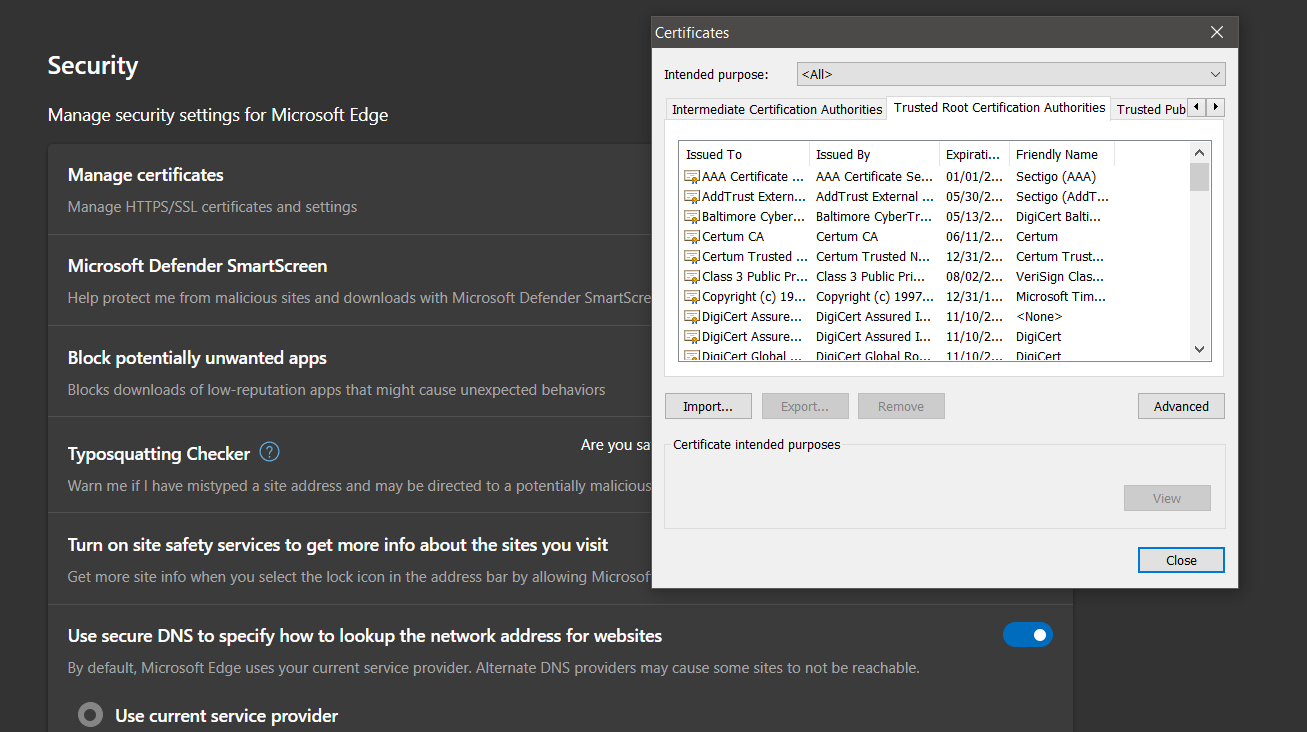
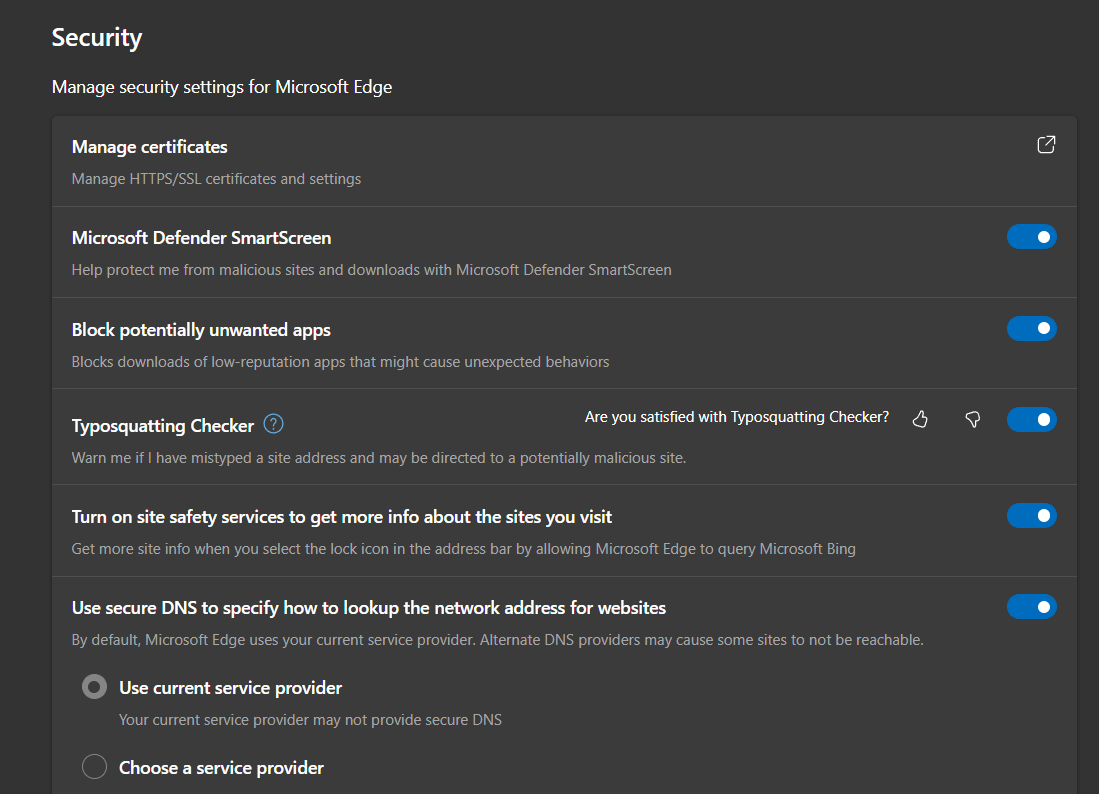
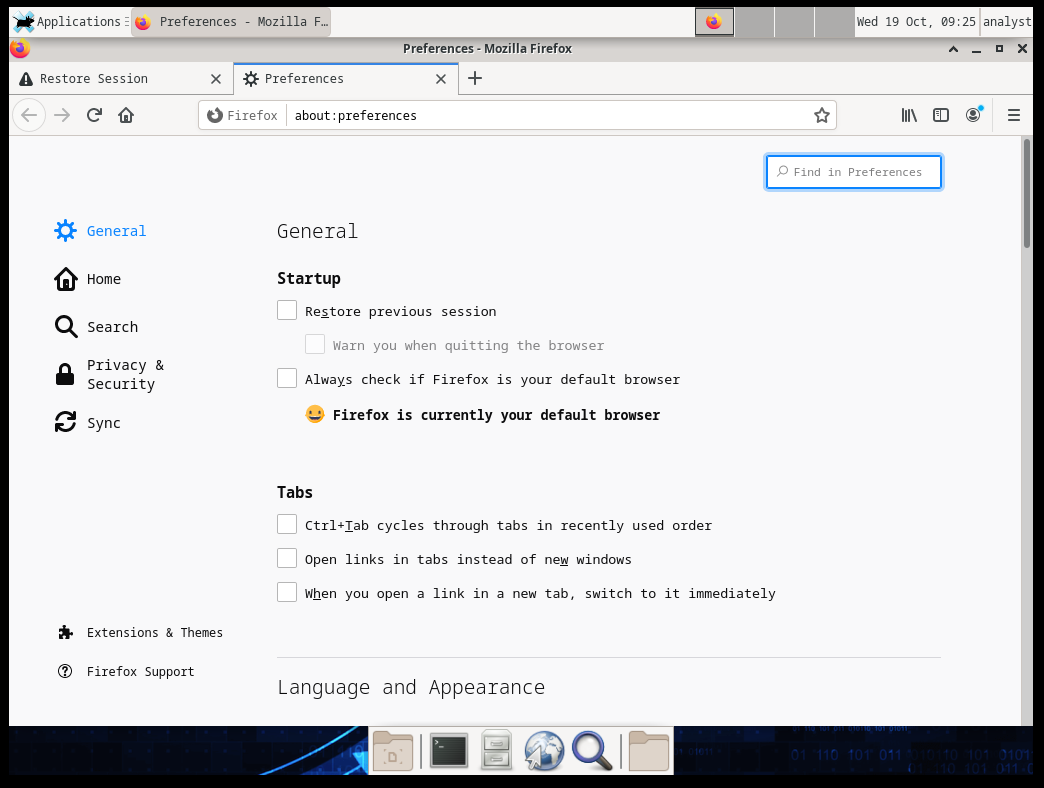
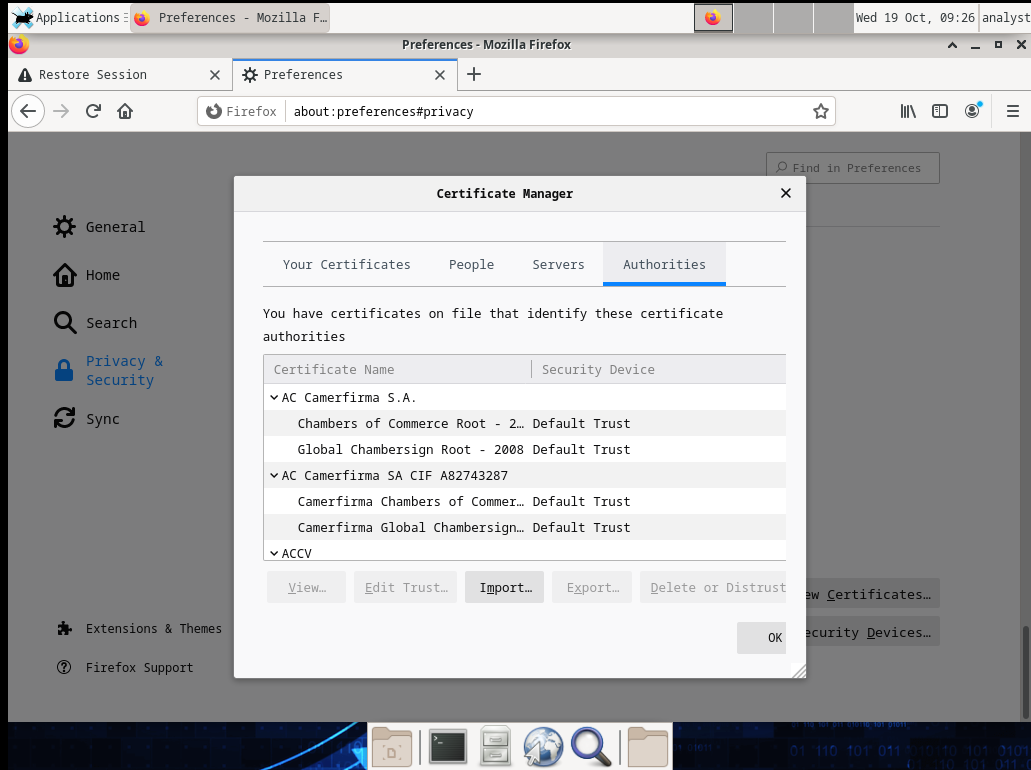
Part 1: Certificates Trusted by Your Browser

Step 1: Display the Root Certificates in Chrome.

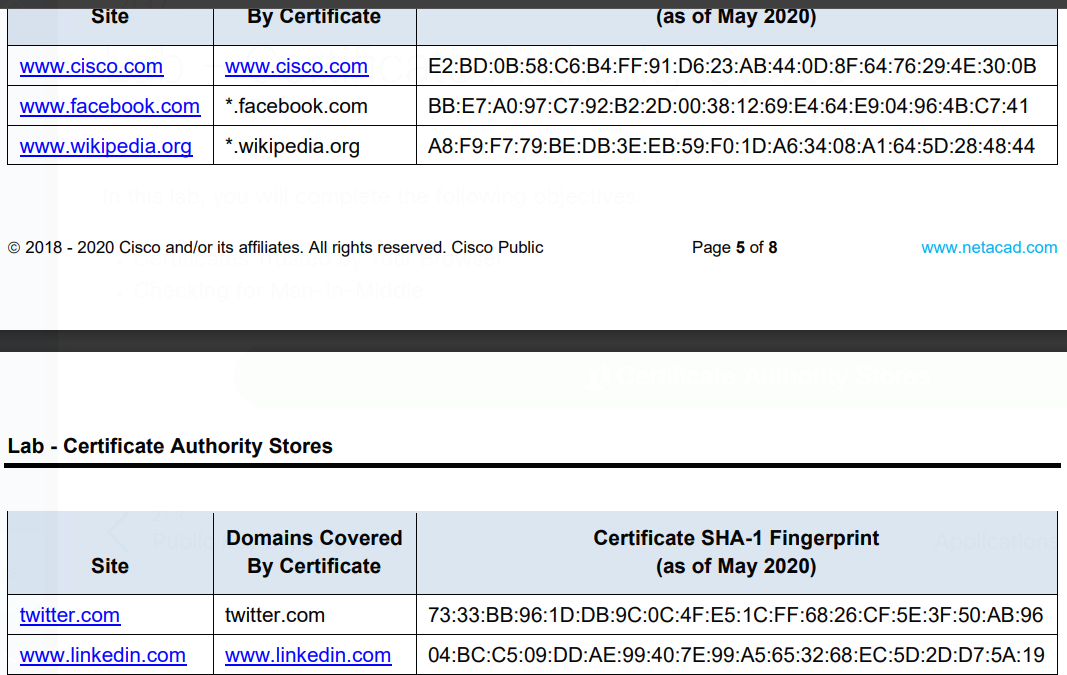
Step 2: Display the Certificates in the CA Store in Firefox.



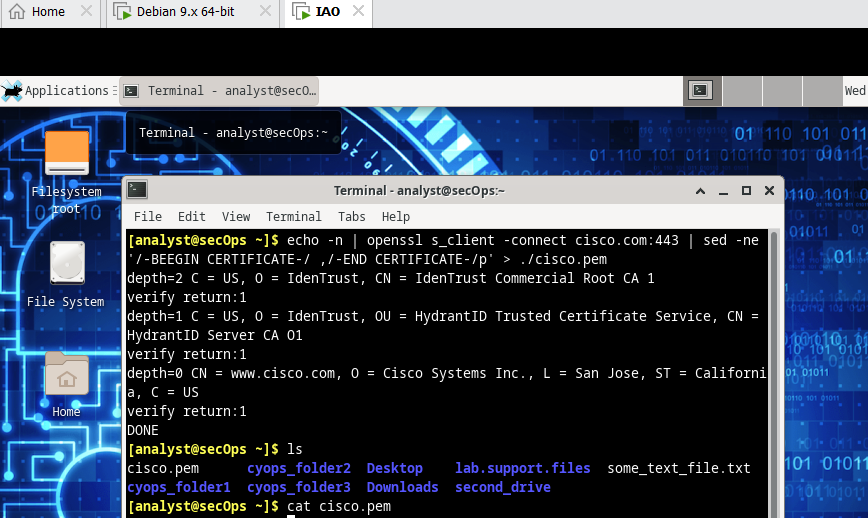


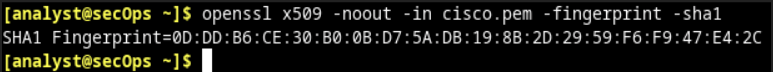
Part 2: Checking for Man-In-Middle

Step 1: Gathering the correct and unmodified certificate fingerprint.



A certificate's fingerprint is the unique identifier of the certificate. Microsoft Internet Explorer calls it Thumbprint. Browsers tend to display it as if it were a part of the certificate. It is not a part of the certificate, but it is computed from it.

Step 2: Gather the certificate fingerprint in use by the CyberOps Workstation VM.  



SHA1 is the hash algorithm use in this case because it is more secure than MD5.

Step 3: Compare the Fingerprints

The fingerprint is different because arcording to secure issue cisco need to change their fingerprint in a period of time. So the public fingerprint is not always correct. We should use this method to retrieve the correct fingerprint.