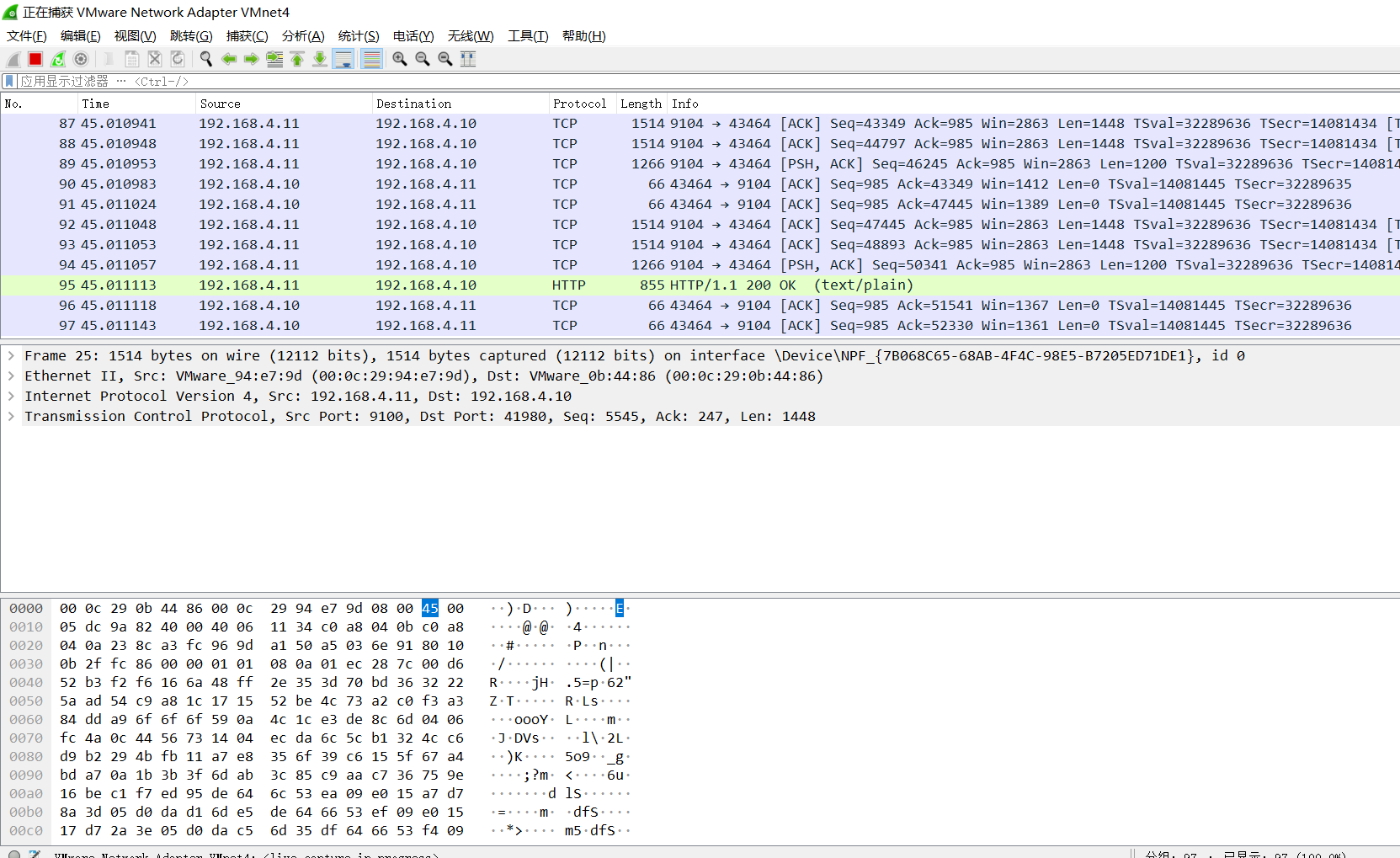
└─$ sudo echo amVycnk6NjU0MzIx | base64 -d

jerry:654321

P3 查看Wireshark抓取的数据包

选择一张网卡，右击选择start capture，查看数据包信息





三、linux基本防护

P1 用户账号安全

修改用户dachui的账户属性，设置为2029-10-01日失效

[root@node1 ~]# useradd dachui

[root@node1 ~]# chage -l dachui #查看用户的有效期

…

帐户过期时间 ：从不

[root@node1 ~]# chage -E 2029-10-01 dachui

[root@node1 ~]# chage -l dachui

…

帐户过期时间 ：10月 01, 2029

…

[root@node1 ~]# chage -E -1 dachui #取消有效期

[root@node1 ~]# chage -l dachui

……

帐户过期时间 ：从不

……

修改密码，并测试登录，成功

[root@node1 ~]# echo a | passwd --stdin dachui

[root@node1 ~]# ssh dachui@127.0.0.1

[dachui@node1 ~]$ exit

使用户登录使立刻修改密码

[root@node1 ~]# chage -d 0 dachui #设置密码立即过期

[root@node1 ~]# ssh dachui@127.0.0.1

dachui@127.0.0.1's password: #输入密码

……

Changing password for dachui.

(current) UNIX password: #输入旧密码

New password: #输入新密码，符合复杂度，taren123

Retype new password: #再次输入taren123

passwd: all authentication tokens updated successfully.

Connection to 127.0.0.1 closed.

[root@node1 ~]# ssh dachui@127.0.0.1 #登录，成功

账号的锁定/解锁

使用passwd命令 -l锁定、 -u解锁、-S查看状态

[root@node1 ~]# passwd -S dachui #查看状态

dachui PS 2020-09-17 0 99999 7 -1 (Password set, SHA512 crypt.)

[root@node1 ~]# passwd -l dachui #锁定用户

Locking password for user dachui.

passwd: Success

[root@node1 ~]# passwd -S dachui

dachui LK 2020-09-17 0 99999 7 -1 (Password locked.) #locked锁定

测试，登录用户

[root@node1 ~]# ssh dachui@127.0.0.1 #失败

[root@node1 ~]# passwd -u dachui #解锁

[root@node1 ~]# ssh dachui@127.0.0.1 #登录成功

强制定期修改密码

[root@node1 ~]# vim /etc/login.defs

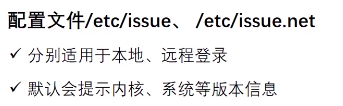
PASS\_MAX\_DAYS 60 #最长有效期时间，只会对后面创建的用户生效

PASS\_MIN\_DAYS 0 #最短有效期时间

PASS\_WARN\_AGE 7 #密码过期之前，提前几天发送信息

P2 伪装登陆提示

伪装登录提示



账户在登录Linux系统时，默认会显示登陆信息（包括操作系统内核信息）

/etc/issue这个配置文件里保存的就是这些登陆信息，修改该文件防止内核信息泄露。

此刻直接用虚拟系统管理器登录打开node1

[root@node1 ~]# vim /etc/issue

Welcome to Tedu.

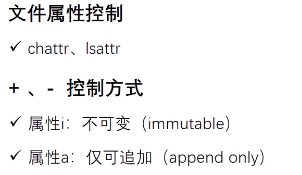
[root@node1 ~]# exit

logout

Welcome to Tedu.

node1 login:

P3 锁定/解锁保护文件



新建文件,并查看文件特殊属性

[root@node1 ~]# vim test.sh

hello the world

ni hao.

[root@node1 ~]# lsattr test.sh

---------------- test.sh

使用+i锁定文件，使用lsattr查看属性并操作测试

[root@node1 ~]# chattr +i test.sh

[root@node1 ~]# lsattr test.sh

[root@node1 ~]# rm test.sh

[root@node1 ~]# echo xx > test.sh

-bash: test.sh: 权限不够

[root@node1 ~]# vim test.sh #修改失败

取消i属性

[root@node1 ~]# chattr -i test.sh

使用+a锁定文件(仅可追加)，使用lsattr查看属性

[root@node1 ~]# chattr +a test.sh

[root@node1 ~]# lsattr test.sh

[root@node1 ~]# echo 123 >> test.sh

[root@node1 ~]# vim test.sh #修改失败

sdsadadahello the world

ni hao.

123

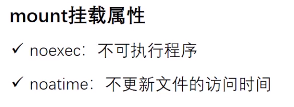
"test.sh" E212: 无法打开并写入文件

取消a属性

[root@node1 ~]# chattr -a test.sh

P4 文件系统挂载属性

文件系统挂载



给/boot分区添加noatime和noexec的属性

[root@node1 ~]# vim /etc/fstab

UUID=8333b4f6-0436-429d-9d85-b857aac28be8 /boot xfs defaults,noexec,noatime 0 0

[root@node1 ~]# mount -o remount /boot #重新挂载/boot分区

[root@node1 ~]# mount | grep /boot #查看挂载信息

[root@node1 ~]# vim /boot/test.sh

#!/bin/bash

while :

do

echo a

done

[root@node1 ~]# chmod +x /boot/test.sh

[root@node1 ~]# cd /boot/

[root@node1 boot]# ./test.sh

-bash: ./test.sh: 权限不够