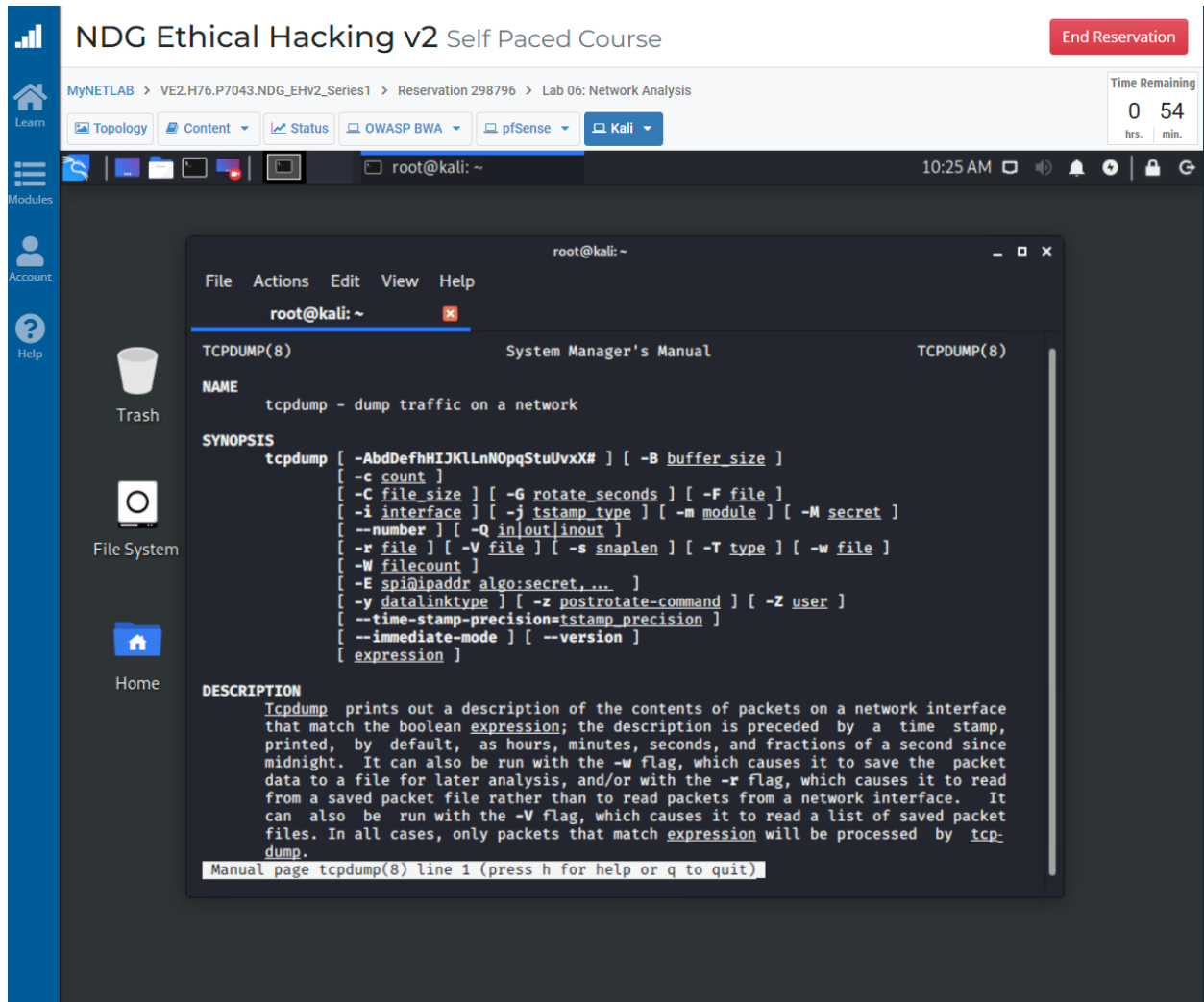


Jason Palmeri
CS53C
Lab 06
Timothy Ryan

Network Analysis



The image shows a screenshot of the NDG Ethical Hacking v2 Self Paced Course interface. The top navigation bar includes the course title, a reservation ID, and a lab title. A sidebar on the left contains icons for Learn, Modules, Account, and Help. The main content area displays a terminal window showing the manual for the tcpdump command. The terminal window has a menu bar with File, Actions, Edit, View, and Help. The terminal output shows the NAME, SYNOPSIS, and DESCRIPTION sections of the tcpdump manual. The DESCRIPTION section explains that tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match expression will be processed by tcpdump.

NDG Ethical Hacking v2 Self Paced Course

MyNETLAB > VE2.H76.P7043.NDG_EHv2_Series1 > Reservation 298796 > Lab 06: Network Analysis

Time Remaining
0 54
hrs. min.

root@kali: ~

10:25 AM

File Actions Edit View Help

root@kali: ~

TCPDUMP(8) System Manager's Manual TCPDUMP(8)

NAME
tcpdump - dump traffic on a network

SYNOPSIS
tcpdump [-AbDefhHIJKLlnNOpqStuUvX#] [-B buffer_size]
[-c count]
[-C file_size] [-G rotate_seconds] [-F file]
[-i interface] [-j timestamp_type] [-m module] [-M secret]
[--number] [-Q in|out|inout]
[-r file] [-V file] [-s snaplen] [-T type] [-w file]
[-W filecount]
[-E spi@ipaddr algo:secret,...]
[-y datalinktype] [-z postrotate-command] [-Z user]
[--time-stamp-precision=timestamp_precision]
[--immediate-mode] [--version]
[expression]

DESCRIPTION
Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match expression will be processed by tcpdump.

Manual page tcpdump(8) line 1 (press h for help or q to quit)

NDG Ethical Hacking v2 Self Paced Course

End Reservation

MyNETLAB > VE2.H76.P7043.NDG_EHv2_Series1 > Reservation 298796 > Lab 06: Network Analysis

Topology

Content

Status

OWASP BWA

pfSense

Kali

Time Remaining

0 50

hrs. min.

root@kali: ~

root@kali: ~

10:29 AM

Trash

File

Actions

Edit

View

Help

root@kali: ~

root@kali:~# man tcpdump

root@kali:~# tcpdump -i eth0

tcpdump: listening on eth0

root@kali: ~

root@kali:~# smbclient -L 192.168.68.12 --option='client min protocol=NT1'

Enter WORKGROUP\root's password:

Sharename	Type	Comment
print\$	Disk	Printer Drivers
apache	Disk	Apache Web Server Root
tomcat	Disk	Tomcat6 Root
var	Disk	/var
etc	Disk	/etc
usr	Disk	/usr
owaspbwa	Disk	/owaspbwa
IPC\$	IPC	IPC Service (owaspbwa server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

Server	Comment
WORKGROUP	Master
WORKGROUP	OWASPBWA

root@kali:~#

Learn

Modules

Account

Help

Trash

File Actions Edit View

root@kali: ~

root@kali:~# man tcpdump
root@kali:~# tcpdump -i etl
tcpdump: listening on eth0

Home

NDG Ethical Hacking v2 Self Paced Course

End Reservation

MyNETLAB > VE2.H76.P7043.NDG_EHv2_Series1 > Reservation 298796 > Lab 06: Network Analysis

Topology Content Status OWASP BWA pSense Kali

Time Remaining
0 47
hrs. min.

root@kali: ~ root@kali: ~ 10:32 AM

File Actions Edit View Help

root@kali: ~

rails Goat-git-1.2rc1	D	0	Mon	Mar	17	01:45:18	2014
WackoPicko-relative_urls-git	D	0	Tue	May	17	21:32:16	2011
webgoat.net-git	D	0	Fri	Mar	14	10:27:02	2014
mutillidae-git	D	0	Tue	Jul	28	22:44:52	2015
WebGoat-svn	D	0	Fri	Jun	29	15:39:36	2012
MCIR-git	D	0	Thu	Jun	18	22:12:33	2015
rails Goat-git-1.1.1	D	0	Mon	Mar	17	00:07:03	2014
rails Goat-git	D	0	Mon	Mar	17	01:45:18	2014
owasp-1-liner-git-modified-for-owaspbwa	D	0	Fri	Feb	1	16:48:05	2013
wivet-svn	D	0	Mon	Jul	16	08:57:29	2012
owasp-esapi-java-swingset-interactive-svn	D	0	Wed	Jan	2	20:10:33	2013
wavsep-git	D	0	Thu	Mar	13	21:58:32	2014
owaspbricks-svn	D	0	Fri	Mar	14	09:25:47	2014
SecurityShepherd-git	D	0	Thu	Jun	18	23:21:23	2015
owasp-1-liner-git-unmodified	D	0	Mon	Jul	29	23:56:53	2013
owasp-modsecurity-crs-git	D	0	Thu	May	14	22:32:49	2015
owasp-1-liner-git	D	0	Fri	Feb	1	16:48:05	2013
owaspbwa-svn	D	0	Thu	Mar	29	17:32:15	2012
rails Goat-git-1.2rc1-broken	D	0	Mon	Jul	29	23:28:57	2013
bwa_cyclone_transfers-git-1.2rc1	D	0	Mon	Jul	22	22:51:03	2013
bwa_cyclone_transfers-git	D	0	Mon	Jul	22	22:51:03	2013
redmine	D	0	Tue	Mar	20	16:12:20	2012
dvwa-git	D	0	Thu	May	14	22:32:52	2015
ModSecurity-git	D	0	Wed	Jul	17	21:16:18	2013
gruyere	D	0	Mon	May	2	22:27:09	2011
owasp-esapi-java-swingset-svn	D	0	Mon	Apr	2	12:27:19	2012
bwa_cyclone_transfers-git-1.1.1	D	0	Mon	Mar	17	00:00:50	2014

7583436 blocks of size 1024. 1099628 blocks available

smb: \>

Learn

Modules

Account

Help

NDG Ethical Hacking v2 Self Paced Course

End Reservation

MyNETLAB > VE2.H76.P7043.NDG_EHv2_Series1 > Reservation 298796 > Lab 06: Network Analysis

Time Remaining
0 45
hrs. min.

TopologyContentStatusOWASP BWApfSenseKali

testdump.pcap

testdump.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

smb

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000877	192.168.9.2	192.168.68.12	SMB	154	Negotiate Protocol Request
6	0.008927	192.168.68.12	192.168.9.2	SMB	197	Negotiate Protocol Response
10	8.850978	192.168.9.2	192.168.68.12	SMB	226	Session Setup AndX Request,
11	8.852837	192.168.68.12	192.168.9.2	SMB	330	Session Setup AndX Response,
13	8.854274	192.168.9.2	192.168.68.12	SMB	556	Session Setup AndX Request,
14	8.877232	192.168.68.12	192.168.9.2	SMB	176	Session Setup AndX Response
16	8.877471	192.168.9.2	192.168.68.12	SMB	162	Tree Connect AndX Request, P
17	8.878608	192.168.68.12	192.168.9.2	SMB	126	Tree Connect AndX Response

Frame 4: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)

Ethernet II, Src: Vmware_99:25:09 (00:50:56:99:25:09), Dst: Vmware_9a:63:ac (00:50:56:9a:63:ac)

Internet Protocol Version 4, Src: 192.168.9.2, Dst: 192.168.68.12

Transmission Control Protocol, Src Port: 48580, Dst Port: 445, Seq: 1, Ack: 1, Len: 88

NetBIOS Session Service

SMB (Server Message Block Protocol)

0000 00 50 56 9a 63 ac 00 50 56 99 25 09 08 00 45 00 PV c P V % E

0010 00 8c 37 00 40 00 40 06 35 0d c0 a8 09 02 c0 a8 7 @ 5

0020 44 0c bd c4 01 bd 82 62 30 33 f5 81 ad 2a 80 18 D b 03 *

0030 01 f6 ce dd 00 00 01 01 08 0a 72 35 aa a6 00 00 r5

0040 1d 0e 00 00 00 54 ff 53 4d 42 72 00 00 00 00 18 T S MBr

0050 43 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 C

0060 fe ff 00 00 00 00 00 31 00 02 4e 54 20 4c 41 4e 1 NT LAN

0070 4d 41 4e 20 31 2e 30 00 02 4e 54 20 4c 4d 20 30 MAN 1.0 NT LM 0

0080 2e 31 32 00 02 53 4d 42 20 32 2e 30 30 32 00 02 .12 SMB 2.002

testdump.pcap

Packets: 1580 · Displayed: 116 (7.3%)

Profile: Default



NDG Ethical Hacking v2 Self Paced Course

[End Reservation](#)

Learn

MyNETLAB > VE2.H76.P7043.NDG_EHv2_Series1 > Reservation 298796 > Lab 06: Network Analysis

Time Remaining

0 45
hrs. min.

Topology

Content

Status

OWASP BWA

pfSense

Kali

Modules

Account

Help

testdump.pcap 10:34 AM

testdump.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http Expression...

No.	Time	Source	Destination	Protocol	Length	Info
640	249.896214	192.168.9.2	192.168.68.12	HTTP	379	GET / HTTP/1.1
648	249.899823	192.168.68.12	192.168.9.2	HTTP	1034	HTTP/1.1 200 OK (text/html)
650	249.992829	192.168.9.2	192.168.68.12	HTTP	345	GET /index.css HTTP/1.1
652	249.994057	192.168.68.12	192.168.9.2	HTTP	1188	HTTP/1.1 200 OK (text/css)
656	249.994414	192.168.9.2	192.168.68.12	HTTP	334	GET /jquery.min.js HTTP/1.1
657	249.994656	192.168.9.2	192.168.68.12	HTTP	340	GET /animatedcollapse.js HTTP/1.1
668	249.997839	192.168.68.12	192.168.9.2	HTTP	142	HTTP/1.1 200 OK (application/javascript)
695	250.002880	192.168.68.12	192.168.9.2	HTTP	74	HTTP/1.1 200 OK (application/javascript)

Frame 640: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
Ethernet II, Src: Vmware_99:25:09 (00:50:56:99:25:09), Dst: Vmware_9a:63:ac (00:50:56:9a:63:ac)
Internet Protocol Version 4, Src: 192.168.9.2, Dst: 192.168.68.12
Transmission Control Protocol, Src Port: 46458, Dst Port: 80, Seq: 1, Ack: 1, Len: 313
Hypertext Transfer Protocol

```
0000 00 50 56 9a 63 ac 00 50 56 99 25 09 08 00 45 00 PV c P V % E
0010 01 6d a8 60 40 00 40 06 c2 cb c0 a8 09 02 c0 a8 m @ @
0020 44 0c b5 7a 00 50 b3 81 52 8c de 95 e7 ec 80 18 D z P R
0030 01 f6 cf be 00 00 01 01 08 0a 72 39 7a ce 00 01 r9z
0040 11 19 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e Host: 192.168.
0060 36 38 2e 31 32 0d 0a 55 73 65 72 2d 41 67 65 6e 68.12 U ser-Agen
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0080 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 X11; Lin ux x86_6
```

Hypertext Transfer Protocol: Protocol

Packets: 1580 · Displayed: 58 (3.7%)

Profile: Default

1126	282.469069	192.168.9.2	192.168.68.12	HTTP	419	GET /tikiwiki HTTP/1.1
1128	282.470873	192.168.68.12	192.168.9.2	HTTP	764	HTTP/1.1 301 Moved Permanent
1162	282.484913	192.168.9.2	192.168.68.12	HTTP	420	GET /tikiwiki/ HTTP/1.1
1268	282.636866	192.168.68.12	192.168.9.2	HTTP	801	HTTP/1.1 302 Found (text/ht
1286	282.642949	192.168.9.2	192.168.68.12	HTTP	480	GET /tikiwiki/tiki-index.php

Transmission Control Protocol, Src Port: 46466, Dst Port: 80, Seq: 1, Ack: 1, Len: 353

Hypertext Transfer Protocol

GET /tikiwiki HTTP/1.1\r\n

Host: 192.168.68.12\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://192.168.68.12/\r\n

Connection: keep-alive\r\n

```
0000 00 50 56 9a 63 ac 00 50 56 99 25 09 08 00 45 00 PV c P V % E
0010 01 95 fb 8a 40 00 40 06 6f 79 c0 a8 09 02 c0 a8 @ @ oy
0020 44 0c b5 82 00 50 6d 56 e1 2e fd 90 65 9f 80 18 D PmV e
0030 01 f6 cf e6 00 00 01 01 08 0a 72 39 fa 0a 00 01 r9
0040 30 e8 47 45 54 20 2f 74 69 6b 69 77 69 6b 69 20 GET /t ikiwiki
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 Host:
0060 31 39 32 2e 31 36 38 2e 36 38 2e 31 32 0d 0a 55 192.168. 68.12 U
0070 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0080 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69 6e la/5.0 ( X11; Lin
```

testdump.pcap

Packets: 1580 · Displayed: 58 (3.7%)

Profile: Default

Wireshark - Follow TCP Stream (tcp.stream eq 0) - testdump.pcap

File Edit View

tcp.stream eq 0

No.	Time
1	0.000000
2	0.000658
3	0.000715
4	0.000877
5	0.001097
6	0.008927
7	0.008942
10	8.850978

Frame 1: 74 bytes on wire (592 bits) captured (74 bytes) over Ethernet II, Src: [redacted], Dst: [redacted], Internet Protocol Version 4, Src: [redacted], Dst: [redacted], Transmission Control Protocol, Seq=1, Win=0, Len=0

...T.SMBr...C...1..NT LANMAN 1.0..NT LM 0.12..SMB
2.002..SMB 2.???..SMBr...C...
2...A...Q...V...owaspbwa...(.+.0..0..
+...7..
0...NONE...SMBs...C...J...T..
a..H..+...>0<..0..
+...7..
*.(NTLMSSP...b...(..
(...U.n.i.x...S.a.m.b.a...SMBs...d..
...0..
+...7..
...NTLMSSP...
0...ba.*.m...D.D.@...O.W.A.S.P.B.W.A...O.W.A.S.P.B.W.A..
O.W.A.S.P.B.W.A...o.w.a.s.p.b.w.a...U.n.i.x...S.a.m.b.a..
3...4...7...W.O.R.K.G.R.O.U.P...SMBs...C...d..
...T..
0...NTLMSSP...X...p...d...l...t..
...b...vj...k...*.b./
...V...r(O..cG.&...&|
...V...'.w...O.W.A.S.P.B.W.A...O.W.A.S.P.B.W.A...O..
w.a.s.p.b.w.a...0.0...e..(?aZ..o.^'.7']...e6..
...\$.c.i.f.s./..
1.9.2...1.6.8...6.8...1.2...W.O.R.K.G.R.O.U.P.r.o.o.t.K.A.L.I.w%..
*...U.n.i.x...S.a.m.b.a...j.SMBs...d..
...?..0..
...U.n.i.x...S.a.m.b.a...3...4...7...W.O.R.K.G.R.O.U.P...
...SMBu...C...d...1...
1.9.2...1.6.8...6.8...1.2...I.P.C.\$...?????
8.SMBu...d...IPC...f.SMB...

Packet 11: 9 client pkts, 9 server pkts, 17 turns. Click to select.

Entire conversation (3,022 bytes) Show and save data as ASCII Stream 0

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

29%) Profile: Default