PKI TLS Assignment

1. Create two Linux VMs, call one Client and the other Server
2. On Server, install NGINX, easy-rsa
3. On the Client, install cURL, tcpdump

TLS

1. On the Server
   1. Create a website
   2. Configure https using self signed ECC certificates
   3. Configure your server to only answer to TLSv1.2 or TLSv1.3
2. On the client
   1. Start tcpdump
   2. Use cURL to connect to the Server
   3. Stop tcpdump
   4. Review the PCAP in Wireshark to identify the TLS handshake and make sure the right protocol and certificates were used

mTLS

1. On the Server
   1. Create a CA using easy-rsa
      1. Use ECC instead of RSA
   2. Create certificates for the Server and the Client
   3. Configure the server to only send the webpage if the Client is validated using mTLS
2. On the Client
   1. Start tcpdump
   2. Use cURL to try to connect to the Server
   3. Stop tcpdump
   4. Review the PCAP in Wireshark and the NGINX log to see how MTLS failed
   5. Start tcpdump
   6. Use cURL + certificates issued in 6(b) to access the server
   7. Stop tcpdumo
   8. Review the PCAP in Wireshark and the NGINX log to see how MTLS succeed
3. On the Server
   1. Revoke the Client’s certificate
   2. Issue a new Client certificate
   3. How do you inform the server that the Client’s old certificate should be rejected?

Discussion

* How should you protect the PKI you created on the Server?
* How often should regenerate the CRL?
* What differences do you notice in the TLS handshake during mTLS vs TLS?
* What do you think would happen if you tried to use a client that was configured to only use RSA ciphers?