Splunk and FIPS (The F stands for Fun)

Gared Seats
Splunk Engineer | Accenture Federal Services

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.

What this talk will cover

- Just going over some FIPS topics and how it relates to Splunk.

NOTE – This is not a fun SSL and Splunk talk. This is only a tiny portion of what Splunk goes over and relates to FIPS.

NOTE 2 – This is also not a talk about how your auditor will tell you how to enable and use FIPS correctly.

What is FIPS

- **FIPS** (Federal Information Processing Standards) are a set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

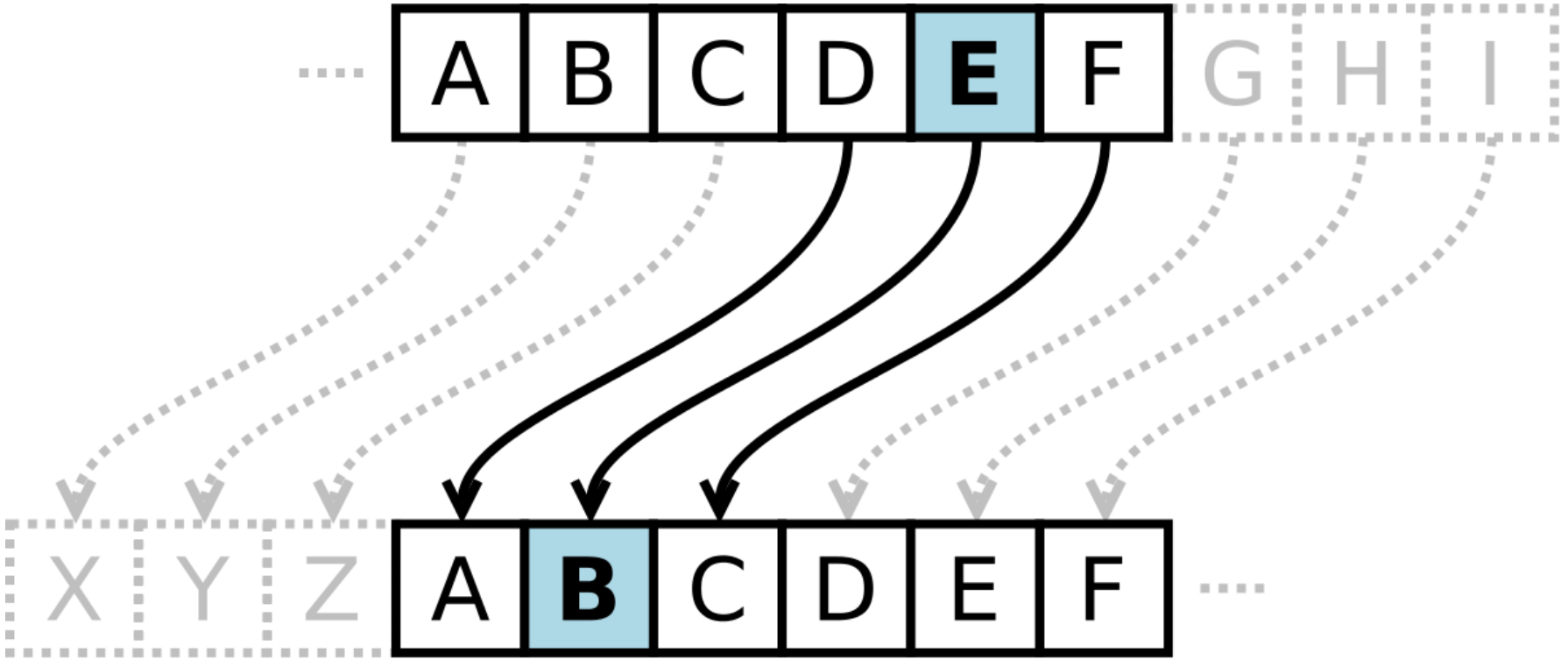
  Note as of Splunk 7.3.1
  Splunk Enterprise and the Universal Forwarder use an embedded FIPS 140-2-validated cryptographic module (Certificate #3126 Module Version fips-2.0.12) running on various platforms per **FIPS 140-2** Implementation Guidance section G.5 guidelines.

The F stands for Fun

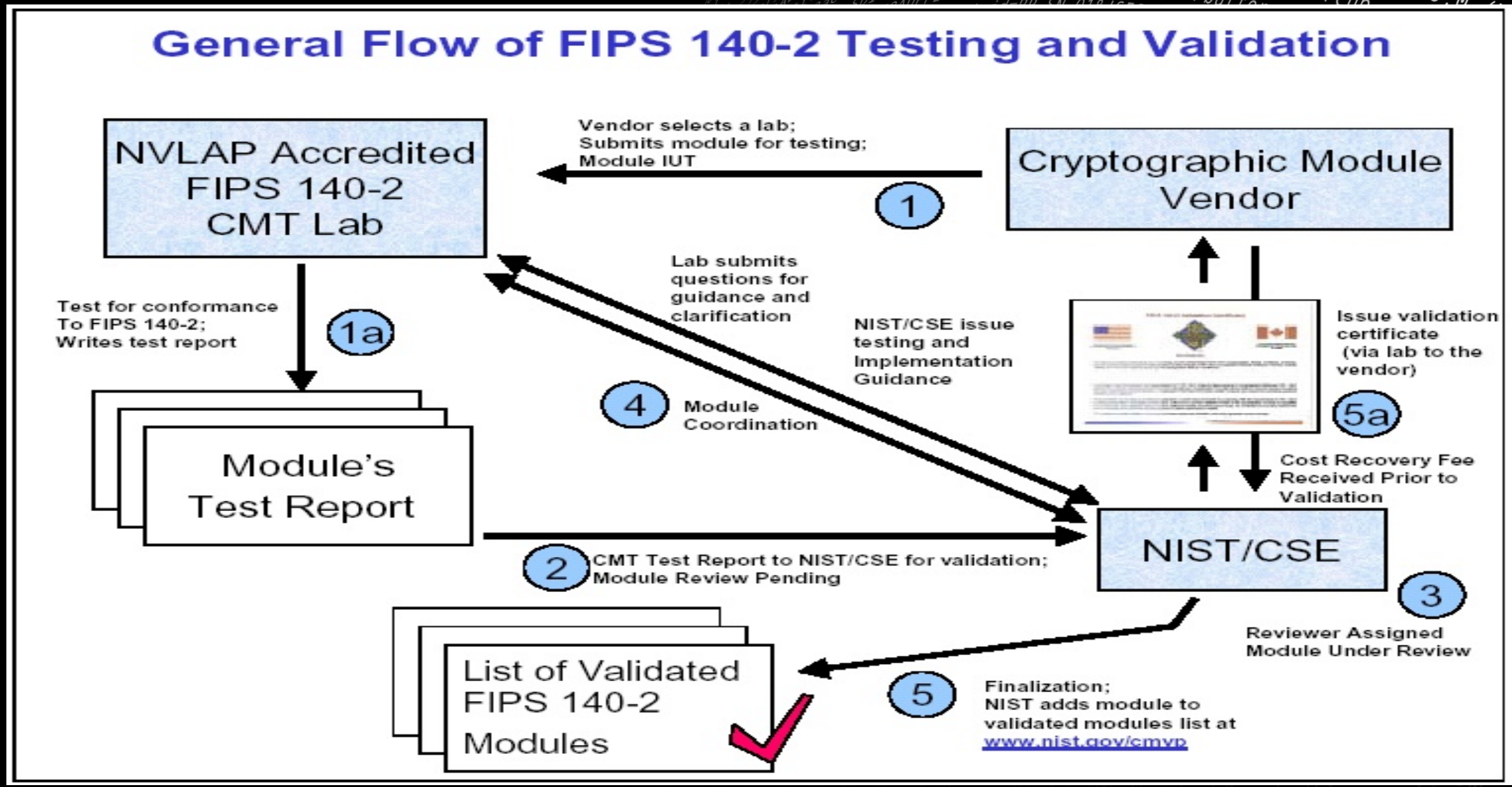
- The joy of having a basic premise of following a certain crypto(cipher) levels forced on to your working systems.
- Following secure policies just because some auditor says so.
- I am sure there is more but lets just stick to these….

Cipher….

- In cryptography, a **cipher** (or **cypher**) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. – Wikipedia



General Flow of FIPS 140-2 Testing and Validation



Splunk with FIPS is Fun!

- Splunk MUST have FIPS set to be enabled **before first start**.
- This is *Auto-Magic if on a Linux System with FIPS enabled.
- This is NOT *Auto-Magic on Windows.

  - Must set **SPLUNK_FIPS=1** in the $SPLUNK_HOME/etc/splunk-launch.conf
- For Windows this will mean you will need to use the CLI to do the install and prevent auto start. (No GUI install for FIPS by default)

  msiexec.exe /I Splunk.msi SPLUNKUSERNAME=SplunkAdmin SPLUNKPASSWORD=Plzchangeme LAUNCHSPLUNK=0 /quiet

*AutoMagic is not a real word

Just to Re-Iterate

- Splunk does **not** enable FIPS auto-magically in Windows even if Windows has FIPS enabled!

Check Your Splunk

- You can check your Splunk in a few ways. (7.2+)

CLI Command

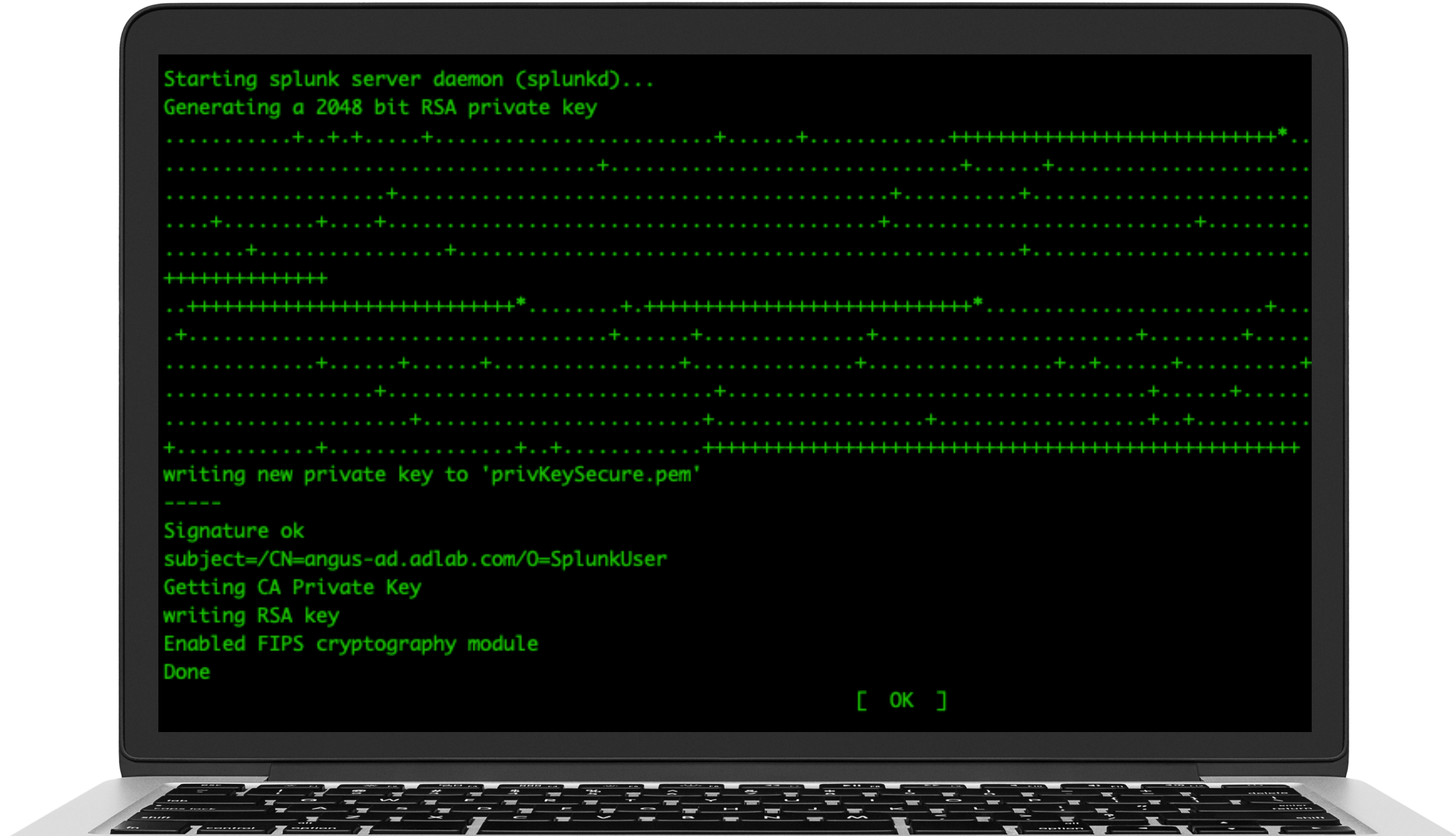
splunk show fips-mode -auth <username>:<password>

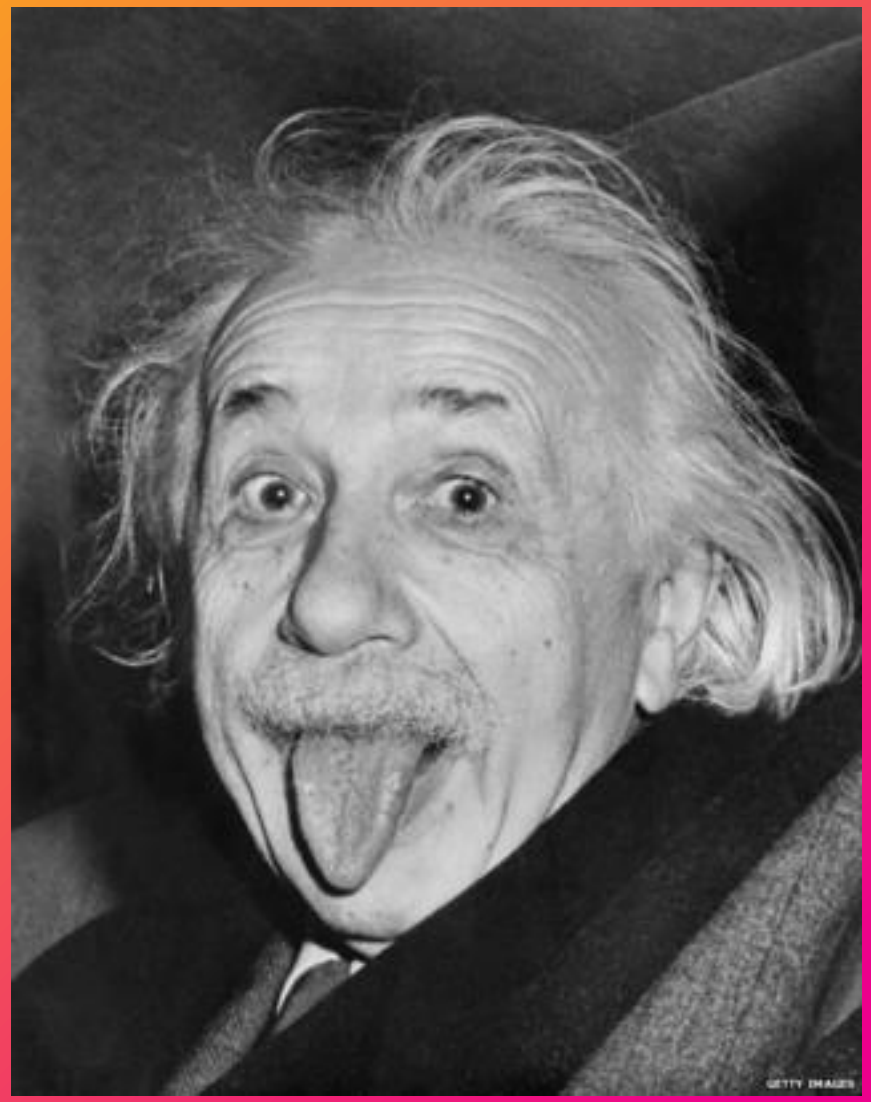
REST CALL

curl -s -k -u <username>:<password>
https://localhost:(mgmt_port)/services/server/info
| grep fips_mode

SEARCH (Also using REST)

"| rest splunk_server=local /services/server/info | fields fips_mode"





The I Stands for Intelligent

Think of how smart you are going to feel after figuring out how this is actually working in your environment.

Right?....

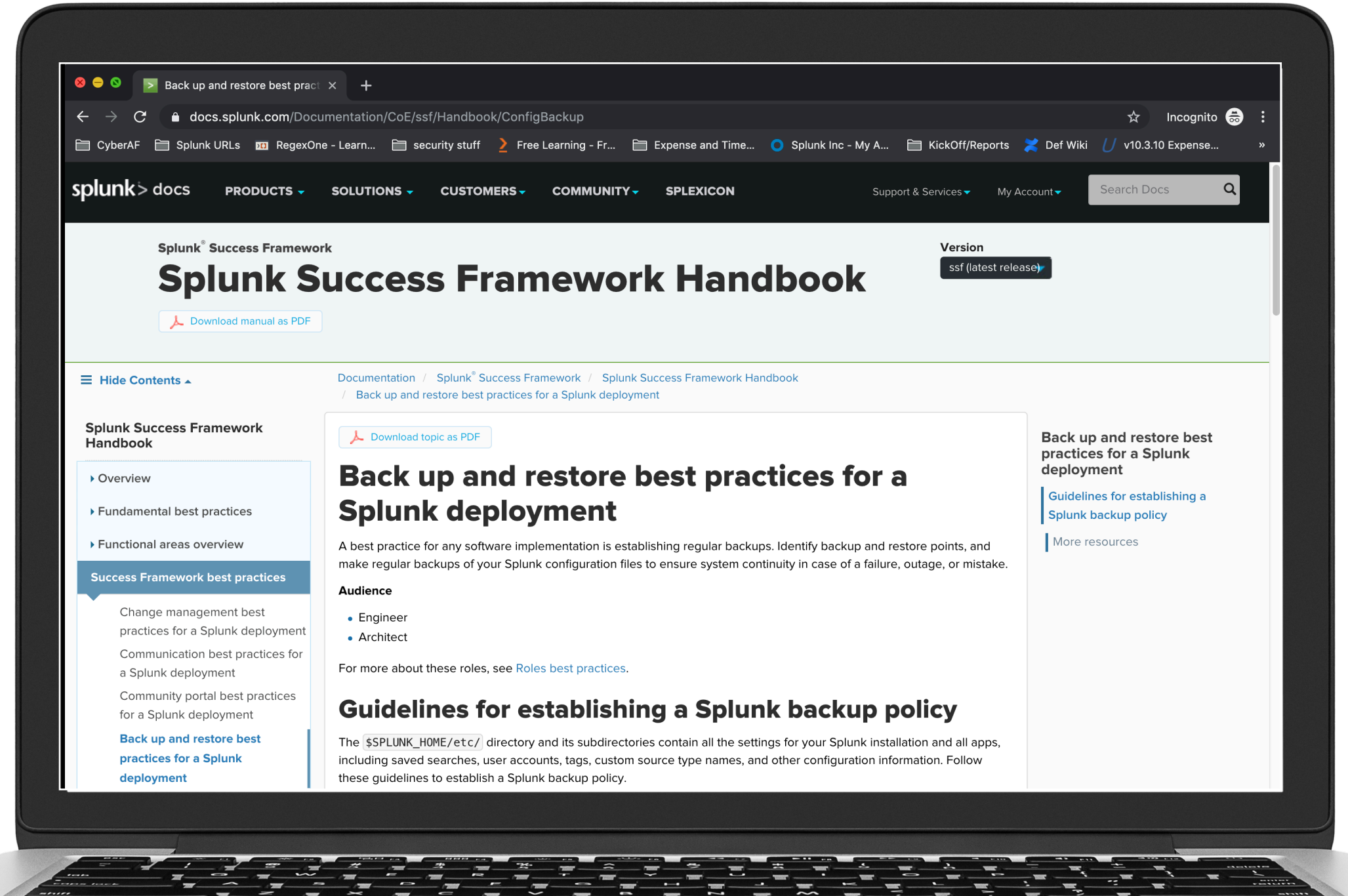
#Winning =

```
[root@localhost etc]# /opt/splunk/bin/splunk show fips-mode
Splunk username: admin
Password:
FIPS mode enabled.
```

But….If your results are something like this…

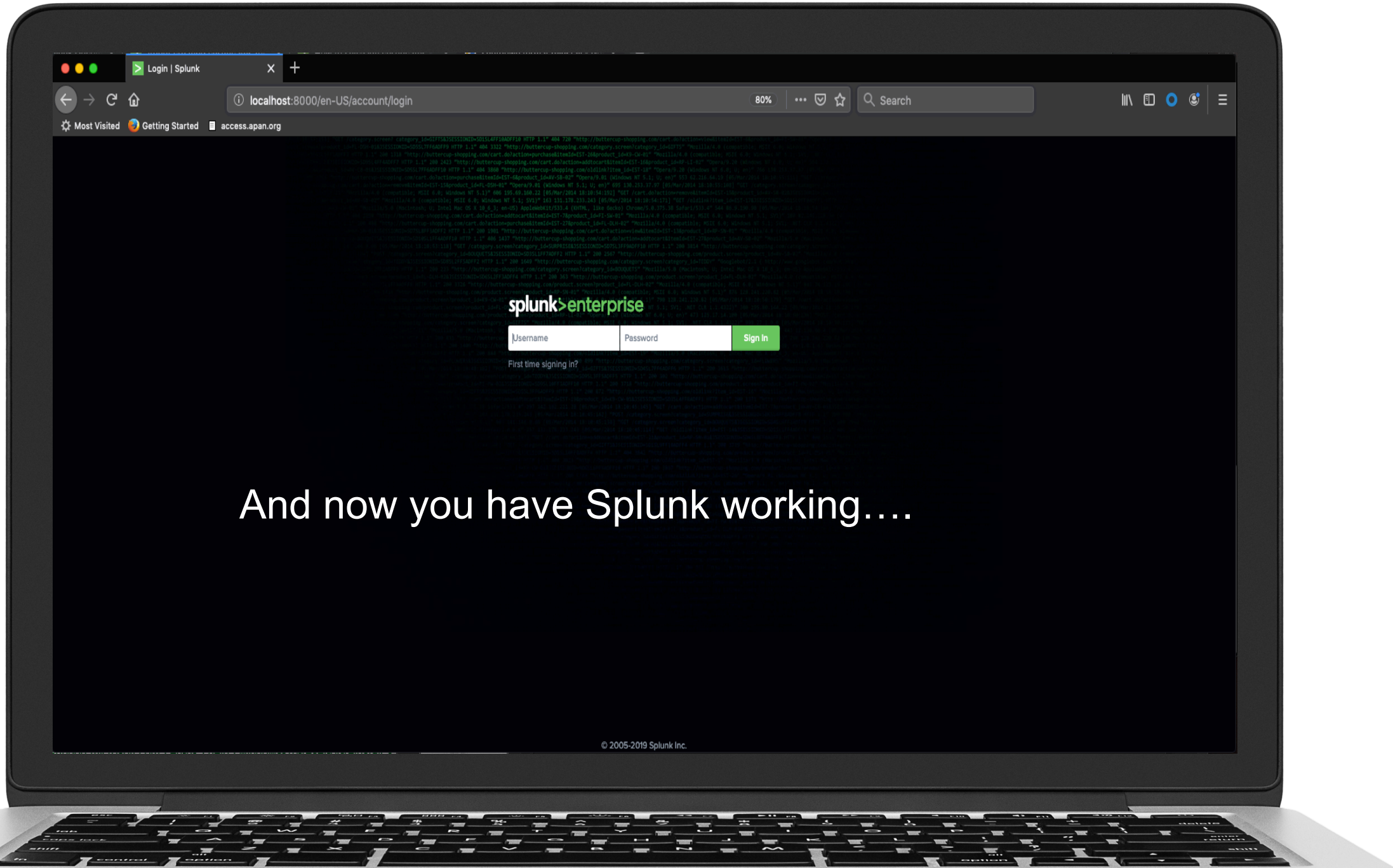
fips_mode

0
or
FIPS mode disabled



Oh no….

SHUTDOWN
FORMAT
REINSTALL!!!



And now you have Splunk working….

Build your Key/Certs the same way

- Making sure you are using FIPS compliant Cipher
- OpenSSL uses FIPS crypto module but it itself is not FIPS (Splunk has this packaged with the Splunk Software so you can run it from the CLI)

$SPLUNK_HOME/bin/splunk cmd openssl genrsa -aes256 -out myCAPrivateKey.key 4096

https://docs.splunk.com/Documentation/Splunk/7.3.2/Security/Validateyourconfiguration

The P Stands for Party

You know what's better than a Party? A FIPS Party building your FIPS certs!!! WOOT WOOT!!!

OpenSSL with FIPS

- When going through the process of you can use the OpenSSL that comes with Splunk to create FIPS compliant Certs. (In Theory….)

  You can confirm with
  ${SPLUNK_HOME}/bin/splunk cmd openssl version
  it should read similar to ‘OpenSSL 1.0.2p-fips 14 Aug 2018’

  set environment variable **OPENSSL_FIPS=1**
  i.e. "**export OPENSSL_FIPS=1**" before generating the certificates with command
  ${SPLUNK_HOME}/bin/splunk cmd openssl

Default server.conf on Splunk 7.3.2 FIPS

```
# SSL settings
# The following provides modern TLS configuration. This configuration drops support
# for old Splunk versions (Splunk 5.x and earlier).
# To add support for Splunk 5.x:
#     - set sslVersions & sslVersionsForClient to tls
#     - and add AES256-SHA to the cipherSuite
# The following non-forward-secrecy ciphers were added to support the kv store:
#     AES256-GCM-SHA384:AES128-GCM-SHA256:AES128-SHA256.
sslVersions = tls1.2
sslVersionsForClient = tls1.2
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
SHA256:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-ECDSA-
AES128-SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:AES128-SHA256
ecdhCurves = prime256v1, secp384r1, secp521r1
```

https://docs.splunk.com/Documentation/Splunk/8.0.0/Security/Ciphersuites

Totally no issues….

KVSTORE Crashes and Fails to Start. I've seen this at multiple sites both with default certs and new Certs being introduced.

- **WARN** IntrospectionGenerator:resource_usage - WatchdogInit - Could not find a valid key='path' under stanza='watchdogaction:script' in conf='server'. Using default value.

  Soooo….this happens because the Kvstore seems like it is still trying to leverage the default certs which is just can't seem to find.

KVSTORE Configs

Server.conf

```
[sslConfig]
sslRootCAPath = $SPLUNK_HOME/etc/auth/FIPS-Splunk/Root_cert.pem
sslPassword = Password

[kvstore]
#serverCert = /opt/splunk/etc/auth/FIPS-Splunk/
# Note this line didn't work.
caCertPath = /opt/splunk/etc/auth/FIPS-Splunk/Root_cert.pem
sslKeysPath = /opt/splunk/etc/auth/FIPS-Splunk/serverchain.pem
sslKeysPassword = Passwor
sslPassword = Password
```

NOTE – even though it says "KeysPath" is "deprecated" you will need to point to the serverchain pem file for this to work. Also if $SPLUNK_HOME path does not work, try to use the full path.

Troubleshoot FIPS

- If you are in FIPS mode and your usual RSA encrypted private keys do not work, they might be incompatible with FIPS. To mitigate this issue, you can convert your Privacy Enhanced Mail (PEM) private key to PKCS#8 format to make them compatible.
- Confirm you are running in FIPS mode. (Yes Really check)
- If you have problems running a Splunk app, confirm that it is certified to run in FIPS mode and does not have dependencies on cryptographic algorithms that FIPS disables (such as MD5 and RC4).
  Note – Some Apps with modular inputs have this issue.
  cough DBConnect App *cough*

And the S stands for…..

“Someone clearly lied to you. FIPS is not any of those ”fun” things…..

Quote - Me

Key Takeaways

1. FIPS should be used when it **Needs to be**
2. FIPS is not a magic bullet to make you “Auto-Secure”
3. FIPS should also not be underestimated as it can break more than you expect.

Q&A

.conf19
splunk>

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION