Documentazione MMSproxy

1. Importazione ed esportazione immagine Docker di Ubuntu (questo passo è opzionale)

importare l'immagine da un file è opzionale, in alternativa Docker tenterà di scaricare il file dai propri repository se esso non fosse presente localmente.
questa fase è necessaria solamente se si ha intenzione di utilizzare il tool all'interno di un container Docker.

1.1 caricamento immagine da file

per caricare l'immagine di ubuntu su docker per poter eseguire i container bisogna eseguire con i privilegi di root da terminale nella stessa cartella del file ubuntu.tar il comando: docker load < ubuntu.tar

1.2 esportazione immagine

per esportare l'immagine in un archivio eseguire con i privilegi di root il comando: docker save ubuntu > ubuntu.tar

2. file e cartelle

all'interno dell'archivio sono presenti tre cartelle:

- **certificati**: contenente i certificati utilizzati per testare il tool
- **CLIENT_SERVER**:
- **sslproxy**: contiene il tool con i file di configurazione
  all'interno sono presenti:
  - **MMS_proxy**: è uno script che avvia il container Docker dell'attaccante
  - **Dockerfile**: un file necessario per la creazione del container
  - **MMSproxy**: cartella contenente i file che verranno caricati nel container, contiene:
    - **init**: script di inizializzazione
    - **start**: script di avvio di sslproxy
    - **SSLproxy-master**: cartella con all'interno il tool sslproxy
    - **valori_MMS**: file di testo con le misure che si vuole far sostituire a quelle intercettate da sslproxy

3. Presupposti

- si suppone di aver compromesso il client e di avere ottenuto una copia del certificato e chiave client utilizzati per stabilire una connessione TLS con il server.
- bisogna aver generato un certificato e una chiave di una root CA
- concatenare il certificato della root CA appena generato con quello presente della CA fidata presente nel client.

nei container che ho utilizzato il file concatenato è client1.cer presente all'interno della cartella:
/CLIENT_SERVER/libiec61850-1.4/examples/tls_client_example

4. Copia certificati

copiare i certificati nelle seguenti posizioni:
posizione certificati client: /sslproxy/MMSproxy/SSLproxy-master/src/certificati/client
il nome del certificato client deve essere: client1.cer
il nome della chiave del client deve essere: client1-key.pem

i certificati della root CA devono trovarsi all'interno della cartella:
/sslproxy/MMSproxy/SSLproxy-master/src/certificati/ca
il nome del certificato della root CA deve essere: root.cer
il nome della chiave della root CA deve essere: root.key

5. File di configurazione per valori MMS

all'interno della cartella sslproxy/MMSproxy è presente un file di configurazione valori_MMS, esso contiene i valori MMS che verranno sostituiti a quelli ricevuti, ha il seguente formato:

TotW: 3.33
TotVaR: 2.22
TotVa: 444.44
Hz: 28.10
PhA: 11.2
PhB: 22.3
PhC: 22.4

i valori relativi ai valori float possono essere modificati da questo file.
sslproxy leggerà questo file e sostituirà i valori dal pacchetto contenente le misure con quelli presenti sul file.

6. Esecuzione container

per eseguire il container eseguire da terminale lo script MMS_proxy situato all'interno della cartella sslproxy.

una volta aperto il container eseguire prima lo script init
per eseguire sslproxy dal container eseguire lo script start passando come parametri i due indirizzi ip dei bersagli.