Kali Telnet Client and Wireshark Capture

The presentation will use Kali Linux capture telnet and ssh packets. Kali will use Wireshark to capture the packets.

Preuss
4/28/2014

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:38 PM root

Computer

Kali Live

The presentation logs into Kali Linux.

KALI LINUX

The quieter you become, the more you are able to hear.

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:40 PM root

The Wireshark Network Analyzer [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

WIRESHARK

The World's Most Popular Network Protocol Analyzer

Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)

Capture

Interface List
Live list of the capture interfaces
(counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

- eth0
- nflog
- any

Capture Options
Start a capture with detailed options

Capture Help

Files

Open
Open

Open Rec

Sa
A ric

Online

Website
he project's website

er's Guide
ser's Guide (online version)

curity
with Wireshark as securely as possible

The presentation starts Wireshark. The wireshark captures will come from eth0.

Make sure Kali is bridge or NAT, depending on your needs. Also, you must have permission from the network owner to capture packets.

Ready to load or capture | No Packets | Profile: Default

The Wireshark Netwo...

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:40 PM root

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	Nortel_c9:10:01	Spanning-tree-(for-bri	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Port
2	0.164103000	192.168.65.2	54.83.197.43	TCP	62	50181 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_
3	0.174075000	192.168.65.2	54.83.197.43	TCP	62	50182 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_
4	1.575162000	192.168.65.2	134.29.228.9	TCP	66	50184 > ipp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
5	1.575173000	192.168.65.2	134.29.228.9	TCP	66	50183 > ipp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
6	1.810010000	Nortel_c9:10:01	Nortel-autodiscovery	NDP	60	FlatNet Hello
7	1.999921000	Nortel_c9:10:01	Spanning-tree-(for-bri	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Port

Kali Wireshark is capturing packets successfully.

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bi
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
```

```
0000  01 80 c2 00 00 00 00 19  e1 c9 10 01 00 26 42 42   ........ .....&BB
0010  03 00 00 00 00 00 80 00  00 19 e1 c9 10 01 00 00   ........ ........
0020  00 00 80 00 00 19 e1 c9  10 01 80 03 00 00 14 00   ........ ........
0030  02 00 0f 00 b6 db 6d 00  00 00 00 00               ......m. ....
```

eth0: <live capture in progress> Fil... Packets: 7 · Displayed: 7 (100.0%) Profile: Default

Capturing from eth0 ...

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:42 PM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# telnet 192.168.66.19
```

The presentation opens the command prompt. At the command prompt, the presentation enters the telent command with the IP address or FQDN of the telnet server.

Remember to use [ ] around IPv6 addresses.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:43 PM root

Computer

Kali Live

albatross08@msctc-linux-spring2014a:~

File Edit View Search Terminal Help

```
root@kali:~# telnet 192.168.66.19
Trying 192.168.66.19...
Connected to 192.168.66.19.
Escape character is '^]'.
Welcome to openSUSE 13.1 "Bottle" - Kernel 3.11.10-7-desktop
msctc-linux-spring2014a login: albatross08
Password:
Last login: Mon Apr 28 13:23:15 CDT 2014 from 192.168.65.254 on pts/3
No mail.
Last login: Mon Apr 28 13:23:43 from 192.168.65.254
Have a lot of fun...
Directory: /home/albatross08
Mon Apr 28 13:23:43 CDT 2014
albatross08@msctc-linux-spring2014a:~> fortune
greenrd's law
        Evey post disparaging someone else's spelling or grammar, or lauding
        one's own spelling or grammar, will inevitably contain a spelling or
        grammatical error.
                -- greenrd in http://www.kuro5hin.org/comments/2002/4/16/61744/5
230?pid=5#6
albatross08@msctc-linux-spring2014a:~>
```

KALI LINUX

The quieter you become, the more you are able to hear

The presentation logs into the telnet server as albatross08. After successful login, the presentation enters the fortune program on the telnet server.

Once the presentation is done. The presentation will enter the command exit to leave the telnet server.

msctc-linux-spring201...

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:44 PM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ssh -l albatross08 192.168.66.19
```

The presentation opens the command prompt. At the command prompt, the presentation enters the ssh command with the IP address or FQDN of the sshd server. The lower case minus L allows entering a different login name for the ssh server.

Remember to use [ ] around IPv6 addresses.

The question is asking if you really trust the host to be who you think. The answer is yes or no.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:43 PM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ssh 192.168.66.19
The authenticity of host '192.168.66.19 (192.168.66.19)' can't be established.
ECDSA key fingerprint is 4b:42:bb:f9:a5:10:20:23:95:ec:ca:d1:9b:45:df:1b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.66.19' (ECDSA) to the list of known hosts.
```

KALI LINUX

The quieter you become, the more you are able to hea

The presentation opens the command prompt. At the command prompt, the presentation enters the ssh command with the IP address or FQDN of the sshd server.

Remember to use [ ] around IPv6 addresses.

The question is asking if you really trust the host to be who you think. The answer is yes or no.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:44 PM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ssh -l albatross08 192.168.66.19
Password:
Last login: Mon Apr 28 13:23:43 2014 from 192.168.65.254
Have a lot of fun...
albatross08@msctc-linux-spring2014a:~> fortune
Given a choice between grief and nothing, I'd choose grief.
                -- William Faulkner
albatross08@msctc-linux-spring2014a:~>
```

The presentation successfully log into the sshd server. The presentation ran the fortune program for fun.

KALI LINU

The quieter you become, the more you a

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:44 PM root

Computer

Kali Live

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# ssh -l albatross08 192.168.66.19
Password:
Last login: Mon Apr 28 13:23:43 2014 from 192.168.65.254
Have a lot of fun...
albatross08@msctc-linux-spring2014a:~> fortune
Given a choice between grief and nothing, I'd choose grief.
                -- William Faulkner
albatross08@msctc-linux-spring2014a:~> exit
```

The presentation enters the exit command to leave the sshd server.

root@kali: ~

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:45 PM root

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Nortel_c9:10:01	Spanning-tree-(for-bri	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
7	1.999921000	Nortel_c9:10:01	Spanning-tree-(for-bri	STP	60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
8	3.999861000	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
9	5.999769000	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
12	7.999720000	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
13	9.999904000	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
15	11.99954300(	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
19	13.99946900(	Nortel_			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po
23	15.99944000(	Nortel			60	Conf. Root = 32768/0/00:19:e1:c9:10:01 Cost = 0 Po

The presentation clicks the Protocol header to sort all the files by protocol.

```
Frame 1: 60 bytes on wire                                  nterface 0
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
```

```
0000  01 80 c2 00 00 00 00 19  e1 c9 10 01 00 26 42 42   ........ .....&BB
0010  03 00 00 00 00 00 80 00  00 19 e1 c9 10 01 00 00   ........ ........
0020  00 00 80 00 00 19 e1 c9  10 01 80 03 00 00 14 00   ........ ........
0030  02 00 0f 00 b6 db 6d 00  00 00 00 00               ......m. ....
```

File: "/tmp/wireshark_pcapng_eth0... Packets: 1209 · Displayed: 1209 (100.0%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1....

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:45 PM root

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
769	140.8745230(	192.168.66.19	192.168.65.254	TELNET	67	Telnet Data ...
771	141.1129440(	192.168.65.254	192.168.66.19	TELNET	67	Telnet Data ...
772	141.1133620(	192.168.66.19	192.168.65.254	TELNET	67	Telnet Data ...
776	141.2821180(	192.168.65.254	192.168.66.19	TELNET	67	Telnet Data ...
777	141.2833640(	192.168.66.19	192.168.65.254	TELNET	67	Telnet Data ...
779	141.4415750(	192.168.65.254	192.168.66.19	TELNET	67	Telnet Data ...
780	141.4419640(	192.168.66.19	192.168.65.254	TELNET	67	Telnet Data ...
782	141.7899990(	192.168.65.254	192.168.66.19	TELNET	68	Telnet Data ...
783	141.7923390(	192.168.66.19	192.168.65.254	TELNET	76	Telnet Data ...

Frame 783: 76 bytes on wire (608 bits), 76 bytes captured (608 b s) on interface 0

Ethernet II, Src: Vmware 80:bb:c6 (00:0c:29:80:bb:c6), Dst: Vmwa :32:11 (00:0c:29:69:32:11)

Internet Protocol Versi 192.168.65.254 (192.168.65.254)

Transmission Control Pr (39990), Seq: 893, Ack: 172, Len: 10

Telnet

The presentation selects a telnet packet.

```
0000  00 0c 29 69 32 11 00                                    E.
0010  00 3e 41 de 40 00 40                                    ..
0020  41 fe 00 17 9c 36 67                                    ..
0030  00 e3 cf 87 00 00 01 01  08 0a 00 0b af 87 ff ff   ........ ........
0040  bc f8 0d 0a 6c 6f 67 6f  75 74 0d 0a             ....logo ut..
```

File: "/tmp/wireshark_pcapng_eth0... Packets: 1209 · Displayed: 1209 (100.0%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1....

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:45 PM root

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

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ar Apply Save

No.	Time	Source		Lengtl	Info
769	140.8745230(	192.168.(		67	Telnet Data ...
771	141.1129440(	192.168.(		67	Telnet Data ...
772	141.1133620(	192.168.(		67	Telnet Data ...
776	141.2821180(	192.168.(		67	Telnet Data ...
777	141.2833640(	192.168.(		67	Telnet Data ...
779	141.4415750(	192.168.(		67	Telnet Data ...
780	141.4419640(	192.168.(		67	Telnet Data ...
782	141.7899990(	192.168.(		68	Telnet Data ...
783	141.7923390(	192.168.(		76	Telnet Data ...

Analyze menu:
- Display Filters...
- Display Filter Macros...
- Apply as Column
- Apply as Filter
- Prepare a Filter
- Enabled Protocols... Shift+Ctrl+E
- Decode As...
- User Specified Decodes...
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream

Frame 783: 76 bytes on wir on interface 0
:32:11 (00:0c:29:69:32:11)
192.168.65.254 (192.168.65.254)
(39990), Seq: 893, Ack: 172, Len: 10

The presentation selects follow a TCP stream.

```
0000  00 0c 29 69 32 11 00 50  56 f0 29 69 08 00 45 10   ..)i2.. ).....E.
0010  00 3e 41 de 40 00 40 06  f5 89 c0 a8 3e 13 c0 a8   .>A.@.@. .i..B...
0020  41 fe 00 17 9c 36 67 52  08 24 78 3e 4c e9 80 18   A....6gR .$x>L...
0030  00 e3 cf 87 00 00 01 01  08 0a 00 0b af 87 ff ff   ........ ........
0040  bc f8 0d 0a 6c 6f 67 6f  75 74 0d 0a               ....logo ut..
```

File: "/tmp/wireshark_pcapng_eth0... Packets: 1209 · Displayed: 1209 (100.0%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1....

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:47 PM root

Follow TCP Stream

Stream Content

```
.......... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'.............
P..... .38400,38400....#.kali.example.org:0.0....'..DISPLAY.kali.example.org:0.0.....x
term..........Welcome to openSUSE 13.1 "Bottle" - Kernel 3.11.10-7-desktop (3).
...msctc-linux-spring2014a login: aallbbaattrroossss0088
.
Password: Tinkerbell
.
Last login: Mon Apr 28 13:23:15 CDT 2014 from 192.168.65.254 on pts/3
No mail.
Last login: Mon Apr 28 13:23:43 from 192.168.65.254
Have a lot of fun...
Directory: /home/albatross08
Mon Apr 28 13:23:43 CDT 2014
.7.]2;albatross08@msctc-linux-spring2014a:~..]1;msctc-linux-
spring2014a..8albatross08@msctc-linux-spring2014a:~> ffoorrttuunnee
.
greenrd's law
.Evey post disparaging someone else's spelling or grammar, or lauding
.one's own spelling or grammar, will inevitably contain a spelling or
.grammatical error.
..-- greenrd in http://www.kuro5hin.org/comments/2002/4/16/61744/5230?pid=5#6
.7.]2;albatross08@msctc-linux-spring2014a:~..]1;msctc-linux-
spring2014a..8albatross08@msctc-linux-spring2014a:~> eexxiitt
.
logout
```

Entire conversation (1073 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

The presentation selects ASCII output. Then the presentation selects Save As

ta ...
ta ...
ta ...
ta ...
ta ...
ta ...
ta ...
ta ...
ta ...

:32:11)
2.168.65.254)
Ack: 172, Len: 10

```
0 bb c6 08 00 45 10   ..)i2... ).....E.
9 c0 a8 42 13 c0 a8   .>A.@.@. .i..B...
4 78 3e 4c e9 80 18   A....6gR .$x>L...
a 00 0b af 87 ff ff   ........ ........
4 0d 0a               ....logo ut..
```

Packets: 1209 · Displayed: 146 (12.1%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1.... Follow TCP Stream

kali-linux-1-0-6-x86 - VMware Player (Non-commercial use only)

Player

Applications Places Sun Apr 27, 7:48 PM root

Wireshark: Save Follow Stream As

Name: telnet_capture_01.txt

Save in folder: root

Create Folder

The presentation gives the file a name, then saves the file.

	Size	Modified
		02/12/2014
C01_04162014.html	42.7 kB	04/16/2014
C02_04162014.html	42.9 kB	04/16/2014
erver01_04162014.html	32.1 kB	04/16/2014
_spring2014-1.html	7.1 kB	04/08/2014
_spring2014-2.html	34.8 kB	04/09/2014
ture_01.txt	1.1 kB	19:46
XP_br166_01.html	32.9 kB	04/09/2014

Cancel Save

4)

_en: 10

0030 00 e3 cf 87 00 00 01 01 08 0a 00 0b af 87 ff ff ....
0040 bc f8 0d 0a 6c 6f 67 6f 75 74 0d 0a ....logo ut..

File: "/tmp/wireshark_pcapng_eth0... Packets: 1209 · Displayed: 146 (12.1%) · Dropped: 0 (0.0%) Profile: Default

*eth0 [Wireshark 1.... Follow TCP Stream