W4D4 – Pratica

FASE 1 – CONFIGURAZIONE DELLE MACCHINE CLIENT\* E SERVER\*\*

KALI:

1. Modifico IP a 192.168.32.100(/24)
2. Installo il modulo apache2 (sudo apt-get install apache2)
3. Abilito a2enmod ssl per abilitare HTTPS su apache2
4. Riavvio apache2
5. Creo una directory dove mettere il mio certificato ssl autofirmato
6. E creo il certificato
7. Modifico poi il file .conf per configurare HTTPS  
   Immagine che contiene testo, schermata

   Descrizione generata automaticamente
8. Abilito il sito SSL con a2ensite default-ssl
9. Riavvio apache2

WINDOWS:

1. Modifico IP a 192.168.32.101(/24)
2. Inserisco in file hosts la dicitura 192.168.32.100 epicode.internal
3. Scarico e installo Wireshark

FASE 2 – ACCESSO A EPICODE.INTERNAL DA W7 CON HTTPS

1. Apro Wireshark
2. Accedo a https://epicode.internal da browser
3. Recupero il traffico con wireshark
4. Risultato:  
   

FASE 3 – CONFIGURAZIONE KALI PER HTTP

1. Apro il file 000-default.conf
2. Metto ServerName a epicode.internal
3. E riavvio apache2

FASE 4 – ACCESSO A EPICODE.INTERNAL DA W7 CON HTTP

1. Apro Wireshark
2. Accedo a https://epicode.internal da browser
3. Recupero il traffico con wireshark
4. Risultato:  
   

FASE 5 – ANALISI

I MAC ADDRESS sono:

SERVER (KALI): 08:00:27:1E:36:4A

CLIENT (WINDOWS 7): 08:00:27:BF:BB:1B

LE DIFFERENZE:

Numero di pacchetti: HTTPS invia un numero di pacchetti maggiore rispetto a HTTP

Il traffico HTTP rivela tutto il contenuto della richiesta e della pagina in chiaro, mentre HTTPS cifra tutto, rendendo solo visibile l’handshake TLS e il traffico cifrato

In HTTP la porta è la :80 mentre in HTTPS è la :443