Debugging Connectivity w/OpenSSL

← and *this* guy…

Michael Camp Bentley

The Splunk Doctor | Stage 2 Security

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

About the Author

He’s not too shabby...

.conf19
splunk>

About the Author

…smells of elderberries

Michael Camp Bentley

…aka JKat54

splunk> REVOLUTION AWARDS 2018 WINNER ECOSYSTEM AWARD

Security Engineer @ Stage 2 Security

Splunk Revolution Award Winner 2018

Splunk Trust Architect 2016-2020

Splunk Certified Consultant II

20+ years of IT

SPLUNK TRUST 2016-2017 | splunk> TRUST 2018 | splunk> TRUST 2019 | splunk> TRUST 2020

Common Network Troubleshooting Tools

We all deserve the right to be wrong…

.conf19
splunk>

Common Tools Used

We all deserve the right to be wrong…

"Ping"

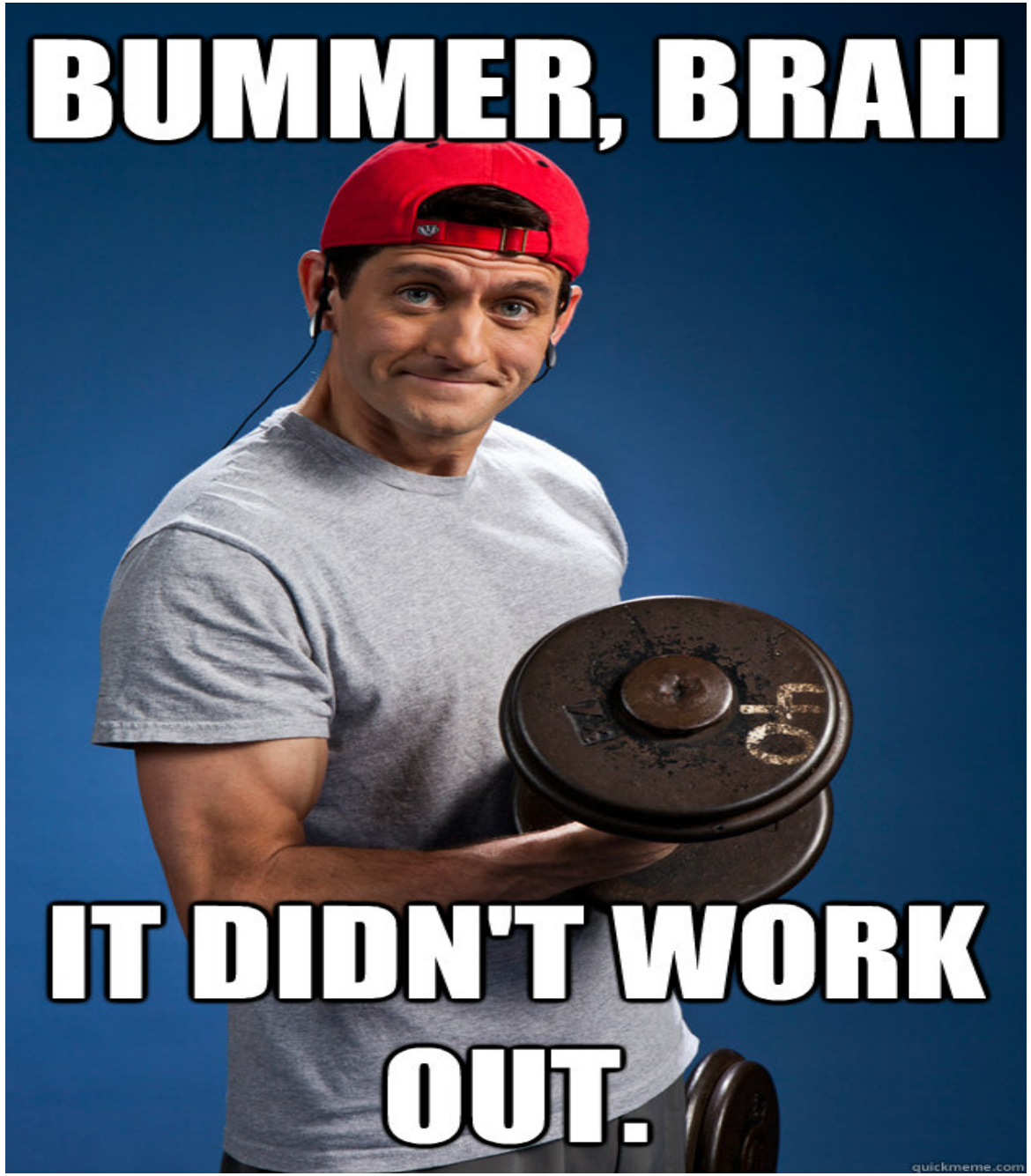
- *Requires ICMP to be enabled*
- *Does not test specific ports*

"Traceroute"

- *Requires ICMP to be enabled*
- *Doesn't test specific ports*
- *Just a bunch of pings*

"Telnet"

- *Is it installed?*
- *Should you install it?*
- *Doesn't work on Secure Connections easily*



Possible Solutions

"Hold my beer…"

.conf19
splunk>

Possible Solutions

"Hold my beer…"

"Netcat"

- *Works for both UDP/TCP!*
- *Is it installed?*
- *Requires some piping to test SSL/TLS*

"Custom Scripts"

- *Beauty is in the eye of the beholder*
- *I can do it in perl, yum install perl?*
- *Not easy to write processes around*

"OpenSSL"

- *Can test most any TCP connection, but not UDP.*
- *Can validate certificates*
- *Comes with every version of Splunk - Even UFs!*

$splunk_home$/bin/openssl

Quick SSL/TLS Primer

"That means Super Splunk Lover, & True Lover of Splunk right?"

.conf19
splunk>

SSL/TLS Primer

"That means Super Splunk Lover, & True Lover of Splunk right?"

Secure Sockets Layer - SSL was one of the first encryption methods used on the interwebs

Transport Layer Security - TLS is one of the latest encryption methods used on the interwebs

History of both:

SSL 1.0 -> SSL 2.0 -> SSL 3.0 -> TLS 1.0 -> TLS 1.1 -> TLS 1.2 (Most of us are here now) -> TLS 1.3

[reference]
https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0

SSL/TLS Options Splunk Supports

"That means Super Splunk Lover, & True Lover of Splunk right?"

- Most versions of SSL/TLS are available, old versions are deprecated and/or unsupported
- Forwarders can use certs for sending / receiving from Peers and Deployment Servers
- Search Heads, Cluster Masters, and Peers can use certs for replicating search artifacts.
- Indexers can use certs for replicating data between Indexers
- KVStore requires a cert for all communications
- For each encrypted connection in splunk you can require valid certificates, check common names of certificates against a list of known common names, and more
- By default $splunk_home$/etc/auth/server.pem is used for web (if https enabled), search, replication, kvstore, and deployment servers. The password for this cert is 'password'.
- **It is very important that you encrypt your splunk traffic with your own certificates!**

Demonstrations

Repeat after me – “Dearest, most gracious and forgiving demo-gods, please let this work…”

.conf19
splunk>

Simple Connectivity Test

…this is easy!

Test if TCP Port 9997 is open to idx1.mycompany.com

openssl s_client -connect idx1.mycompany.com:9997

[“-connect {SERVER}:{PORT}” can be FQDNs if DNS is enabled on your client, or it can be IP addresses as well.]

Simple TCP w/TLS 1.2 Test

…this is an easy 1 too!

Test if TCP Port 9996 is open and accepting TLS1.2 connections on idx1.mycompany.com

openssl s_client -connect idx1.mycompany.com:9996 -tls1_2

Other SSL/TLS Options:

-ssl2, -ssl3, -tls1, -tls1_1, -tls1_2, -no_ssl2, -no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2
These options require or disable the use of the specified SSL or TLS protocols. By default the initial handshake uses a version-flexible method which will negotiate the highest mutually supported protocol version.

Advanced TCP w/TLS1.2 & Client Cert Test

…getting to the cool stuff

Test if TCP Port 9995 is open and accepting TLS1.2 connections on idx1.mycompany.com using/Splunk default server.pem certificate:

openssl s_client -connect idx1.mycompany.com:9995 -tls1_2 -cert /opt/splunk/etc/auth/server.pem

Advanced SMTP Test w/STARTTLS

…ever wanted to script your email?

Test if SMTP port 25 is open and accepting STARTTLS connections on mail.mycompany.com using an interactive prompt:

openssl s_client -connect smtp.gmail.com:25 -tls1_2 -starttls smtp -crlf

[“-starttls smtp” enables STARTTLS support with SMTP]

[“-crlf” enables interactive input from user]

250 XRDST
ehlo
250-mail_gateway Hello [your ip]
250-SIZE 73400320
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-AUTH NTLM LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
AUTH LOGIN dGVzdA==
334 UGFzc3dvcmQ6
cGFzc3dvcmQ=
235 2.7.0 Authentication successful

Links

…getting to the cool stuff

Manual on OpenSSL S_Client:
https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html

TLS/SSL Wikipedia:
https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0

Test Ports w/TA-WebTools and it's testport SPL command:
https://splunkbase.splunk.com/app/4146/#/details

Contact the Author:
https://linkedin.com/in/global-splunk-consultant

Thank You!

…you're awesome

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION