INTRODUZIONE ALL'HACKING

(Esercizio di fine modulo)

Ho usato Apache 2 per svolgere l'esercizio, visto che la traccia non richiedeva un software server open-source specifico, mentre per l'indirizzi IP ho deciso come anche cosigliato nella call di pratica di mantere gli indirizzi IP gia configurati in precedenza senza stravorgerli.

CONFIGURAZIONE SERVER HTTP

1) Per prima cosa ho verificato lo stato di Apache 2 controllando che il servizio fosse attivo

2) Ho verificato i siti abilitati (epicode-http)

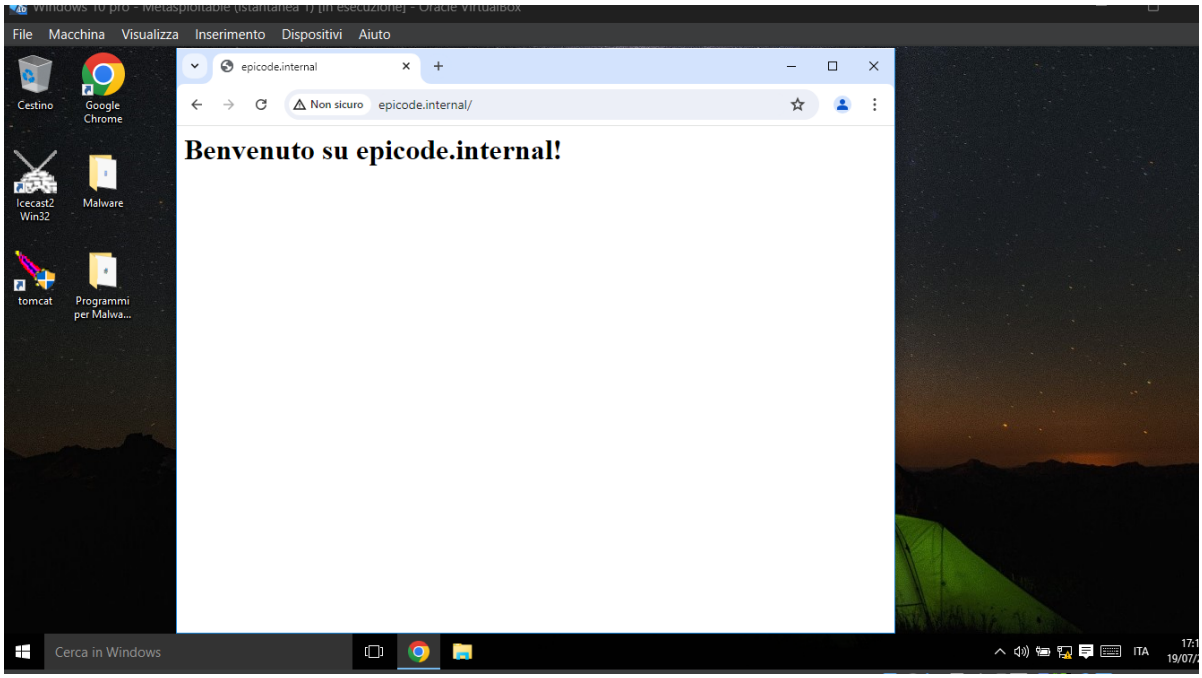
3) Ho creato il Virtual Host HTTP modificando il contenuto su Kali

4) Ho abilitato il sito e riavviato Apache 2

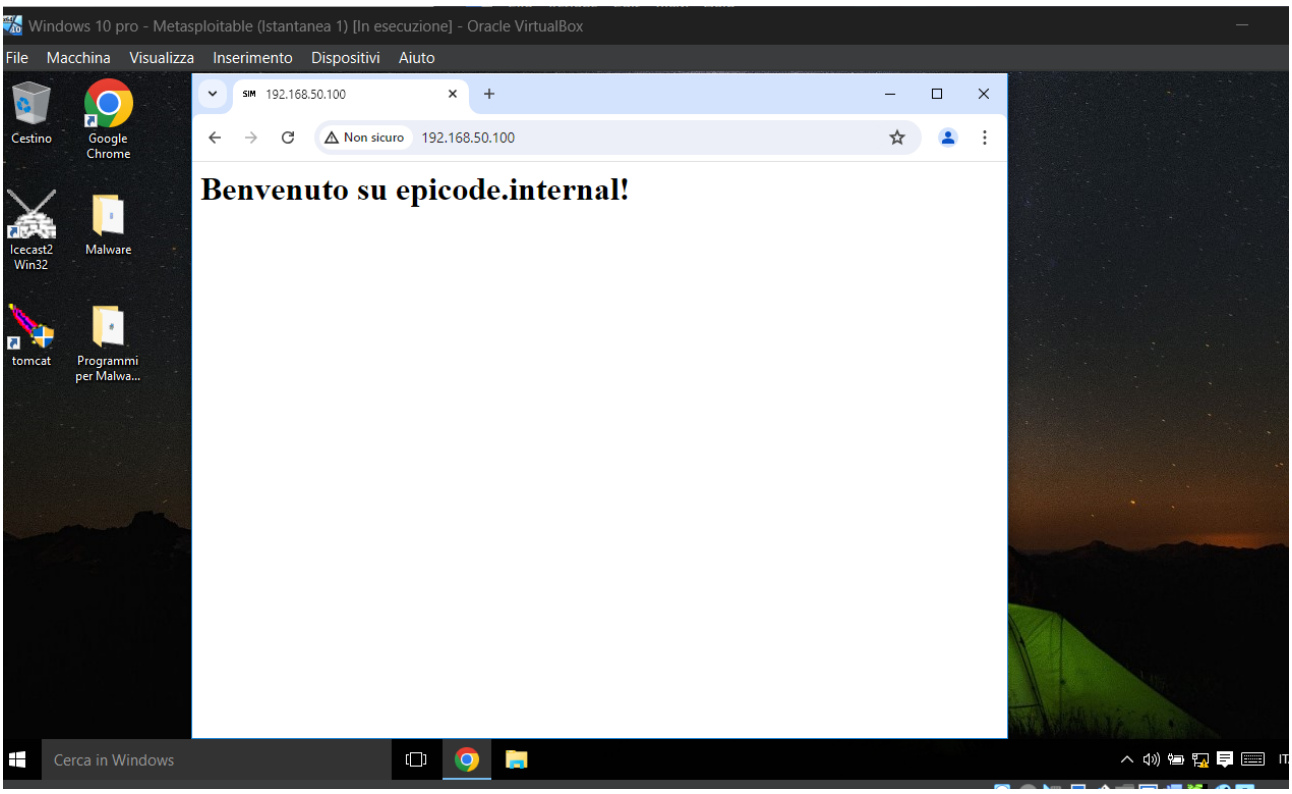
5) Infine ho effettuato i test di accesso:

Windows

Scrivendo Link 1 http://epicode.internal



Link 2: http://192.168.50.100

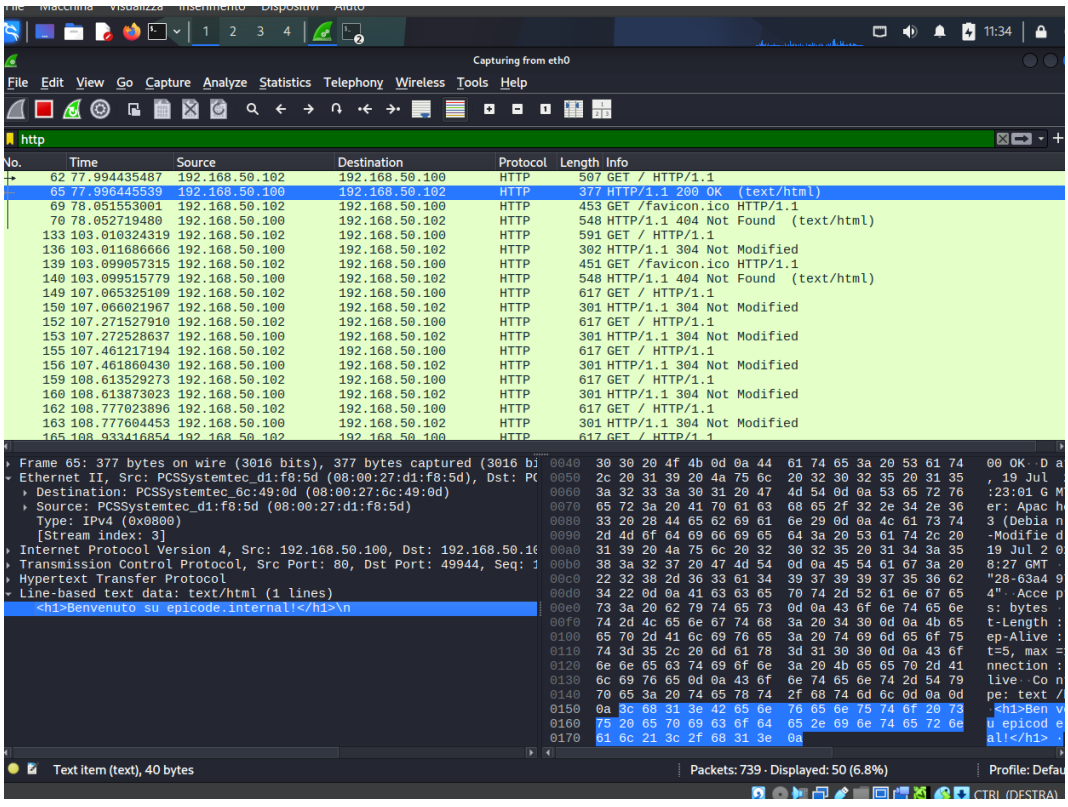


Intercettazione del Traffico HTTP con Wireshark

Ho avviato Wireshark selezionando eth0

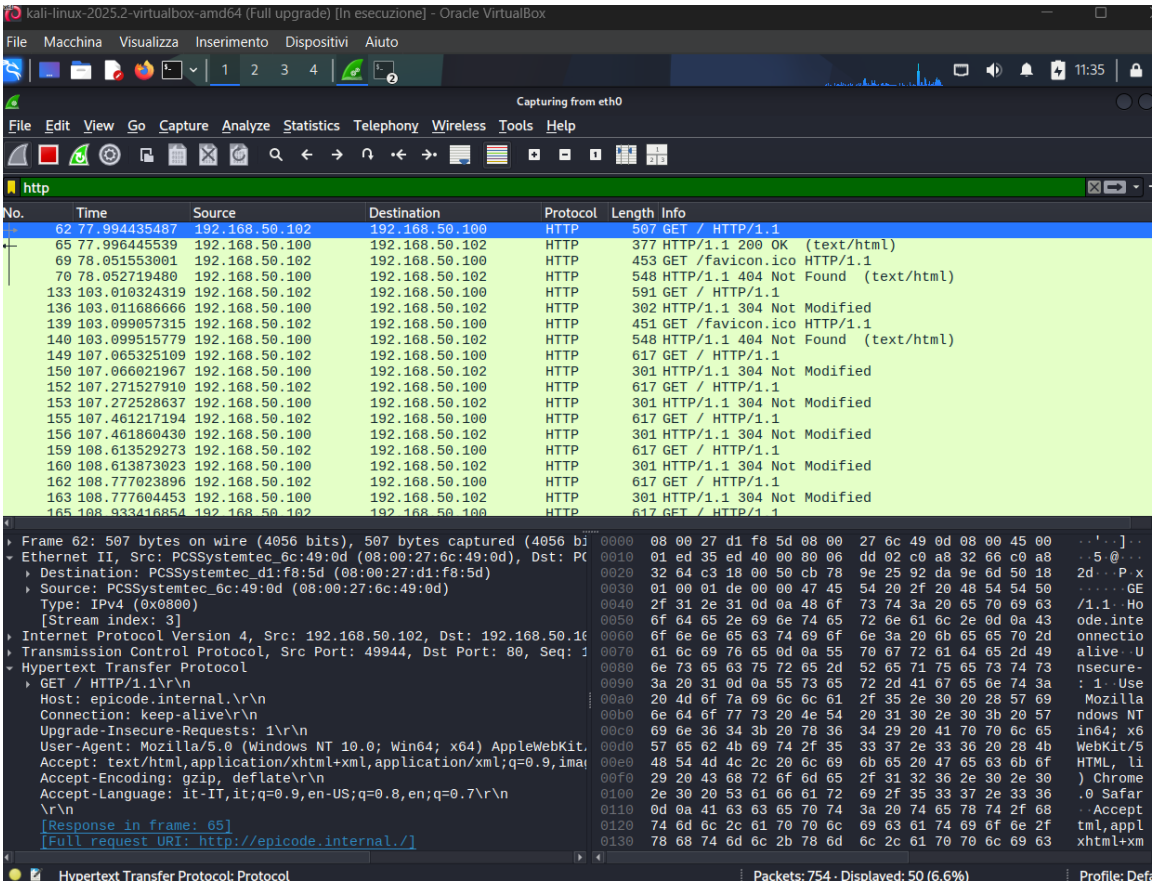
1 Paccheto

Ho effettuato l'accesso su Google Chrome con http://epicode.internal per generare traffico e ho cliccato su HTTP 377 HTTP/1.1 200 ok , nella sezione Ethernet II si trovano i MAC addres



2 Paccheto

Ho effettuato l'accesso su Google Chrome con http://192.168.50.100 per generare traffico per un 2 pacchetto e ho cliccato su HTTP 507 GET HTTP/1.1, nella sezione Ethernet II si trovano i MAC address



PASSAGGIO AL SERVER HTTPS

Configurazione Server HTTPS

1) Come prima cosa ho disattivato l' HTTP con i realativi comandi su Kali per effettuare il passaggio a HTTPS

2) Poi ho generato il certificato self-signed creandolo con epicode.internal, gli altri campi gli ho lasciati di default

3) Successivamente ho verificato il file controllando i suoi permessi e che sia presente

4) Ho configurato il virtual Host HTTPS scrivendo il contenuto sulla Kali

5) Poi ho attivato il modulo SSL e il sito e infine ho riavviato Apache 2

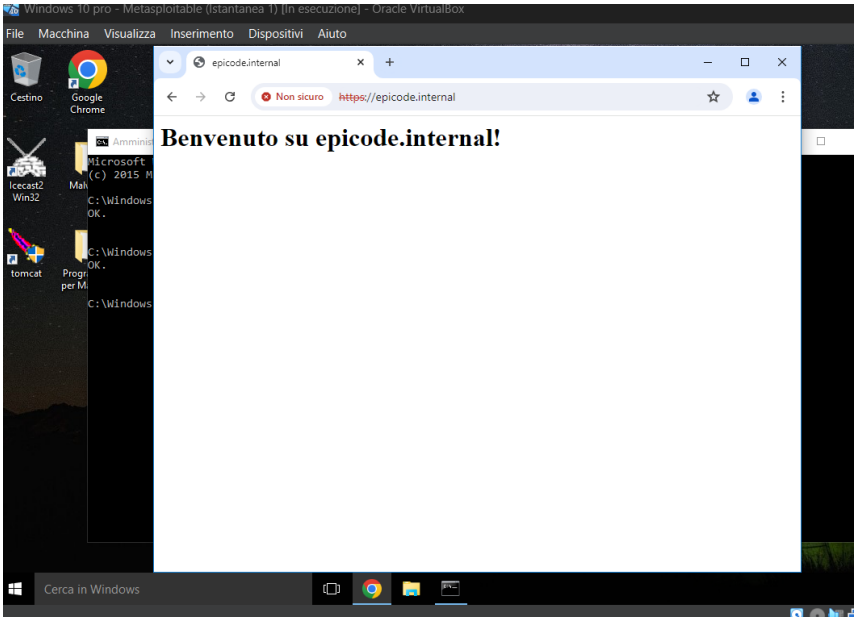
6) Ho verificato che Apache 2 ascolta sulla porta 443

7) Ho disattivato momentanemante i firewalls su windows solo il tempo per svolgere e completare l'esercizo https

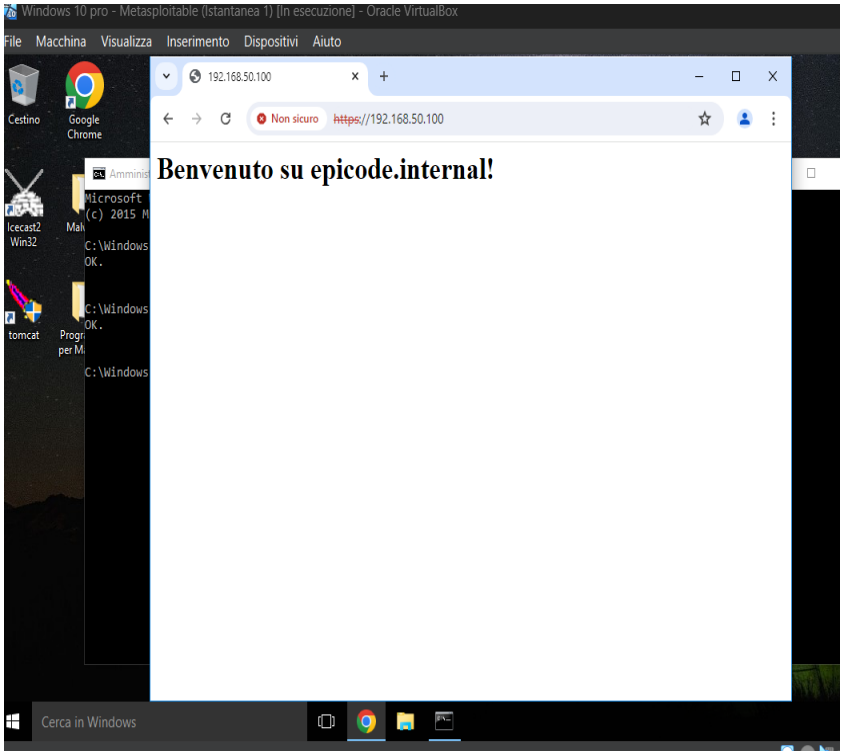
8) Infine ho effettuato i test di accesso:

Windows

Scrivendo Link 1: https://epicode.internal



Link 2: https://192.168.50.100

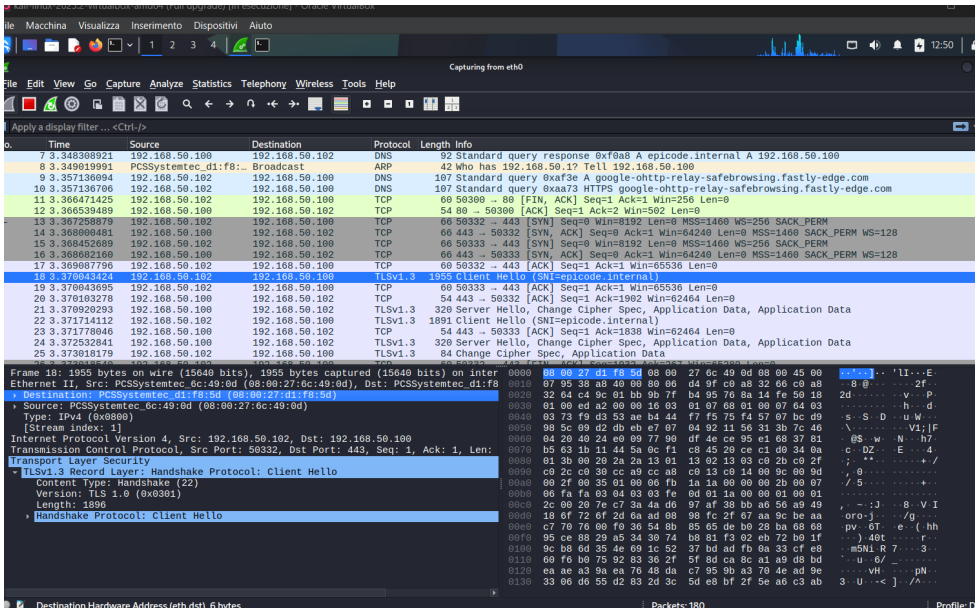


Intercettazione del Traffico HTTPS con Wireshark

Ho avviato Wireshark selezionando eth0

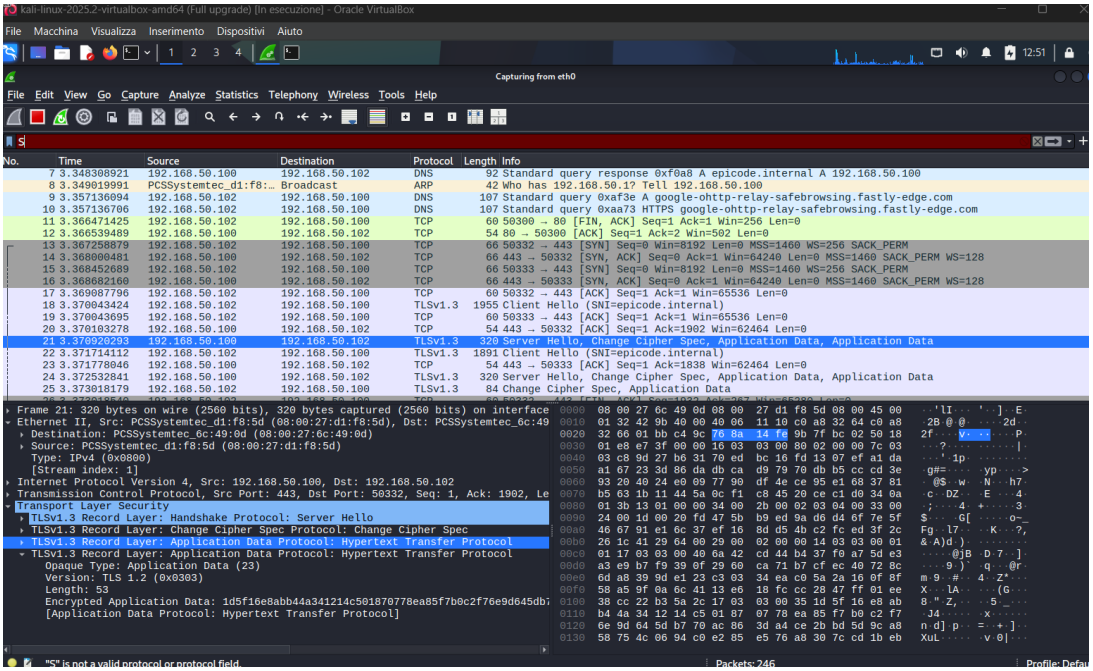
1 Paccheto

Ho rieffettuato l'accesso questa volta con https://epicode.internal per generare traffico e ho cliccato su TLSv1.3 1955 Clien Hello (SNI=epicode.internal), nella sezione Ethernet II si trovano i MAC addres



2 Paccheto

Ho effettuato l'accesso con https://192.168.50.100 per generare traffico per un 2 pacchetto e ho cliccato su TLSv1.3 320 Server Hello, Chamge Cipher Spec, Application Data, Application Data, nella sezione Ethernet II si trovano i MAC address



HO ANALIZZATO LE DIFFERENZE TRA IL TRAFFICO HTTP E HTTPS

HTTP

Usa la porta 80

Con Wireshark posso filtrare il traffico con tcp.port == 80 per HTTP

I dati viaggiano in chiaro.

Non è sicuro: un attaccante può intercettare o modificare i dati (tipo password) con un attacco man-in-the-middle.

E' più veloce, ma senza protezione.

HTTPS

Usa la porta 443:

Con Wireshark posso filtrare il traffico con tcp.port == 443

I dati sono crittografati con TLS/SSL: e il contenuto appare come dati binari illeggibili, a meno che non abbia la chiave privata del server.

Usa TLS per crittografare tutto e autenticare il server con un certificato, proteggendo i dati sensibili.

E' un po' più lento per via dell'handshake TLS, che richiede uno scambio iniziale di messaggi, ma offre molta più sicurezza.

Ho dedotto che

Gli indirizzi MAC (come quello del PC: 192.168.50.102 o del server, 08:00:27:d1:f8:5d) non cambiano, perché dipendono dalla rete fisica e non dal protocollo.

HTTPS è la scelta migliore per la sicurezza, anche se più complesso.