CONSEGNA CORSO CYBER SECURITY W3D4

STUDENTE: ORAZIO MORGILLO

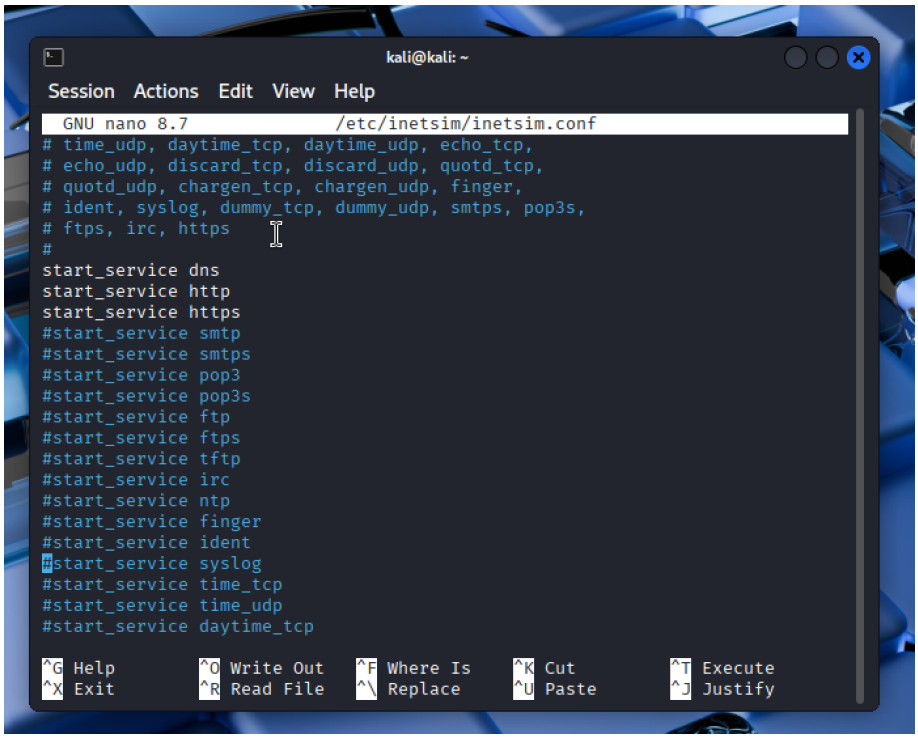
L'obiettivo dell'esercizio è quello di simulare con le macchine virtuali un'architettura in cui un client server (windows) richiede tramite browser una risorsa all'hostname (kali) epicode.internal. successivamente bisogna intercettare le comunicazioni e il contenuto delle richieste https e http in entrata ed uscita su whireshark

Premessa: come visto a lezione di pratica e come riscontrato da altri colleghi, ho problemi con il dns server e quindi non riesco a visualizzare la pagina epicode.internal.
Da browser su windows sono riuscito a richiedere le pagine https://192.168.50.100 e http://192.168.50.100

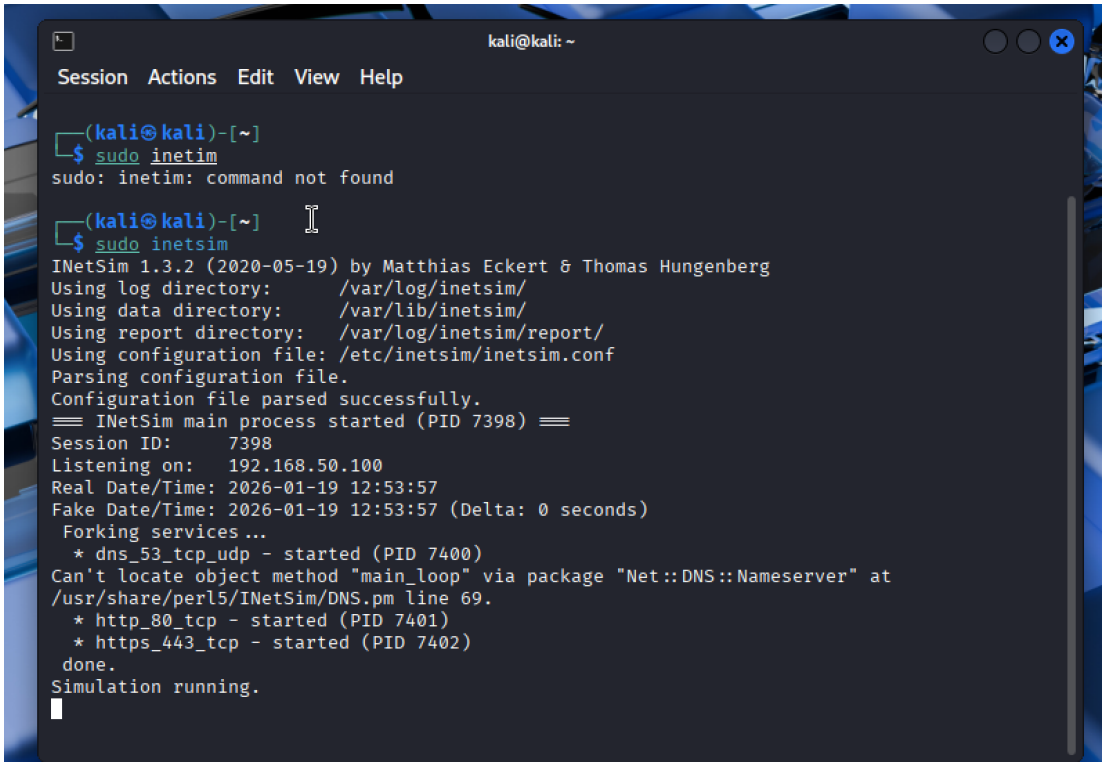
Requisiti:
Kali: 192.168.50.100
Windows: 192.168.50.102
HTTPS server: attivo
HTTP server: attivo
DNS server: attivo

Svolgimento:

per prima cosa, su Kali ho controllato che le due macchine fossero in comunicazione tramite il comando ping 192.168.50.102.
successivamente, ho attivato i servizi https, http e dns dal terminale con il comando sudo nano /etc/inetsim/inetsim.conf e configurato l'indirizzo ip 192.168.50.100 su service_bind_address e dns_default_ip.
Inetsim è un simulatore di servizi internet preconfigurato su Kali linux.

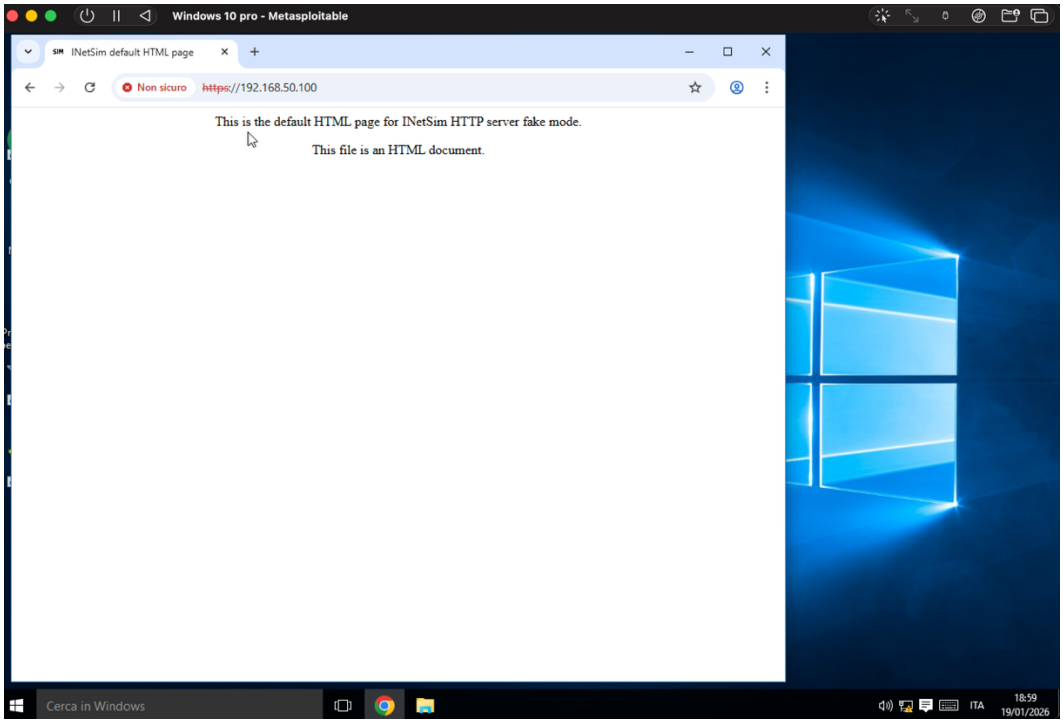


Ho fatto partire poi il comando sudo inetsim che ci da come output la schermata di seguito e che vuol dire che il servizio https è in ascolto sulla porta 443 e il servizio http sulla porta 80.

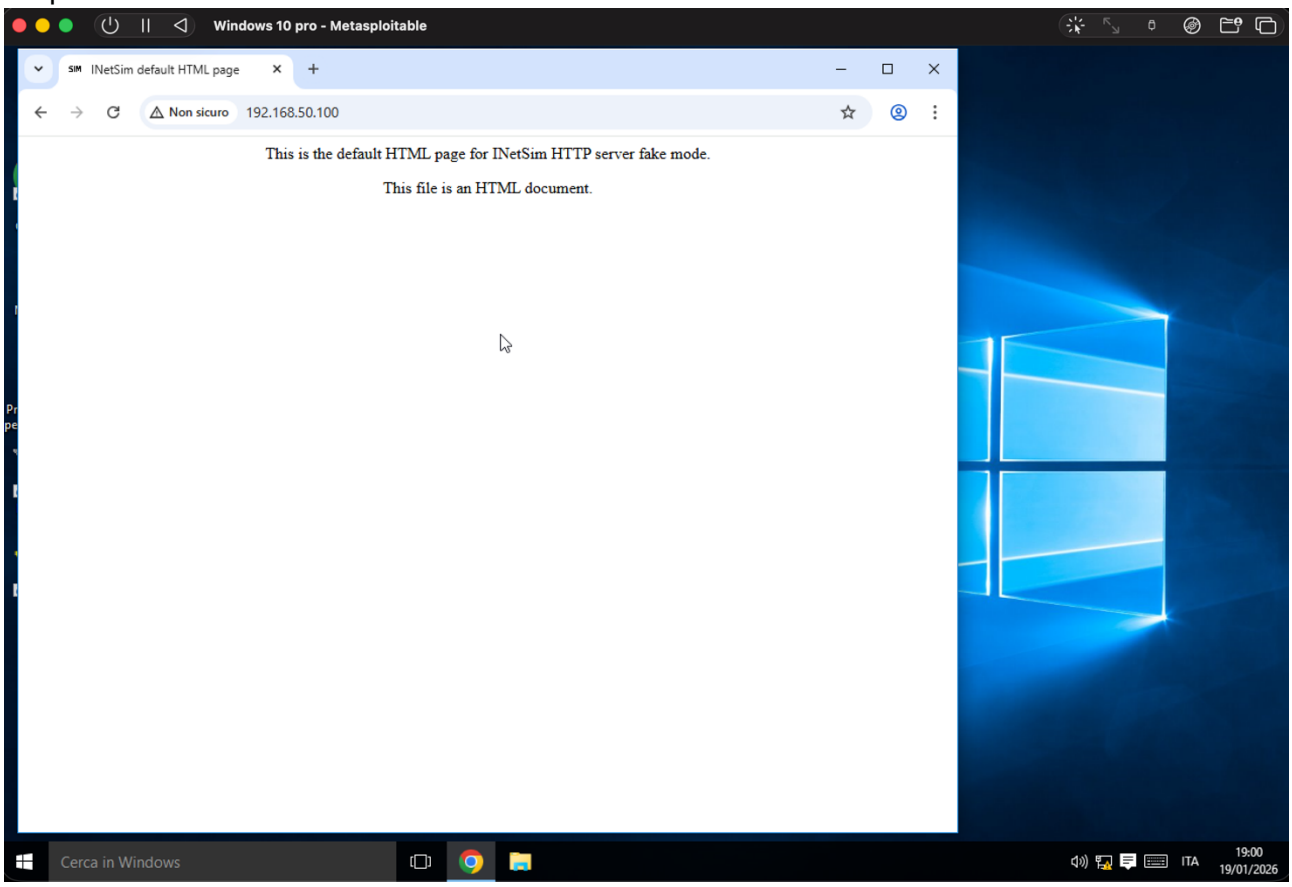


Tenendo aperto sudo inetsim su Kali, ci spostiamo su Windows e ci connettiamo via browser agli indirizzi https://192.168.50.100 e http://192.168.50.100 che restituiscono le schermate di seguito che ci indicano che il servizio è attivo.

https:

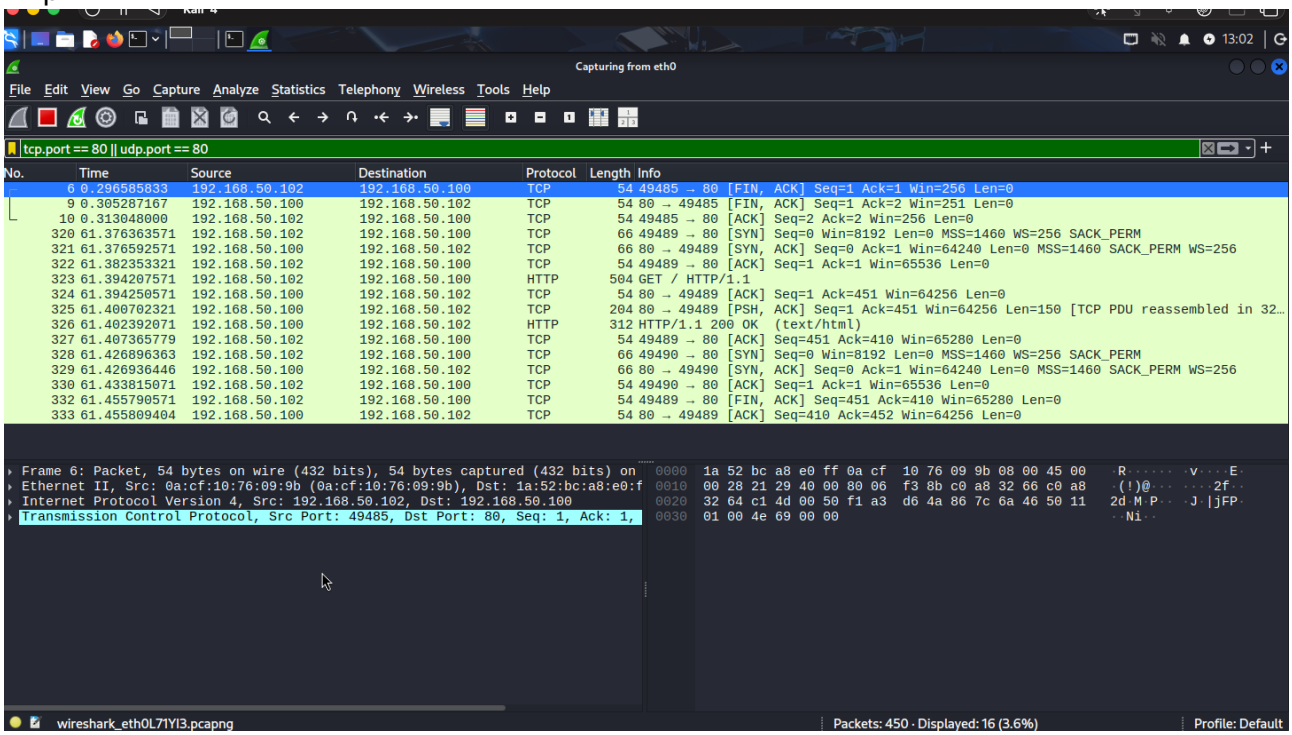


http:

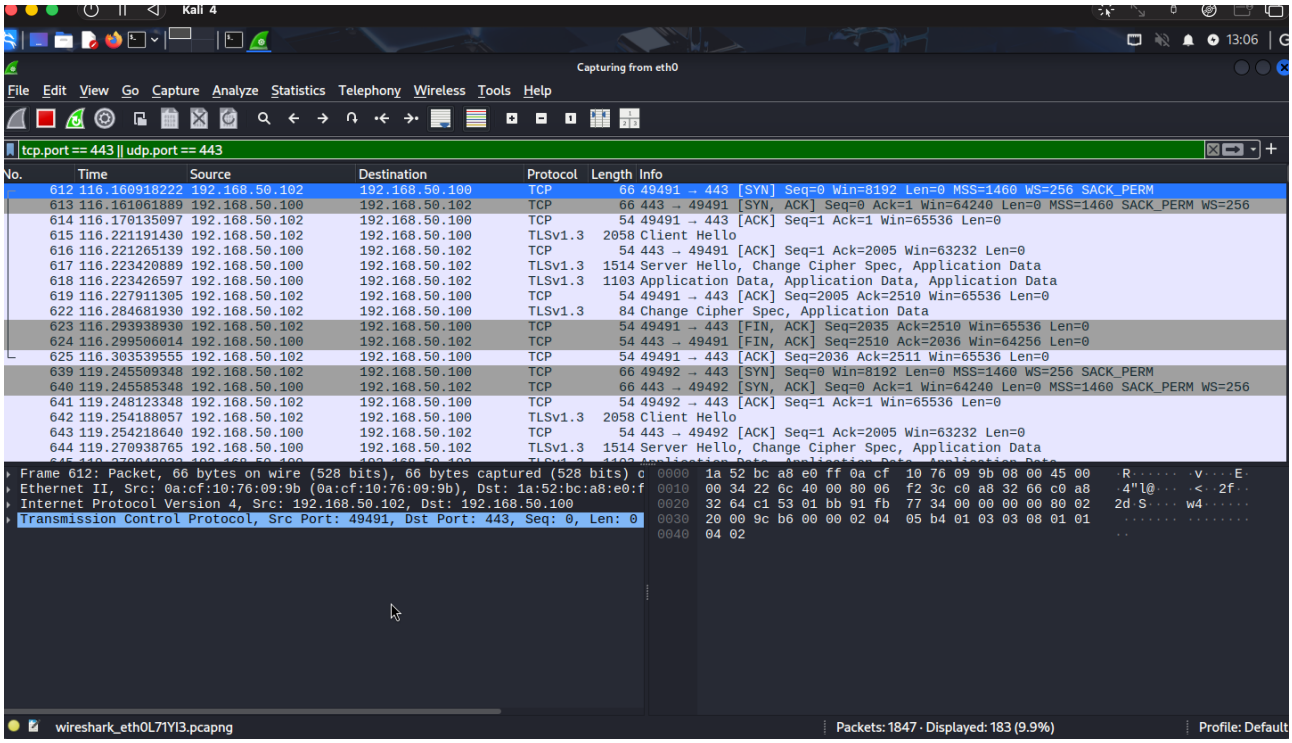


Apriamo ora whireshark eintercettiamo le comunicazioni in entrata ed uscita.

http:



https:



Whireshark mostra Il traffico HTTP sulla porta 80 mostrando intestazioni, URL e payload non crittografati, filtrabili con "http" o "tcp.port == 80".
HTTPS sulla porta 443 appare come pacchetti TLS crittografati, con soli dettagli come indirizzi IP, porte e fasi di handshake senza dati leggibili.