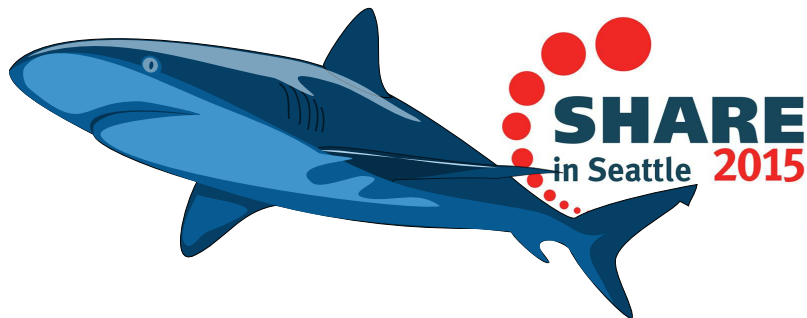


SHARK@SHARE



wireshark Hands-On Lab

Thursday, March 5, 2015

01:45 PM – 02:45 PM

Sheraton Seattle, Redwood

Session 16752

<https://ibm.biz/SHARKatSHARE>



#SHAREorg



SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.



Wireshark Lab Part I. General Questions

- How long was the trace running?
 - The trace captured a timeframe of _____ seconds
- What is the average packet rate?
 - The average packet rate is _____ packets/s
- What are the 3 top talker IP addresses in the trace?
 - IP address 1: ____:____:____:____ - _____ packets
 - IP address 2: ____:____:____:____ - _____ packets
 - IP address 3: ____:____:____:____ - _____ packets
- Save number_1's traffic under a new filename
 - Filter: ip.addr eq aa.bb.cc.dd
 - File → Export specified packets → wireshark pcapng format!
 - Filename: SHARE16752.TopTalker.pcapng

Wireshark Lab Part II. TCP Questions

- How many TCP sessions start in this trace
 - The trace contains _____ new TCP connections
- How many TCP sessions terminate in this trace
 - The trace contains _____ terminating TCP connections
- What are the top 3 clients connecting in the trace?
 - IP address 1: ____:____:____:____ - _____ new sessions
 - IP address 2: ____:____:____:____ - _____ new sessions
 - IP address 3: ____:____:____:____ - _____ new sessions
- Save number_1's traffic under a new filename
 - Filter: ip.addr eq aa.bb.cc.dd - File → Export specified packets
 - Filename: SHARE16752.TopTalker.client1.pcapng
- Save number_2's and number_3's traffic also
 - File → Export ...

Wireshark Lab Part III. TN3270 Questions

- How many TN3270 sessions are started in the trace?
 - There are ____ new TN3270 sessions starting in the trace
- How many TCP ports is the TN3270 Server listening on?
 - The TN3270 Server listens on ports _____
- What are the top 3 clients connecting to the TN3270 server?
 - IP address 1: ____:____:____:____ - _____ new sessions
 - IP address 2: ____:____:____:____ - _____ new sessions
 - IP address 3: ____:____:____:____ - _____ new sessions
- What is the percentage of all TN3270 traffic in the trace?
 - Filter: tcp.port==23 or tcp.port==nnnn || tcp.port= nnnn ...
 - Filename: SHARE16752.TopTalker.client1.pcapng
- Save all TN3270 traffic under a new file
 - File → Export ... SHARE16752.TN3270.pcapng

Wireshark Lab Part III. TLS Questions

- How many active TLS sessions are in the trace?
 - There are _____ sessions that carry TLS application data.
- What other server ports besides TN3270 support TLS?
 - Following servers sent a ServerHello: Ports _____
- What are the top clients connecting via SSL to the TN3270?
 - IP address 1: _____._____._____.____ - _____ ClientHello packets
 - IP address 2: _____._____._____.____ - _____ ClientHello packets
 - IP address 3: _____._____._____.____ - _____ ClientHello packets
 - IP address 4: _____._____._____.____ - _____ ClientHello packets
 - IP address 5: _____._____._____.____ - _____ ClientHello packets
- Save all traffic of the IP subnet of #4 and #5 under a new file
 - File → Export ... SHARE16752.IPSubnet.pcapng

Wireshark Lab Part Background

- What the TCP payload looks like

Telnet Negotiation

```
FFFD2E DO TLS
FFFC2E WONT TLS
FFFD28 DO TN3270E
FFFB28 WILL TN3270E
FFFA28 SB TN3270E
      00 Associate
      01 Connect
      02 Dev-Type
      03 Functions
      04 Is
      05 Reason
      06 Reject
      07 Request
      08 Send
```

Keepalive Probes

```
FFFB06 WILL TIMEMARK
FFFC06 WONT TIMEMARK
FFFD06 DO TIMEMARK
```

```
8055010301 SSLV2 ClientHello V31
14 --- Change Cipher Spec ---
1403vv 0001 01 ChangeCipherSpec
15 --- Alert -----
1603vv xxxx yy
      00 SSL3.0
16 --- Handshake Protocol ---
1603vv xxxx yy
      00 SSL3.0
      01 TLS1.0
      02 TLS1.1
      03 TLS1.2
      01 ClientHello
      02 ServerHello
      0B Certificate
      0E ServerHelloDone
      10 ClientKeyExchange
17 --- Application Data ---
1703vv xxxx yy Encrypted ApplData
```

Successful TN3270 Negotiation

SEATTLE.PCOMM.VTAMP.pcapng [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 2 Expression... Clear Apply Save

No.	Time	Source	SHARE_SEATTLE_2015:Session 16752 #SHARKatSHARE	Data
13	0.000	Win7.Client	<--- SYN Win7 [Fingerprint: 8192:128:1:M*	
14	0.000	TN3270.Server	---> SYN_ACK zOS fingerprint[65535:64:0:*,M*,W*	
15	0.000	Win7.Client	<--- 3-way-HS completed ESTABLISHED :-)	
16	0.001	TN3270.Server	DO TN3270E ---> :-)	fffd28
17	0.049	Win7.Client	<----- WILL TN3270E :-)	fffb28
18	0.010	TN3270.Server	TN3270E --> SB Send Device-Type SE ---> :-	fffa280802fff0
19	0.051	Win7.Client	TN3270E <--- SB Device-Type Req SE :-	fffa28020749424d2d44594e414d4943fff0
20	0.000	TN3270.Server	TN3270E --> SB Device-Type Is IBM-xxx, Connect	fffa28020449424d2d44594e414d49430149565a24543539
21	0.086	Win7.Client	TN3270E <--- SB Functions Req: Bind-Img Rsp Sys	fffa28030700020405fff0
22	0.000	TN3270.Server	TN3270E --> SB Function Is Bind-img,Rsp,Sys-Req	fffa28030400020405fff0
23	0.006	TN3270.Server	TN3270E --> BIND	030000000031010303b1903080008787f887000200000000
24	0.000	Win7.Client	<--- ACK (Win)	
25	0.000	TN3270.Server	TN3270E --> BID (ContRes)	0900020001ffef
26	0.063	Win7.Client	TN3270E <--- DR	
27	0.000	TN3270.Server	---> ACK zOS	
28	0.000	TN3270.Server	TN3270E --> Erase Write	0003020002f5c61140403c5c6f401d601140401d60c9c2d4
29	0.000	TN3270.Server	TN3270E --> Data	40404040f0f07af0f540114dd21d6040114e4b1de8c3d5d4
30	0.000	Win7.Client	<--- ACK (Win)	
31	0.020	Win7.Client	TN3270E <--- DR	
32	0.000	TN3270.Server	---> ACK zOS	

Successful TLS Negotiation



SHARE16752.pcapng

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 1559 Expression... Clear Apply Save p0f 3wayHS

Source	Coloring Rule Name	data	tcp_ws	tcp.relative	ip.l
172.21.25.200	p0f win7_Tstamp	8192:128:1:60:M*,N,W*,N,N,T	8192	0.000000000	
172.20.0.16	z0S 16K 32768:64:*:48:M*,N,W0		32768	0.000068000	
172.21.25.200	3-way_HS complete ! ESTABLISHED		66792	0.000489000	
172.21.25.200	SSLv2 Client Hello	801f010301000600000001	66792	0.006968000	
172.20.0.16	TLS Server Hello	16030103da0200004d030	32735	0.008024000	1
172.21.25.200	TLS Client Key exchange	160301010610000102010	65800	0.009955000	
172.20.0.16	TLS Change Cipher Spec	140301000101	32450	0.013136000	
172.20.0.16	TLS Handshake	1603010028dc10d53bf05	32450	0.013248000	
172.20.0.16	TLS AppData	17030100182a0768ad5b8	32450	0.013493000	
172.21.25.200			65748	0.013794000	
172.21.25.200	TLS AppData	170301001881fc02911af	65720	0.015390000	
172.20.0.16	TLS AppData	1703010020e6ad97ed1d3	32739	0.015570000	
172.21.25.200	TLS AppData	1703010030bd0dd205086	65684	0.016326000	
172.20.0.16	TLS AppData	1703010020a4aab9622af	32715	0.016894000	
172.21.25.200	TLS Close Notify	15030100180ac8720d0ae	65644	0.024988000	
172.20.0.16	TLS Close Notify	150301001864e35020407	32739	0.025175000	
172.21.25.200	FIN		65644	0.025296000	
172.21.25.200	RST: W0		0	0.025539000	

File: "/home/mburkhar/2015/... Packe... Profile: SHARE2015