SMB Masterclass Outtakes and Lessons Learned

Eddi Blenkers

#sf25eu

1

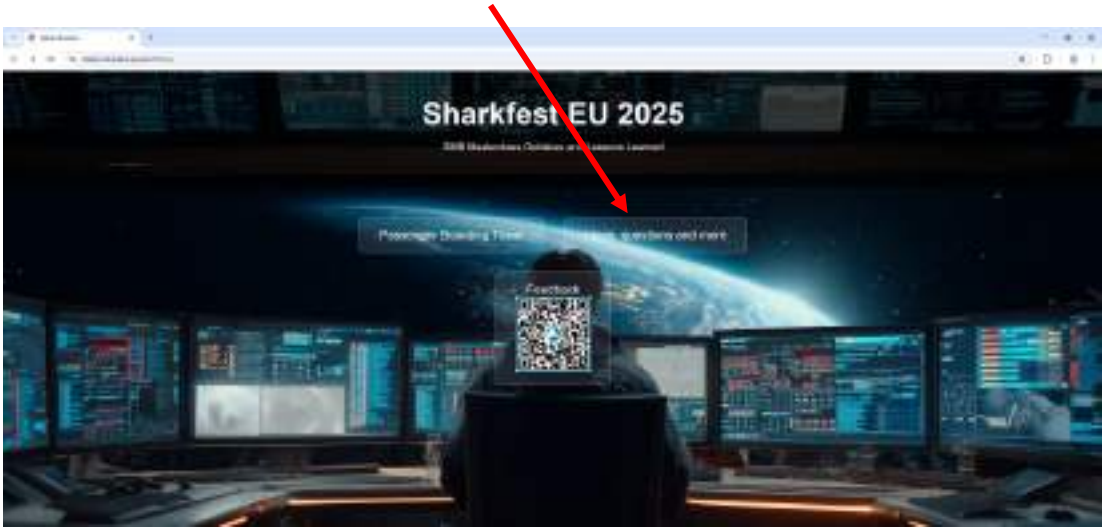
Abstract

- 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 Winsocke 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,
  p*ushing 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

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

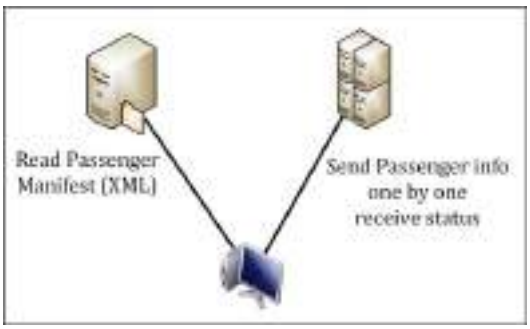
Passenger Boarding Application

- 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

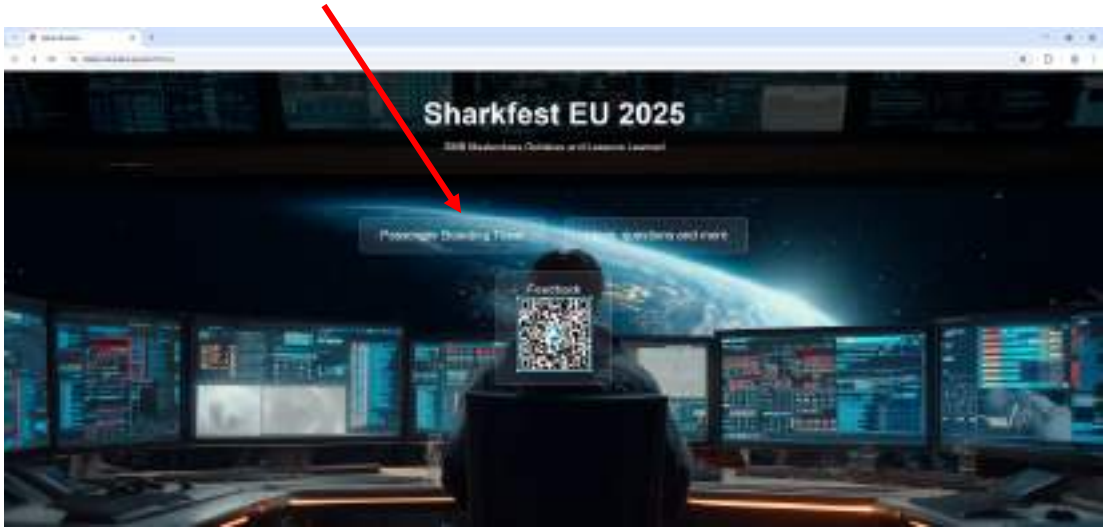
Possible Causes for Poor Performance

- 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

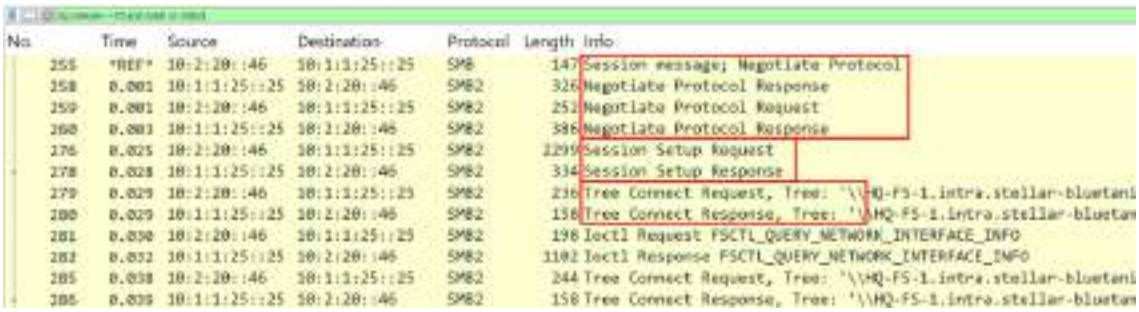
Tree Connect

- 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
255	*REF*	10:2:20::46	10:1:1:25::25	SMB	147	Session message; Negotiate Protocol
258	0.001	10:1:1:25::25	10:2:20::46	SMB2	326	Negotiate Protocol Response
259	0.001	10:2:20::46	10:1:1:25::25	SMB2	252	Negotiate Protocol Request
260	0.003	10:1:1:25::25	10:2:20::46	SMB2	386	Negotiate Protocol Response
276	0.025	10:2:20::46	10:1:1:25::25	SMB2	2295	Session Setup Request
278	0.028	10:1:1:25::25	10:2:20::46	SMB2	334	Session Setup Response
279	0.029	10:2:20::46	10:1:1:25::25	SMB2	236	Tree Connect Request, Tree: "\\HQ-FS-1.intra.stellar-bluetani
280	0.029	10:1:1:25::25	10:2:20::46	SMB2	150	Tree Connect Response, Tree: "\\HQ-FS-1.intra.stellar-bluetan
281	0.030	10:2:20::46	10:1:1:25::25	SMB2	198	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
282	0.032	10:1:1:25::25	10:2:20::46	SMB2	1102	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
285	0.038	10:2:20::46	10:1:1:25::25	SMB2	244	Tree Connect Request, Tree: "\\HQ-FS-1.intra.stellar-bluetani
286	0.039	10:1:1:25::25	10:2:20::46	SMB2	150	Tree Connect Response, Tree: "\\HQ-FS-1.intra.stellar-bluetan

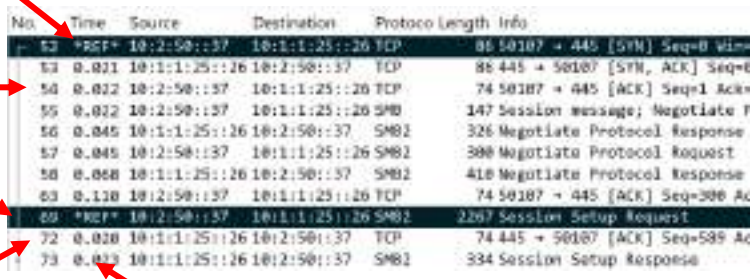
18

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

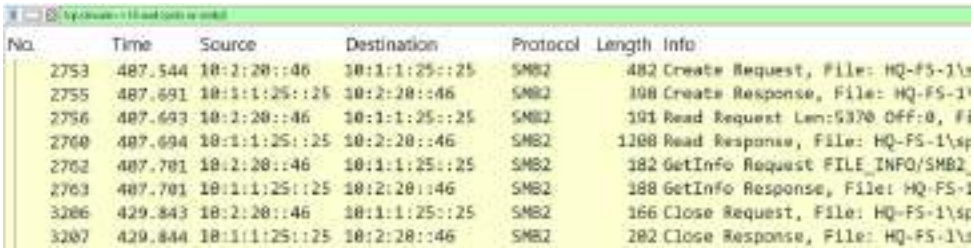
Time of Response : 0.023

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



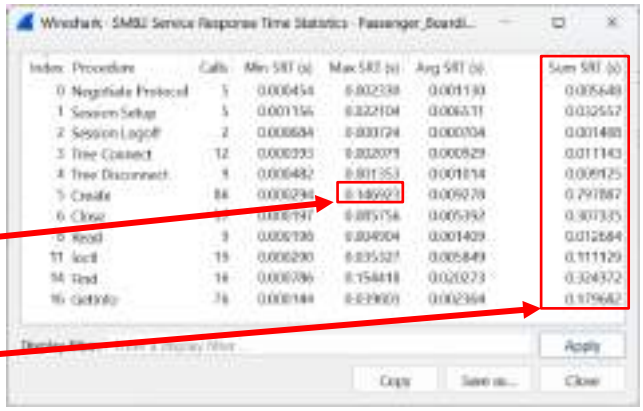
20

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

Ups.
146 msec is long

Overall not a huge issue



21

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

#sf25eu

22

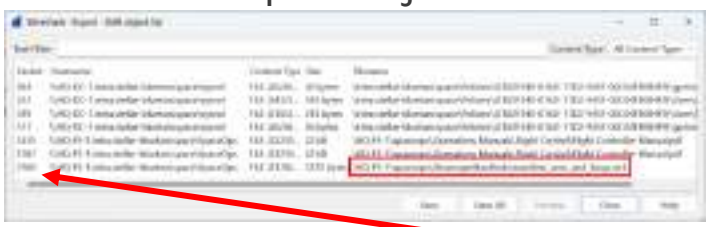
Find Standard Problems

- Use the Wireshark Expert to identify packet loss, window size problems etc.
- A few packet drops do not contribute to the overall response time

23

Rule out SMB Performance

- Step 1: Find the file share
  Use File → Export Objects → SMB to locate the share



- Step 2: Find Read Request
  Serviced within 1 msec
- Step 3: Check Server Performance
  Statistics → Service Response Time → SMB2

24

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

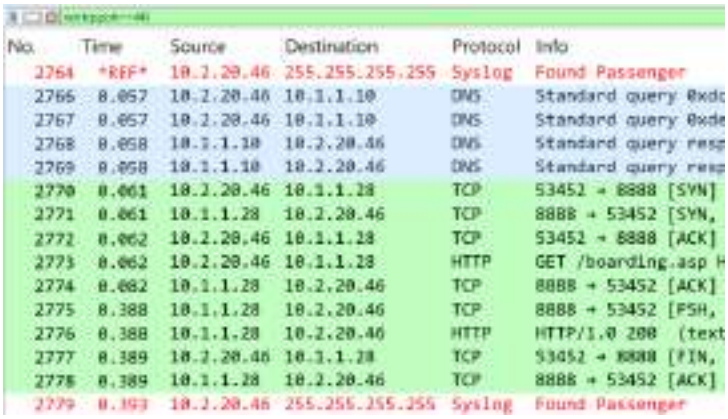
350 msec per Request? The VISUAL approach

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

DNS Query
after 57 msec → slow!

TCP Handshake
1 msec → quick!

HTTP Response
after 326 msec → slow!

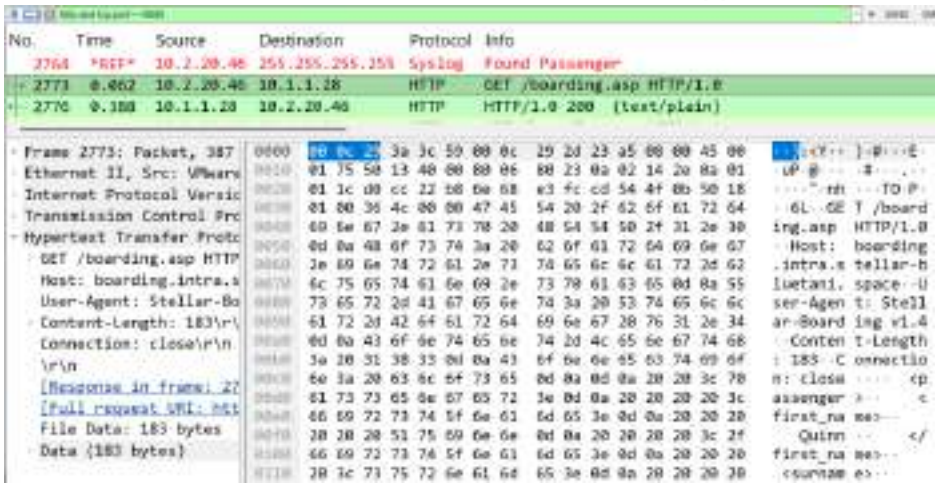


No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found Passenger
2766	0.057	10.2.20.46	10.1.1.10	DNS	Standard query 0xdc
2767	0.057	10.2.20.46	10.1.1.10	DNS	Standard query 0xde
2768	0.058	10.1.1.10	10.2.20.46	DNS	Standard query resp
2769	0.058	10.1.1.10	10.2.20.46	DNS	Standard query resp
2770	0.061	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [SYN]
2771	0.061	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [SYN,
2772	0.062	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [ACK]
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp H
2774	0.082	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [ACK]
2775	0.388	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [PSH,
2776	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (text
2777	0.389	10.2.20.46	10.1.1.28	TCP	53452 → 8888 [FIN,
2778	0.389	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [ACK]
2779	0.393	10.2.20.46	255.255.255.255	Syslog	Found Passenger

27

Examine Data

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

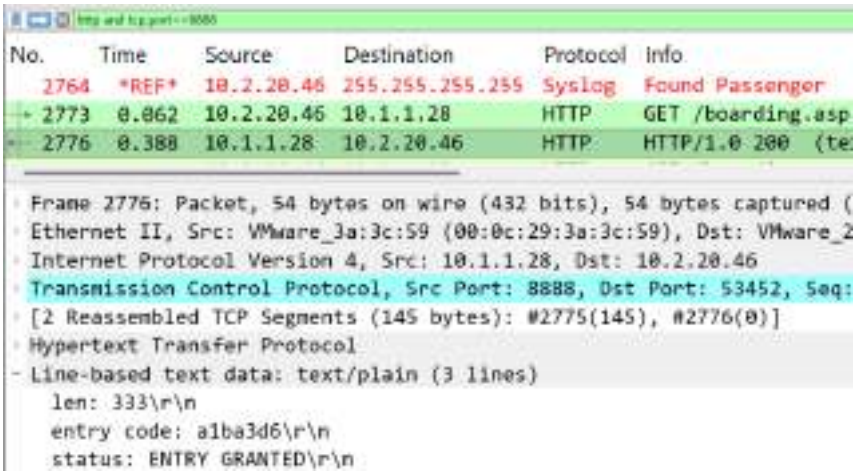


No.	Time	Source	Destination	Protocol	Info
2764	*REF*	10.2.20.46	255.255.255.255	Syslog	Found Passenger
2773	0.062	10.2.20.46	10.1.1.28	HTTP	GET /boarding.asp HTTP/1.0
2776	0.388	10.1.1.28	10.2.20.46	HTTP	HTTP/1.0 200 (text/plain)

28

Server Response

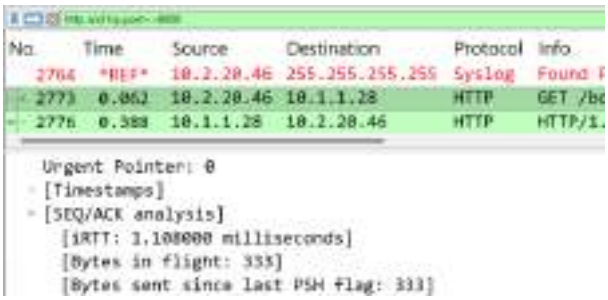
- Notice the response time: 388 – 62 = 326 msec



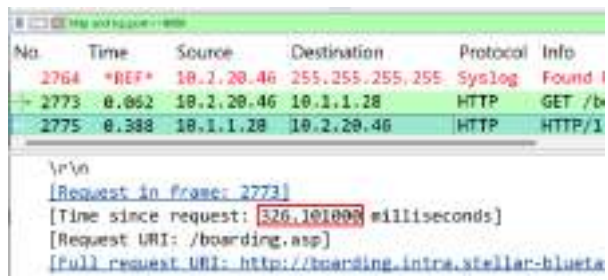
29

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**



30

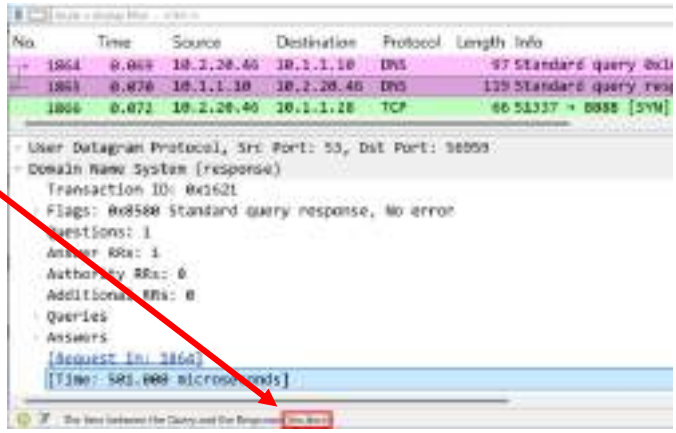
The Systematic Approach

- 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=642
2771	0.061	10.1.1.28	10.2.20.46	TCP	8888 → 53452 [SYN, ACK] Seq=0 Ac
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=642
2783	0.471	10.1.1.28	10.2.20.46	TCP	8888 → 53453 [SYN, ACK] Seq=0 Ac
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	0.771	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!

SharkFest'25 EUROPE

#sf25eu

37