#### 扫描与抓包分析

### **3.1 问题**

本案例要求熟悉Linux主机环境下的常用安全工具，完成以下任务操作：

1. 使用NMAP扫描来获取指定主机/网段的相关信息
2. 使用tcpdump分析FTP访问中的明文交换信息

### **3.2 步骤**

实现此案例需要按照如下步骤进行。

步骤一：使用NMAP扫描来获取指定主机/网段的相关信息

1）安装软件

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# yum -y install nmap
2. //基本用法：
3. # nmap [扫描类型] [选项] <扫描目标 ...>
4. //常用的扫描类型
5. // -sS，TCP SYN扫描（半开）
6. // -sT，TCP 连接扫描（全开）
7. // -sU，UDP扫描
8. // -sP，ICMP扫描
9. // -A，目标系统全面分析

[root@proxy ~]# yum -y install nmap

//基本用法：

# nmap [扫描类型] [选项] <扫描目标 ...>

//常用的扫描类型

// -sS，TCP SYN扫描（半开）

// -sT，TCP 连接扫描（全开）

// -sU，UDP扫描

// -sP，ICMP扫描

// -A，目标系统全面分析

2）检查192.168.4.100主机是否可以ping通

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -sP 192.168.4.100
2. Starting Nmap 6.40 ( http://nmap.org ) at 2018-06-06 21:59 CST
3. mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
4. Nmap scan report for host3 (192.168.4.100)
5. Host is up (0.00036s latency).
6. MAC Address: 52:54:00:71:07:76 (QEMU Virtual NIC)
7. Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

[root@proxy ~]# nmap -sP 192.168.4.100

Starting Nmap 6.40 ( http://nmap.org ) at 2018-06-06 21:59 CST

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 host3 (192.168.4.100)

Host is up (0.00036s latency).

MAC Address: 52:54:00:71:07:76 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

使用-n选项可以不执行DNS解析

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -n -sP 192.168.4.100
2. Starting Nmap 6.40 ( http://nmap.org ) at 2018-06-06 22:00 CST
3. Nmap scan report for 192.168.4.100
4. Host is up (0.00046s latency).
5. MAC Address: 52:54:00:71:07:76 (QEMU Virtual NIC)
6. Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

[root@proxy ~]# nmap -n -sP 192.168.4.100

Starting Nmap 6.40 ( http://nmap.org ) at 2018-06-06 22:00 CST

Nmap scan report for 192.168.4.100

Host is up (0.00046s latency).

MAC Address: 52:54:00:71:07:76 (QEMU Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

3）检查192.168.4.0/24网段内哪些主机可以ping通

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -n -sP 192.168.4.0/24
2. Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:01 CST
3. Nmap scan report for 192.168.4.1
4. Host is up.
5. Nmap scan report for 192.168.4.7
6. Host is up.
7. Nmap scan report for 192.168.4.120
8. Host is up (0.00027s latency).
9. MAC Address: 00:0C:29:74:BE:21 (VMware)
10. Nmap scan report for 192.168.4.110
11. Host is up (0.00016s latency).
12. MAC Address: 00:50:56:C0:00:01 (VMware)
13. Nmap scan report for 192.168.4.120
14. Host is up (0.00046s latency).
15. MAC Address: 00:0C:29:DB:84:46 (VMware)
16. Nmap done: 256 IP addresses (5 hosts up) scanned in 3.57 seconds

[root@proxy ~]# nmap -n -sP 192.168.4.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:01 CST

Nmap scan report for 192.168.4.1

Host is up.

Nmap scan report for 192.168.4.7

Host is up.

Nmap scan report for 192.168.4.120

Host is up (0.00027s latency).

MAC Address: 00:0C:29:74:BE:21 (VMware)

Nmap scan report for 192.168.4.110

Host is up (0.00016s latency).

MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.4.120

Host is up (0.00046s latency).

MAC Address: 00:0C:29:DB:84:46 (VMware)

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.57 seconds

4）检查目标主机所开启的TCP服务

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -sT 192.168.4.100
2. Starting Nmap 5.51 ( http://nmap.org ) at 2018-05-17 17:55 CST
3. Nmap scan report for 192.168.4.100
4. Host is up (0.00028s latency).
5. Not shown: 990 closed ports
6. PORT STATE SERVICE
7. 21/tcp open ftp
8. 22/tcp open ssh
9. 25/tcp open smtp
10. 80/tcp open http
11. 110/tcp open pop3
12. 111/tcp open rpcbind
13. 143/tcp open imap
14. 443/tcp open https
15. 993/tcp open imaps
16. 995/tcp open pop3s
17. MAC Address: 00:0C:29:74:BE:21 (VMware)
19. Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds

[root@proxy ~]# nmap -sT 192.168.4.100

Starting Nmap 5.51 ( http://nmap.org ) at 2018-05-17 17:55 CST

Nmap scan report for 192.168.4.100

Host is up (0.00028s latency).

Not shown: 990 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

25/tcp open smtp

80/tcp open http

110/tcp open pop3

111/tcp open rpcbind

143/tcp open imap

443/tcp open https

993/tcp open imaps

995/tcp open pop3s

MAC Address: 00:0C:29:74:BE:21 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds

5）检查192.168.4.0/24网段内哪些主机开启了FTP、SSH服务

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -p 21-22 192.168.4.0/24
2. Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:00 CST
3. Nmap scan report for 192.168.4.1
4. Host is up (0.000025s latency).
5. PORT STATE SERVICE
6. 21/tcp open ftp
7. 22/tcp open ssh
9. Nmap scan report for 192.168.4.7
10. Host is up.
11. PORT STATE SERVICE
12. 21/tcp filtered ftp
13. 22/tcp filtered ssh
15. Nmap scan report for 192.168.4.120
16. Host is up (0.00052s latency).
17. PORT STATE SERVICE
18. 21/tcp open ftp
19. 22/tcp open ssh
20. MAC Address: 00:0C:29:74:BE:21 (VMware)
22. Nmap scan report for pc110.tarena.com (192.168.4.110)
23. Host is up (0.00038s latency).
24. PORT STATE SERVICE
25. 21/tcp closed ftp
26. 22/tcp closed ssh
27. MAC Address: 00:50:56:C0:00:01 (VMware)
29. Nmap scan report for 192.168.4.120
30. Host is up (0.00051s latency).
31. PORT STATE SERVICE
32. 21/tcp closed ftp
33. 22/tcp closed ssh
34. MAC Address: 00:0C:29:DB:84:46 (VMware)
36. Nmap done: 256 IP addresses (5 hosts up) scanned in 4.88 seconds

[root@proxy ~]# nmap -p 21-22 192.168.4.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:00 CST

Nmap scan report for 192.168.4.1

Host is up (0.000025s latency).

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

Nmap scan report for 192.168.4.7

Host is up.

PORT STATE SERVICE

21/tcp filtered ftp

22/tcp filtered ssh

Nmap scan report for 192.168.4.120

Host is up (0.00052s latency).

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

MAC Address: 00:0C:29:74:BE:21 (VMware)

Nmap scan report for pc110.tarena.com (192.168.4.110)

Host is up (0.00038s latency).

PORT STATE SERVICE

21/tcp closed ftp

22/tcp closed ssh

MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.4.120

Host is up (0.00051s latency).

PORT STATE SERVICE

21/tcp closed ftp

22/tcp closed ssh

MAC Address: 00:0C:29:DB:84:46 (VMware)

Nmap done: 256 IP addresses (5 hosts up) scanned in 4.88 seconds

6）检查目标主机所开启的UDP服务

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -sU 192.168.4.100             //指定-sU扫描UDP
2. 53/udp open domain
3. 111/udp open rpcbind

[root@proxy ~]# nmap -sU 192.168.4.100 //指定-sU扫描UDP

53/udp open domain

111/udp open rpcbind

7）全面分析目标主机192.168.4.100和192.168.4.5的操作系统信息

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# nmap -A 192.168.4.100,5
3. Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:03 CST
4. Nmap scan report for 192.168.4.100                     //主机mail的扫描报告
5. Host is up (0.0016s latency).
6. Not shown: 990 closed ports
7. PORT STATE SERVICE VERSION
8. 21/tcp open ftp vsftpd 2.2.2
9. | ftp-anon: Anonymous FTP login allowed (FTP code 230)
10. | -rw-r--r-- 1 0 0 1719 Aug 17 13:33 UserB.pub
11. | -rw-r--r-- 1 0 0 122 Aug 13 05:27 dl.txt
12. | drwxr-xr-x 2 14 0 4096 Aug 13 09:07 pub
13. | -rw-rw-r-- 1 505 505 170 Aug 17 13:18 tools-1.2.3.tar.gz
14. |\_-rw-rw-r-- 1 505 505 287 Aug 17 13:22 tools-1.2.3.tar.gz.sig
15. 22/tcp open ssh OpenSSH 5.3 (protocol 2.0)
16. | ssh-hostkey: 1024 86:be:d6:89:c1:2d:d9:1f:57:2f:66:d1:af:a8:d3:c6 (DSA)
17. |\_2048 16:0a:15:01:fa:bb:91:1d:cc:ab:68:17:58:f9:49:4f (RSA)
18. 25/tcp open smtp Postfix smtpd
19. 80/tcp open http Apache httpd 2.2.15 ((Red Hat))
20. |\_http-methods: No Allow or Public header in OPTIONS response (status code 302)
21. | http-title: 302 Found
22. |\_Did not follow redirect to https://192.168.4.100//
23. 110/tcp open pop3 Dovecot pop3d
24. |\_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING STLS SASL(PLAIN)
25. 111/tcp open rpcbind
26. MAC Address: 00:0C:29:74:BE:21 (VMware)
27. No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
28. TCP/IP fingerprint:
29. OS:SCAN(V=5.51%D=8/19%OT=21%CT=1%CU=34804%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM=52
30. OS:11ED90%P=x86\_64-redhat-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I
31. OS:%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O
32. OS:5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6
33. OS:=3890)ECN(R=Y%DF=Y%T=40%W=3908%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
34. OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
35. OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
36. OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
37. OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
38. OS:N%T=40%CD=S)
40. Network Distance: 1 hop
41. Service Info: Host: mail.tarena.com; OS: Unix
43. TRACEROUTE
44. HOP RTT ADDRESS
45. 1 1.55 ms 192.168.4.100

[root@proxy ~]# nmap -A 192.168.4.100,5

Starting Nmap 5.51 ( http://nmap.org ) at 2017-05-17 18:03 CST

Nmap scan report for 192.168.4.100 //主机mail的扫描报告

Host is up (0.0016s latency).

Not shown: 990 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.2.2

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

| -rw-r--r-- 1 0 0 1719 Aug 17 13:33 UserB.pub

| -rw-r--r-- 1 0 0 122 Aug 13 05:27 dl.txt

| drwxr-xr-x 2 14 0 4096 Aug 13 09:07 pub

| -rw-rw-r-- 1 505 505 170 Aug 17 13:18 tools-1.2.3.tar.gz

|\_-rw-rw-r-- 1 505 505 287 Aug 17 13:22 tools-1.2.3.tar.gz.sig

22/tcp open ssh OpenSSH 5.3 (protocol 2.0)

| ssh-hostkey: 1024 86:be:d6:89:c1:2d:d9:1f:57:2f:66:d1:af:a8:d3:c6 (DSA)

|\_2048 16:0a:15:01:fa:bb:91:1d:cc:ab:68:17:58:f9:49:4f (RSA)

25/tcp open smtp Postfix smtpd

80/tcp open http Apache httpd 2.2.15 ((Red Hat))

|\_http-methods: No Allow or Public header in OPTIONS response (status code 302)

| http-title: 302 Found

|\_Did not follow redirect to https://192.168.4.100//

110/tcp open pop3 Dovecot pop3d

|\_pop3-capabilities: USER CAPA UIDL TOP OK(K) RESP-CODES PIPELINING STLS SASL(PLAIN)

111/tcp open rpcbind

MAC Address: 00:0C:29:74:BE:21 (VMware)

No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=5.51%D=8/19%OT=21%CT=1%CU=34804%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM=52

OS:11ED90%P=x86\_64-redhat-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I

OS:%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O

OS:5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6

OS:=3890)ECN(R=Y%DF=Y%T=40%W=3908%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O

OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=

OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%

OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(

OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=

OS:N%T=40%CD=S)

Network Distance: 1 hop

Service Info: Host: mail.tarena.com; OS: Unix

TRACEROUTE

HOP RTT ADDRESS

1 1.55 ms 192.168.4.100

步骤二：使用tcpdump分析FTP访问中的明文交换信息

1）准备Vsftpd服务器（192.168.4.5操作）

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# yum -y install vsftpd
2. [root@proxy ~]# systemctl restart vsftpd

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

[root@proxy ~]# systemctl restart vsftpd

2）启用tcpdump命令行抓包

执行tcpdump命令行，添加适当的过滤条件，只抓取访问主机192.168.4.5的21端口的数据通信 ，并转换为ASCII码格式的易读文本。

这里假设，192.168.4.5主机有vsftpd服务，如果没有需要提前安装并启动服务！！！

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 21
2. tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
3. listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
4. .. ..                                            //进入等待捕获数据包的状态
5. //监控选项如下：
6. // -i，指定监控的网络接口（默认监听第一个网卡）
7. // -A，转换为 ACSII 码，以方便阅读
8. // -w，将数据包信息保存到指定文件
9. // -r，从指定文件读取数据包信息
10. //tcpdump的过滤条件：
11. // 类型：host、net、port、portrange
12. // 方向：src、dst
13. // 协议：tcp、udp、ip、wlan、arp、……
14. // 多个条件组合：and、or、not

[root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 21

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

.. .. //进入等待捕获数据包的状态

//监控选项如下：

// -i，指定监控的网络接口（默认监听第一个网卡）

// -A，转换为 ACSII 码，以方便阅读

// -w，将数据包信息保存到指定文件

// -r，从指定文件读取数据包信息

//tcpdump的过滤条件：

// 类型：host、net、port、portrange

// 方向：src、dst

// 协议：tcp、udp、ip、wlan、arp、……

// 多个条件组合：and、or、not

3）执行FTP访问，并观察tcpdump抓包结果

从192.168.4.100访问主机192.168.4.5的vsftpd服务。

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@client ~]# yum -y install ftp
2. [root@client ~]# ftp 192.168.4.5
3. Connected to 192.168.4.200 (192.168.4.200).
4. 220 (vsFTPd 3.0.2)
5. Name (192.168.4.200:root): tom //输入用户名
6. 331 Please specify the password.
7. Password: //输入密码
8. 530 Login incorrect.
9. Login failed.
10. ftp>quit //退出

[root@client ~]# yum -y install ftp

[root@client ~]# ftp 192.168.4.5

Connected to 192.168.4.200 (192.168.4.200).

220 (vsFTPd 3.0.2)

Name (192.168.4.200:root): tom //输入用户名

331 Please specify the password.

Password: //输入密码

530 Login incorrect.

Login failed.

ftp>quit //退出

观察抓包的结果（回到porxy主机观察tcpdump抓包的结果）：

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]#
2. ... …
3. 18:47:27.960530 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 1:14, ack 21, win 65515, length 13
4. E..5..@.@......x...d.\*..G.\c.1BvP.......USER tom
5. 18:47:29.657364 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 14:27, ack 55, win 65481, length 13
6. E..5..@.@......x...d.\*..G.\p.1B.P.......PASS 123

[root@proxy ~]#

... …

18:47:27.960530 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 1:14, ack 21, win 65515, length 13

E..5..@.@......x...d.\*..G.\c.1BvP.......USER tom

18:47:29.657364 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 14:27, ack 55, win 65481, length 13

E..5..@.@......x...d.\*..G.\p.1B.P.......PASS 123

4)再次使用tcpdump抓包，使用-w选项可以将抓取的数据包另存为文件，方便后期慢慢分析。

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A -w ftp.cap \
2. > host 192.168.4.5 and tcp port 21                            //抓包并保存

[root@proxy ~]# tcpdump -A -w ftp.cap \

> host 192.168.4.5 and tcp port 21 //抓包并保存

tcpdump命令的-r选项，可以去读之前抓取的历史数据文件

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A -r ftp.cap | egrep '(USER|PASS)'    //分析数据包
2. .. ..
3. E..(..@.@.. ...x...d.\*..G.\c.1BbP.............
4. 18:47:25.967592 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 1:21, ack 1, win 229, length 20
5. E..<FJ@.@.jE...d...x...\*.1BbG.\cP...V...220 (vsFTPd 2.2.2)
6. … …
7. 18:47:27.960530 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 1:14, ack 21, win 65515, length 13
8. E..5..@.@......x...d.\*..G.\c.1BvP.......USER mickey
9. … …
10. 18:47:27.960783 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 21:55, ack 14, win 229, length 34
11. E..JFL@.@.j5...d...x...\*.1BvG.\pP...i~..331 Please specify the password.
12. … …
13. 18:47:29.657364 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 14:27, ack 55, win 65481, length 13
14. E..5..@.@......x...d.\*..G.\p.1B.P.......PASS pwd123
15. … …
16. 18:47:29.702671 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 55:78, ack 27, win 229, length 23
17. E..?FN@.@.j>...d...x...\*.1B.G.\}P.......230 Login successful.

[root@proxy ~]# tcpdump -A -r ftp.cap | egrep '(USER|PASS)' //分析数据包

.. ..

E..(..@.@.. ...x...d.\*..G.\c.1BbP.............

18:47:25.967592 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 1:21, ack 1, win 229, length 20

E..<FJ@.@.jE...d...x...\*.1BbG.\cP...V...220 (vsFTPd 2.2.2)

… …

18:47:27.960530 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 1:14, ack 21, win 65515, length 13

E..5..@.@......x...d.\*..G.\c.1BvP.......USER mickey

… …

18:47:27.960783 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 21:55, ack 14, win 229, length 34

E..JFL@.@.j5...d...x...\*.1BvG.\pP...i~..331 Please specify the password.

… …

18:47:29.657364 IP 192.168.4.5.ftp > 192.168.4.100.novation: Flags [P.], seq 14:27, ack 55, win 65481, length 13

E..5..@.@......x...d.\*..G.\p.1B.P.......PASS pwd123

… …

18:47:29.702671 IP 192.168.4.100.novation > 192.168.4.5.ftp: Flags [P.], seq 55:78, ack 27, win 229, length 23

E..?FN@.@.j>...d...x...\*.1B.G.\}P.......230 Login successful.

步骤三：扩展知识，使用tcpdump分析Nginx的明文账户认证信息信息

1）在proxy主机(192.168.4.5)准备一台需要用户认证的Nginx服务器

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# cd /usr/local/nginx/conf/
2. [root@proxy ~]# cp nginx.conf.default nginx.conf //还原配置文件
3. [root@proxy ~]# vim /usr/local/nginx/conf/nginx.conf
4. server {
5. listen 80;
6. server\_name localhost;
7. auth\_basic "xx";
8. auth\_basic\_user\_file "/usr/local/nignx/pass";
9. … …
10. [root@proxy ~]# htpasswd -c /usr/local/nginx/pass jerry //创建账户文件
11. New password:123 //输入密码
12. Re-type new password:123 //确认密码
13. [root@proxy ~]# nginx -s reload

[root@proxy ~]# cd /usr/local/nginx/conf/

[root@proxy ~]# cp nginx.conf.default nginx.conf //还原配置文件

[root@proxy ~]# vim /usr/local/nginx/conf/nginx.conf

server {

listen 80;

server\_name localhost;

auth\_basic "xx";

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

… …

[root@proxy ~]# htpasswd -c /usr/local/nginx/pass jerry //创建账户文件

New password:123 //输入密码

Re-type new password:123 //确认密码

[root@proxy ~]# nginx -s reload

2）在proxy主机使用tcpdump命令抓包

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

[root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

3)在真实机使用浏览器访问192.168.4.5

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@pc001 ~]# firefox http://192.168.4.5 //根据提示输入用户名与密码

[root@pc001 ~]# firefox http://192.168.4.5 //根据提示输入用户名与密码

4）回到proxy查看抓包的数据结果

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80
2. tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
3. listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
4. … …
5. Authorization: Basic dG9tOjEyMzQ1Ng==
6. … …

[root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

… …

Authorization: Basic dG9tOjEyMzQ1Ng==

… …

5) 查看base64编码内容

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# echo "dG9tOjEyMzQ1Ng==" | base64 -d
2. tom:123456
3. [root@proxy ~]# echo "tom:123456" | base64
4. dG9tOjEyMzQ1Ngo=

**扩展知识，使用tcpdump分析Nginx的明文账户认证信息信息**

1）在proxy主机(192.168.4.5)准备一台需要用户认证的Nginx服务器

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

# [root@proxy ~]# cd /usr/local/nginx/conf/

1. [root@proxy ~]# cp nginx.conf.default nginx.conf //还原配置文件
2. [root@proxy ~]# vim /usr/local/nginx/conf/nginx.conf
3. server {
4. listen 80;
5. server\_name localhost;
6. auth\_basic "xx";
7. auth\_basic\_user\_file "/usr/local/nignx/pass";
8. … …
9. [root@proxy ~]# htpasswd -c /usr/local/nginx/pass jerry //创建账户文件
10. New password:123 //输入密码
11. Re-type new password:123 //确认密码
12. [root@proxy ~]# nginx -s reload

[root@proxy ~]# cd /usr/local/nginx/conf/

[root@proxy ~]# cp nginx.conf.default nginx.conf //还原配置文件

[root@proxy ~]# vim /usr/local/nginx/conf/nginx.conf

server {

listen 80;

server\_name localhost;

auth\_basic "xx";

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

… …

[root@proxy ~]# htpasswd -c /usr/local/nginx/pass jerry //创建账户文件

New password:123 //输入密码

Re-type new password:123 //确认密码

[root@proxy ~]# nginx -s reload

2）在proxy主机使用tcpdump命令抓包

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

[root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

3)在真实机使用浏览器访问192.168.4.5

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@pc001 ~]# firefox http://192.168.4.5 //根据提示输入用户名与密码

[root@pc001 ~]# firefox http://192.168.4.5 //根据提示输入用户名与密码

4）回到proxy查看抓包的数据结果

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80
2. tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
3. listening on eth0, link-type **EN10MB** (Ethernet), capture size 262144 bytes
4. … …
5. Authorization: Basic dG9tOjEyMzQ1Ng==
6. … …

[root@proxy ~]# tcpdump -A host 192.168.4.5 and tcp port 80

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

… …

Authorization: Basic dG9tOjEyMzQ1Ng==

… …

5) 查看base64编码内容

[copytextpop-up](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN202001/SECURITY/DAY04/CASE/01/index.html)

1. [root@proxy ~]# echo "dG9tOjEyMzQ1Ng==" | base64 -d
2. tom:123456
3. [root@proxy ~]# echo "tom:123456" | base64
4. dG9tOjEyMzQ1Ngo=