Splunk4Admins - Encryption of Data in Transit (DIT)

Cheat Sheet for Lab Commands

Task 1:

Follow the guide to download and install splunk securely.

```
sudo su -
cd /opt/showlab
mkdir s4a-s-aio
cd /tmp
wget -O splunk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz
"https://download.splunk.com/products/splunk/releases/X.X.X/linux/splu
nk-x.x.x-xxxxxxxxxxxx-Linux-x86_64.tgz"
tar -xf /tmp/splunk-xxxx-release.tgz -C /opt/showlab/s4a-s-aio/
chown -R splunk: /opt/showlab/s4a-s-aio
exit
```

Task 2:

```
mkdir /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts
cd /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl genrsa -aes256
-out myCertAuthPrivateKey.key 2048
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl req -new -key
myCertAuthPrivateKey.key -out myCertAuthCertificate.csr
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl x509 -req -in
myCertAuthCertificate.csr -sha512 -signkey myCertAuthPrivateKey.key
-CAcreateserial -out myCertAuthCertificate.pem -days 1095
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl genrsa -aes256
-out myServerPrivateKey.key 2048
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl req -new -key
myServerPrivateKey.key -out myServerCertificate.csr
```

```
/opt/showlab/s4a-s-aio/splunk/bin/splunk cmd openssl x509 -req -in
myServerCertificate.csr -SHA256 -CA myCertAuthCertificate.pem -CAkey
myCertAuthPrivateKey.key -CAcreateserial -out myServerCertificate.pem
-days 1095
```

Task 3:

```
cat myServerCertificate.pem myServerPrivateKey.key
myCertAuthCertificate.pem > myCombinedCertificate.pem
```

Task 4:

```
cd all_indexer_base
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local
vi inputs.conf
```

```
# BASE SETTINGS
[splunktcp-ssl://9997]

# SSL SETTINGS
[SSL]
serverCert =
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

```
vi server.conf
```

```
[sslConfig]
sslRootCAPath =
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.pem
```

```
/opt/showlab/s4a-s-aio/splunk/bin/splunk restart splunkd
cp
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.p
em /opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/
cp
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.p
em /opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/
mv myCombinedCertificate.pem myClientCertificate.pem

cd /opt/showlab/s4a-s-uf/splunkforwarder/etc/apps
mkdir all_forwarder_outputs
cd all_forwarder_outputs
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local
vi outputs.conf
```

```
# BASE SETTINGS

[tcpout]
defaultGroup = primary_indexer
forceTimebasedAutoLB = true
forwardedindex.0.whitelist = (_audit|_introspection|_internal)

[tcpout:primary_indexer]
server = localhost:9997
disabled = 0
clientCert =
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myClientCertificate.
pem
useClientSSLCompression = true
sslPassword = myCertificatePassword
```

```
# sslCommonNameToCheck = aio.mycompany.com
# sslVerifyServerCert = true
```

vi server.conf

```
[sslConfig]
sslRootCAPath =
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myCertAuthCertificat
e.pem
```

/opt/showlab/s4a-s-uf/splunkforwarder/bin/splunk restart

Task 5:

cd /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/
cp myServerPrivateKey.key mySplunkWebPrivateKey.key
openssl rsa -in myServerPrivateKey.key -out mySplunkWebPrivateKey.key
cp myCombinedCertificate.pem mySplunkWebCertificate.pem
cd /opt/showlab/s4a-s-aio/splunk/etc/apps
mkdir all_search_base
cd all_search_base
mkdir metadata
mkdir local
cd metadata
vi local.meta

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

cd ../local
vi web.conf

```
[settings]
httpport = 8443
enableSplunkWebSSL = true
privKeyPath =
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/mySplunkWebPrivateKey.key
serverCert =
```

```
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/mySplunkWebCertificate.pem
```

/opt/showlab/s4a-s-aio/splunk/bin/splunk restart

Task 6:

cd /opt/showlab/s4a-s-aio/splunk/etc/apps/all_indexer_base/local

```
[sslConfig]
enableSplunkdSSL = true
sslRootCAPath =
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.pem
serverCert =
/opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

vi /opt/showlab/s4a-s-aio/splunk/etc/system/local/server.conf

```
#[sslConfig]
#sslPassword = $7$oE9ikOJjA9cnEaOfw+NaLbzufl3TqLyigBHfwWYpYgm8hhziWqx9fg==
```

/opt/showlab/s4a-s-aio/splunk/bin/splunk restart
cp -r
/opt/showlab/s4a-s-uf/splunkforwarder/etc/apps/all_deploymentclient/
/opt/showlab/s4a-s-aio/splunk/etc/deployment-apps/

cd
/opt/showlab/s4a-s-uf/splunkforwarder/etc/apps/all_deploymentclient/lo
cal

```
[sslConfig]
enableSplunkdSSL = true
sslRootCAPath =
```

```
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myCertAuthCert
ificate.pem
serverCert =
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myCombinedCert
ificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

vi /opt/showlab/s4a-s-uf/splunkforwarder/etc/system/local/server.conf

```
#[sslConfig]
#sslPassword =
$7$oE9ikOJjA9cnEaOfw+NaLbzufl3TqLyigBHfwWYpYgm8hhziWqx9fg==
```

/opt/showlab/s4a-s-uf/splunkforwarder/bin/splunk restart