SHARKFEST EU 2019 PACKET CHALLENGE

All challenge trace files can be downloaded from **www.packet-foo.com/sf19eu**. Good luck!

Some HTTP

Trace File: SomeHTTP.pcapng

Something to get you warmed up.

1. What is the server IP address?
2. What is the hostname of the website requested by the browser?
3. What is the HTTP status code given by the web server?
4. What is the FQDN of the location the web server redirects to?
5. How many packets have a FIN flag set?

Bad Address

Trace File: BadAddress.pcapng

Everybody wants an IP address…

1. How many unique non-broadcast MAC addresses can be found in the trace?
2. Why does the filter expression “bootp” give you a warning in Wireshark 3.x and higher?
3. What is the IP address offered to the client?
4. Is the IP address accepted?
5. Why does the client keep requesting an IP address?

Do it Yourself

Trace File: DIY.pcapng

A developer programmed a microcontroller to send data via TCP. Something looks bad though…

1. What is the largest segment size that will work for both client and server?
2. Where was the capture taken (Client local/SPAN/TAP/Server local)?
3. What is the initial round trip time of the connection?
4. How many router hops are between client and server?
5. Why does the transmission of TCP data from 192.168.0.2 to 192.168.0.1 fail?

SMBForce

Trace File: SMBForce.pcapng

For this part of the packet challenge we have shamelessly recycled trace files that were captured for the preparation of the 2018 Sharkfest. You will quickly notice that the trace is rooted in the Star Wars universe. Show us that you are a true Packet Jedi!

1. How many SMB servers are used in this network?
2. There is a Tie Fighter zapping through the network. What is it's IP address?
3. The TIE fighter's pilot (or user) should be authorized by a Kerberos ticket. Oops. For once the pilot slipped and used NTLM for authentication. What is the username?
4. Which SMB or SMB2 Dialect is used by the Tie fighter when approaching Corelia?
5. The last question is only for true Jedi Masters: The username found for question 3 is somewhat short. What is the "Full Name" for that account?

SHARKFEST EU 2019 PACKET CHALLENGE ANSWER SHEET

Fill out this answer sheet and turn it in at the registration table by 6pm on Thursday.

SomeHTTP Trace File: SomeHTTP.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

Bad Address Trace File: BadAddress.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

Do it Yourself Trace File: DIY.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments:

SMBForce Trace File: SMBForce.pcapng

1. _____
2. _____
3. _____
4. _____
5. _____

Comments: