

SMB Masterclass Outtakes and Lessons Learned

Eddi Blenkers

#sf25eu

1

Abstract

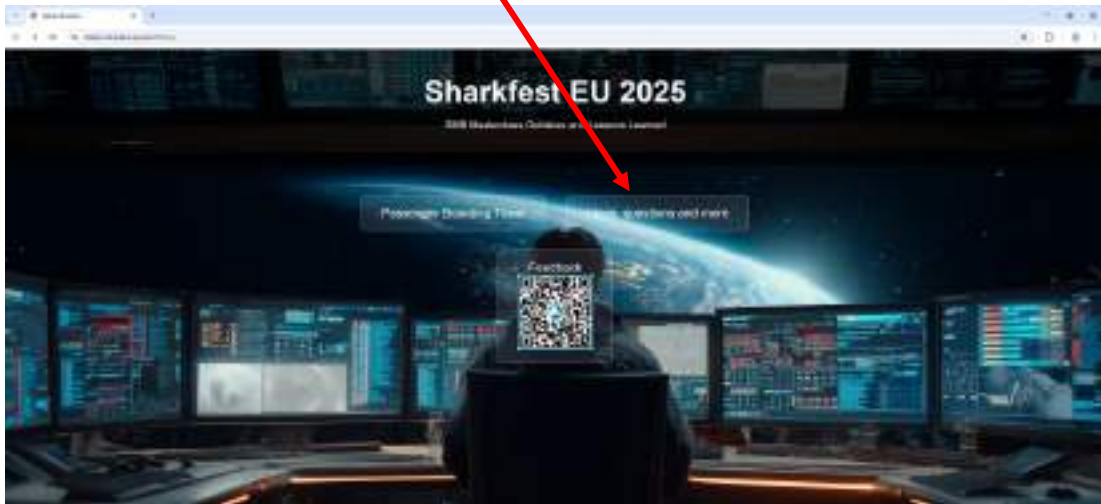
- I had the honor to prepare the SMB masterclass for this years Sharkfest EU.
- The class puts students into the role of a network engineer in a fictious company where they solve real world problems.
- At the end of the class, a few traces were left undiscussed. Outtakes.
- <https://www.stellar-bluetani.space/sf25eu/>

2

Participate!



Click here for interaction



3

Using Mindwendel



Place questions, copy display filters and share what you take away from this presentation



4

What I learned while preparing the Class



- Teaching is learning and one way to learn is teaching
 - Details on CreateFile, Cache Manager
 - Obscure results on writing Code
 - Unexpected system behavior
- Things rarely work as expected
 - Some things don't work as documented
 - Focus on the goal, not on the path.
Often, multiple methods will generate the same results
- Start early. It always takes longer than expected.

5

Coding for Multiple Platforms is hard!



- Mixed architecture x86 and x64 is a bitch if you write your own code.
 - Not just software, but also Dotnet runtime and stuff
 - Glad that I did not have to add stuff
 - XP was eliminated from the lab after this message popped up:



- Hats off and deep bow to the Wireshark developers for supporting so many OS platforms

6

The Winsockete Lame List



- A list of deadly sins that no programmer should commit
<https://tangentsoft.com/wskfaq/articles/lame-list.html>
- Wonderfully verbal ratings for bad coding
*totally lame, thrashing in a sea of lameness,
pushing the lameness envelope or
Stooping to unspeakable depths of lameness*
- Alas, a few real-world applications are still
Seeping lameness from every crack and crevice

7

Caching Can be a Bitch



**Clearing Client
Cache Creates
Consistent
Conclusions**

mostly



8

Clearing Client Caches



- Noteworthy Bookmarks:
 - <https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/re-initialize-offline-files-cache-database>
 - <https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/access-offline-files-file-server-removed-from-network>
- Set Registry Keys, then reboot:
 - REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache" /v FormatDatabase /t REG_DWORD /d 1 /f
 - REG ADD "HKLM\System\CurrentControlSet\Services\CSC\Parameters" /v FormatDatabase /t REG_DWORD /d 1 /f
- Registry keys will be deleted after reboot.

9

Introducing Stellar Bluetani



- Mariupol Station uses a number of critical applications to process incoming ships and their passengers.
- A few lame applications replicate cases that we have seen in the real world.



10

Passenger Boarding Application



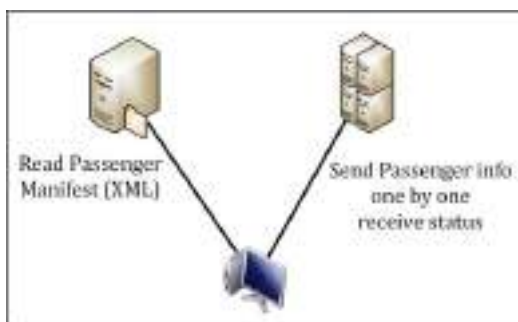
- All ships transmit a manifest with passenger data to the station before docking.
- The station's security service clears the passenger for boarding.
 - Read passenger data
 - Transmit passenger data to a central data
 - Central server will grant or deny access to the station
- Processing the last ship took 10 seconds for 30 passengers
- This is too slow to process large cruise ships with hundreds of passengers.

11

What we know about the Application



- Workstation ST-MP-WS-46 is configured for dual stack **10.2.20.46** and **10:2:20::46**
- Boarding App reads manifest.xml from file server
- Make HTTP requests with passenger data to **boarding.intra.stellar-bluetani.space** on port **8888**



12

Your Turn



- Which factors could contribute to the poor performance?
- Enter your ideas at the White Board!



13

Possible Causes for Poor Performance



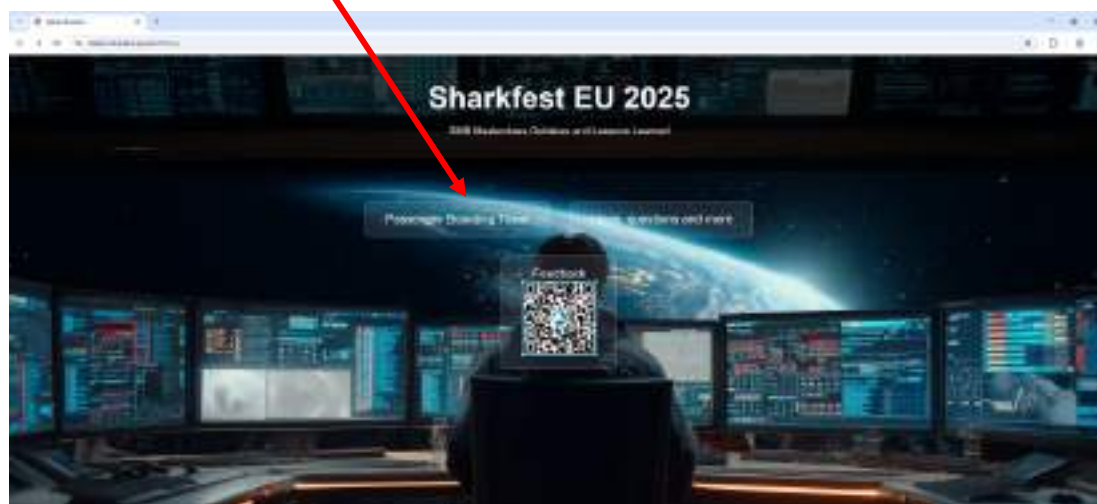
- Latency
- Packet loss
- Bandwidth limitations
- Change in network topology
- Slow Server
- Slow Client
- ... And whatever you have entered on the whiteboard

14

Wireshark Time



Trace file at <https://www.stellar-Bluetani.space/sf25eu>



15



SMB in a Nutshell

#sf25eu

16

Connecting to an SMB server

Negotiate Dialect

- Usually 4 packets
- Should result in SMB 3.1.1

Session Setup

- 2 packets when Kerberos is used
- 4 packets for Challenge/Response in a Workgroup

Tree Connect

- Specify the name of the share
- IPC\$ is not a reserved name for named pipes ("TCP via SMB")

17

Handshake in a trace file

- Apply the filter **tcp.stream eq 18 and (smb or smb2)**

No.	Time	Source	Destination	Protocol	Length	Info
155	0.000	10.1.1.25:25	10.1.1.25:25	SMB	147	Session message; Negotiate Protocol
158	0.001	10.1.1.25:25	10.1.1.25:25	SMB2	326	Negotiate Protocol Response
159	0.001	10.1.1.25:25	10.1.1.25:25	SMB2	252	Negotiate Protocol Request
160	0.001	10.1.1.25:25	10.1.1.25:25	SMB2	386	Negotiate Protocol Response
176	0.023	10.1.1.25:25	10.1.1.25:25	SMB2	1295	Session Setup Request
178	0.028	10.1.1.25:25	10.1.1.25:25	SMB2	314	Session Setup Response
179	0.029	10.1.1.25:25	10.1.1.25:25	SMB2	216	Tree Connect Request, Tree: '\\HQ-FS-1.intra.stellar-bluetani
180	0.029	10.1.1.25:25	10.1.1.25:25	SMB2	158	Tree Connect Response, Tree: '\\HQ-FS-1.intra.stellar-bluetani
181	0.030	10.1.1.25:25	10.1.1.25:25	SMB2	198	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
182	0.032	10.1.1.25:25	10.1.1.25:25	SMB2	1102	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
185	0.038	10.1.1.25:25	10.1.1.25:25	SMB2	244	Tree Connect Request, Tree: '\\HQ-FS-1.intra.stellar-bluetani
186	0.038	10.1.1.25:25	10.1.1.25:25	SMB2	158	Tree Connect Response, Tree: '\\HQ-FS-1.intra.stellar-bluetani

18

Example Response Time Calculation



Ctrl-T to set Time Reference to first packet of 3-way handshake

Initial Roundtrip Time at
3rd packet of handshake

Another Time Reference
at start of request

ACK = Server has
received the request

No.	Time	Source	Destination	Protocol	Length	Info
53	0.021	10:1:1:25::26	10:1:1:25::26	TCP	86	50107 → 445 [SYN] Seq=0 win=0
54	0.022	10:1:1:25::26	10:1:1:25::26	TCP	86	445 → 50107 [SYN, ACK] Seq=0
55	0.022	10:1:1:25::26	10:1:1:25::26	TCP	74	50107 → 445 [ACK] Seq=1 Ack=0
56	0.045	10:1:1:25::26	10:1:1:25::26	SMB	326	Session message; Negotiate F
57	0.045	10:1:1:25::26	10:1:1:25::26	SMB	308	Negotiate Protocol Response
58	0.068	10:1:1:25::26	10:1:1:25::26	SMB	418	Negotiate Protocol Request
63	0.110	10:1:1:25::26	10:1:1:25::26	TCP	74	50107 → 445 [ACK] Seq=308 Ac
69	*0.02*	10:1:1:25::26	10:1:1:25::26	SMB	2267	Session Setup Request
72	0.020	10:1:1:25::26	10:1:1:25::26	TCP	74	445 → 50107 [ACK] Seq=589 Ac
73	0.023	10:1:1:25::26	10:1:1:25::26	SMB	334	Session Setup Response

Time of Response : 0.023

Minus RTT = 3 msec

19

Process Files



- Send a Create Command to begin processing the trace
- Then follow Read, Write and other requests
- Finally, Close when the file is no longer accessed

No.	Time	Source	Destination	Protocol	Length	Info
2753	487.544	10:1:1:25::25	10:1:1:25::25	SMB	482	Create Request, File: HQ-FS-1\
2755	487.691	10:1:1:25::25	10:1:1:25::25	SMB	108	Create Response, File: HQ-FS-1\
2756	487.693	10:1:1:25::25	10:1:1:25::25	SMB	191	Read Request Len:5370 Off:0, Fi
2760	487.694	10:1:1:25::25	10:1:1:25::25	SMB	1288	Read Response, File: HQ-FS-1\sp
2762	487.701	10:1:1:25::25	10:1:1:25::25	SMB	182	GetInfo Request FILE_INFO/SMB2
2763	487.701	10:1:1:25::25	10:1:1:25::25	SMB	188	GetInfo Response, File: HQ-FS-1
3286	429.843	10:1:1:25::25	10:1:1:25::25	SMB	166	Close Request, File: HQ-FS-1\sp
3287	429.844	10:1:1:25::25	10:1:1:25::25	SMB	282	Close Response, File: HQ-FS-1\sp

20

Check the SMB response times

- Statistics → Service Response Times
- Check for repeated requests or long response times
- Expect less than 10 msec from file server
- Take the iRTT into account

Index	Procedure	Calls	Min SRT (s)	Max SRT (s)	Avg SRT (s)	Sum SRT (s)
0	Negotiate Protocol	5	0.000454	0.002338	0.001130	0.005648
1	Session Setup	5	0.001156	0.002104	0.000571	0.002857
2	Session Logoff	2	0.000634	0.001724	0.000704	0.001408
3	Tree Connect	12	0.000233	0.002079	0.000829	0.011143
4	Tree Disconnect	9	0.000482	0.001353	0.001014	0.009125
5	Create	84	0.000294	0.189522	0.000270	0.297867
6	Close	17	0.000197	0.001756	0.000392	0.307335
7	Read	9	0.000130	0.004604	0.001409	0.012684
11	lock	15	0.000290	0.005327	0.000849	0.111129
14	Find	16	0.000736	0.154411	0.020273	0.324372
16	GetInfo	76	0.000144	0.009603	0.000364	0.179602

Ups.
146 msec is long

Overall not
a huge issue

21

If it's not SMB, then what it is?

22

A look at the Passenger Manifest



- Goto Packet (**Ctrl-G**) 2760 and examine the read response
- Looks like XML:

```
<?xml version='1.0' encoding='utf-8'?>
<passenger-manifest>
<ship>
  <name>
    ...
  </captain>
</ship>
<passengers>
  <passenger>
    <first_name>
      Quinn
    </first_name>
    ...
  </passenger>
```

25

If it's not the network, and not SMB, then what?



- Let's step through the trace file
- Notice Packet 2764
 - The application sends a broadcast for every processed record
 - Feature was added to aid in debugging
 - Decode UDP port 33333 as Syslog
 - Create Coloring Rule to highlight packet
- **Ctrl-T** Set a time reference on packet 2764
- **Ctrl-F** for **udp.port == 33333** to find next broadcast
 - Frame 2779: Notice 393 msec
 - Frame 2792: Notice 780 msec

26

350 msec per Request? The VISUAL approach



- Apply filter **not tcp.port == 445**

DNS Query
after 57 msec → slow!

TCP Handshake
1 msec → quick!

HTTP Response
after 326 msec → slow!

No.	Time	Source	Destination	Protocol	Info
2764	*RFP*	10.1.20.46	255.255.255.255	Syslog	Found Passenger
2766	0.057	10.1.20.46	10.1.1.10	DNS	Standard query 0xdc
2767	0.057	10.1.20.46	10.1.1.10	DNS	Standard query 0xdc
2768	0.058	10.1.1.10	10.1.20.46	DNS	Standard query resp
2769	0.058	10.1.1.10	10.1.20.46	DNS	Standard query resp
2770	0.061	10.1.20.46	10.1.1.28	TCP	53452 → 8888 [SYN]
2771	0.061	10.1.1.28	10.1.20.46	TCP	8888 → 53452 [SYN]
2772	0.062	10.1.20.46	10.1.1.28	TCP	53452 → 8888 [ACK]
2773	0.062	10.1.20.46	10.1.1.28	HTTP	GET /boarding.asp H
2774	0.062	10.1.1.28	10.1.20.46	TCP	8888 → 53452 [ACK]
2775	0.388	10.1.1.28	10.1.20.46	TCP	8888 → 53452 [PSH]
2776	0.388	10.1.1.28	10.1.20.46	HTTP	HTTP/1.0 200 (text
2777	0.389	10.1.20.46	10.1.1.28	TCP	53452 → 8888 [FIN]
2778	0.389	10.1.1.28	10.1.20.46	TCP	8888 → 53452 [ACK]
2779	0.393	10.1.20.46	255.255.255.255	Syslog	Found Passenger

27

Examine Data



- HTTP Request contains passenger data
- Cannot be decoded, because Content-Type is missing

No.	Time	Source	Destination	Protocol	Info
2764	*RFP*	10.1.20.46	255.255.255.255	Syslog	Found Passenger
2773	0.062	10.1.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0
2776	0.388	10.1.1.28	10.1.20.46	HTTP	HTTP/1.0 200 (text/plain)

Frame 2773: Packet, 387	0000	00 0c 20 3a 3c 50 00 0c 29 2d 23 35 00 00 45 00	[Decoded]
Ethernet II, Src: VMware	0010	01 15 50 13 40 00 00 00 08 23 0a 02 14 20 8a 01	UP
Internet Protocol Versio	0020	01 1c 00 00 22 28 0a 08 e3 fc cd 54 4f 0b 50 18	...rdh...TO P
Transmission Control Pro	0030	01 80 36 4c 00 00 47 45 54 20 2f 62 6f 61 72 64	...6L...GE T /board
Hypertext Transfer Protoc	0040	60 1e 67 2e 61 73 78 20 48 54 54 50 2f 31 2e 30	ing.asp HTTP/1.0
GET /boarding.asp HTTP	0050	0d 0a 48 6f 73 74 3a 20 62 6f 61 72 64 69 6e 67	Host: boarding
Host: boarding.intra.s	0060	3e 89 6e 74 72 61 2e 73 7a 65 6c 6c 61 72 2d 62	.intra.s tellar-h
User-Agent: Stellar-Bo	0070	6c 75 65 74 61 6e 69 2e 73 79 61 63 65 0d 8a 55	luetani, space-U
Content-Length: 183\r\n	0080	73 65 72 2d 41 67 65 6e 7a 3a 20 53 74 65 6c 6c	ser-Agen t: Stell
Connection: close\r\n\r\n	0090	61 72 2d 42 64 61 72 64 69 6e 67 28 76 31 2e 34	ar-Board ing v1.4
[Response in frame: 27	00a0	0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68	Content-Length
[Full request URL: GET	00b0	3a 20 31 38 33 0d 8a 43 6f 6e 6c 65 63 74 69 6f	: 183 -C connectio
File Data: 183 bytes	00c0	6e 3a 20 63 6c 6f 73 65 0d 8a 0d 0a 20 20 3c 70	n: close ... cp
Data (183 bytes)	00d0	61 73 73 65 6e 67 65 72 3e 0d 0a 20 20 20 20 3c	assenger ... c
	00e0	66 69 72 73 74 5f 6e 61 6d 65 3e 0d 0a 20 20 20	first_na mes
	00f0	20 20 28 51 75 69 6e 6e 0d 0a 20 20 20 20 3c 2f	Quinn ... </
	0100	66 69 72 73 74 5f 6e 61 6d 65 3e 0d 0a 20 20 20	first_na mes
	0110	20 3c 73 75 72 6e 61 6d 65 3e 0d 0a 20 20 20 20	<summary> es...

28

Server Response

- Notice the response time: $388 - 62 = 326$ msec

No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found Passenger
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp
2776	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (te

Frame 2776: Packet, 54 bytes on wire (432 bits), 54 bytes captured (Ethernet II, Src: VMware_3a:3c:59 (00:0c:29:3a:3c:59), Dst: VMware_2
 Internet Protocol Version 4, Src: 10.1.1.28, Dst: 10.2.20.46
 Transmission Control Protocol, Src Port: 8888, Dst Port: 53452, Seq:
 [2 Reassembled TCP Segments (145 bytes): #2775(145), #2776(0)]
 Hypertext Transfer Protocol
 - Line-based text data: text/plain (3 lines)
 len: 333\r\n
 entry code: alba3d6\r\n
 status: ENTRY GRANTED\r\n

29

Benefit from the Wireshark Decode

- TCP reveals the iRTT
 - Filter for `tcp.analysis.initial_rtt > x`
- HTTP reveals the response time on application level
 - Filter for `http.time > x`

No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found P
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /ba
2776	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.

Urgent Pointer: 0
 [Timestamps]
 [SEQ/ACK analysis]
 [iRTT: 1.100000 milliseconds]
 [Bytes in flight: 333]
 [Bytes sent since last PSN flag: 333]

No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found P
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /ba
2775	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1

\r\n
 [Request in frame: 2773]
 [Time since request: 326.101000 milliseconds]
 [Request URI: /boarding.asp]
 [Full request URI: http://boarding.intra.stellar-bluea

30

The Systematic Approach



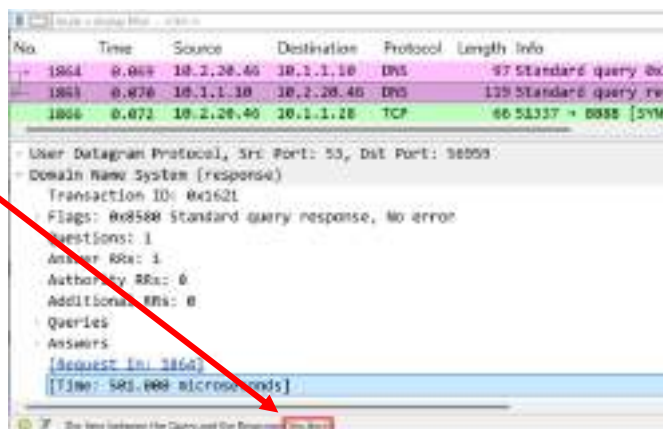
- This trace is easy to analyze:
 - Only traffic from one workstation to a single server
 - Not polluted by routine traffic from weather apps etc.
- How to process larger files
 - Track response times measured by Wireshark
 - Use service response time statistics

31

Response Times measured by Wireshark



- Note that Wireshark will track the response times for many protocols.
- Note the artificial field **dns.time**
- The field name is shown in the status bar
- Other popular protocols are SMB, HTTP and more

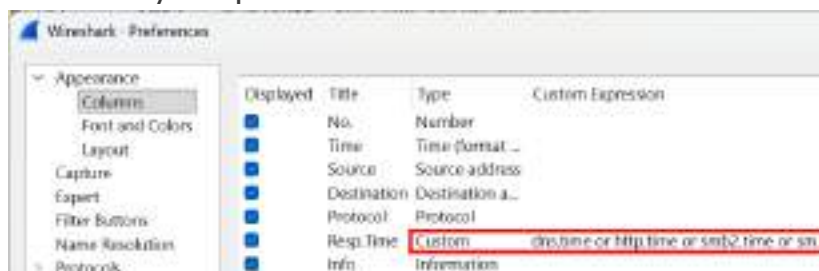


32

Search for Slow Response Times



- Option 1: Use repeated search operations
 - Search for **dns.time > 0.1** or **smb.time > 0.1** or **http.time > 0.1**
- Option 2: Prepare a Performance-Profile
 - New Profile
 - Add Column Response Time
 - Sort trace by Response Time



33

Stop Using HTTP 1.0



- Filter for **tcp.port == 8888**
- New TCP session for each passenger

No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found Passenger
2770	0.061	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [SYN] Seq=0 Win=6420
2771	0.061	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [SYN, ACK] Seq=0 Ack=
2772	0.062	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [ACK] Seq=1 Ack=1 W
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0
2774	0.082	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [ACK] Seq=1 Ack=334
2775	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (text/plain)
2776	0.388	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [FIN, ACK] Seq=146
2777	0.389	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [FIN, ACK] Seq=334
2778	0.389	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [ACK] Seq=147 Ack=3
2782	0.470	10.2.20.46	10.1.1.28	TCP	53453 → 8888 [SYN] Seq=0 Win=6420
2783	0.471	10.1.1.28	10.2.20.46	TCP	8888 → 53453 [SYN, ACK] Seq=0 Ack=
2784	0.471	10.2.20.46	10.1.1.28	TCP	53453 → 8888 [ACK] Seq=1 Ack=1 W
2785	0.471	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0

34

Wait, there is more!

- Client is repeating DNS query for AAAA record of server
- Response delivers a CNAME which is only available through IPv4

No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found Passenger
2766	0.057	10.2.20.46	10.1.1.10	DNS	Standard query 0xdcc5 A boarding.intra.st
2767	0.057	10.2.20.46	10.1.1.10	DNS	Standard query 0xdeaf AAAA boarding.intra
2768	0.058	10.1.1.10	10.2.20.46	DNS	Standard query response 0xdeaf AAAA board
2769	0.058	10.1.1.10	10.2.20.46	DNS	Standard query response 0xdcc5 A boarding
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0
2775	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (text/plain)
2780	0.468	10.2.20.46	10.1.1.10	DNS	Standard query 0x4744 AAAA boarding.intra
2781	0.469	10.1.1.10	10.2.20.46	DNS	Standard query response 0x4744 AAAA board
2785	0.471	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0
2787	0.773	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (text/plain)
2795	0.846	10.2.20.46	10.1.1.10	DNS	Standard query 0xb0f8 AAAA boarding.intra
2796	0.846	10.1.1.10	10.2.20.46	DNS	Standard query response 0xb0f8 AAAA board

35

Your Turn

- What did you take away from this session?
- Leave a note at the White Board!



36

Your Feedback, Please!



#sf25eu