EPICODE

Andrea Rocca
CSPT0323

Cybersecurity Analyst

Week 3 - W3D4 Pratica

Pre-requisiti: Network 3

Esercizio

- Configurazione **policy su Windows Firewall** per permettere il ping da macchina Linux a macchina Windows 7 su laboratorio virtuale
- Utilizzo dell'utility **INetSim** per l'emulazione di servizi Internet
- Cattura ed analisi di pacchetti con **Wireshark**

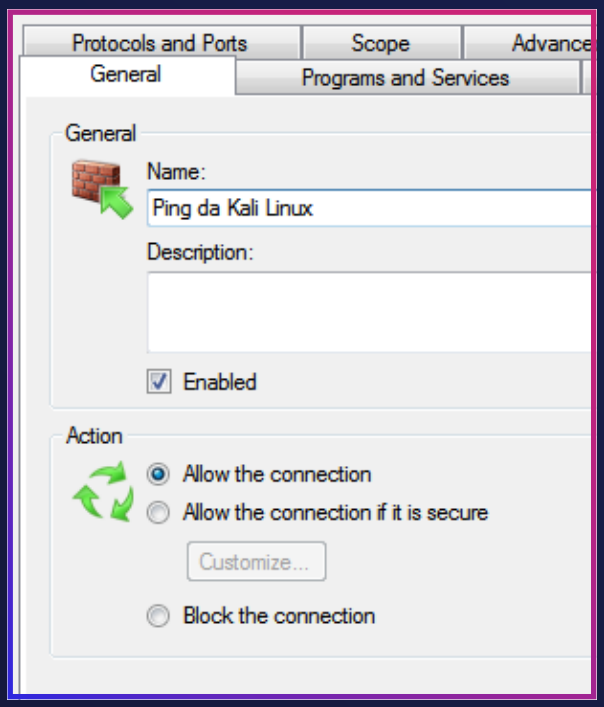
EPICODE

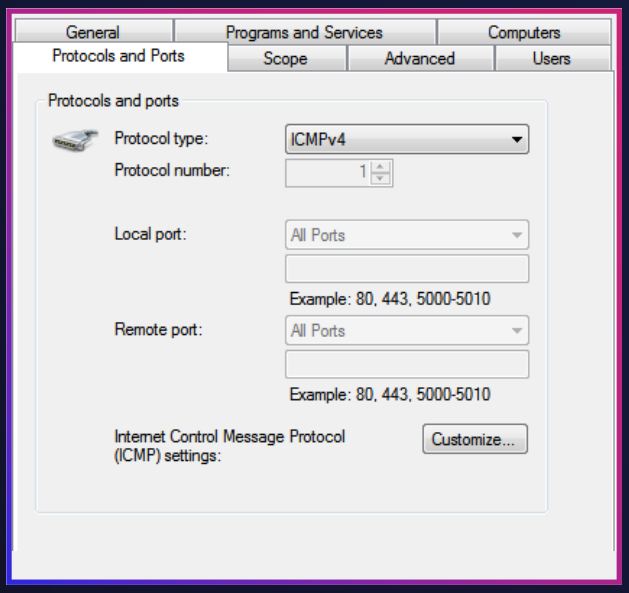
Andrea Rocca
CSPT0323

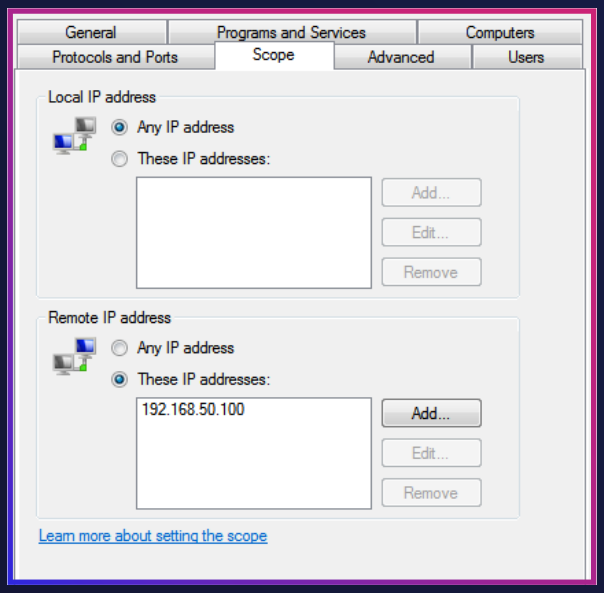
CONFIGURAZIONE POLICY SU WINDOWS 7

Dalle impostazioni avanzate relative a Windows Firewall, è stata configurata **un'eccezione** per consentire il ping dalla macchina Linux.

Questo è stato fatto creando una nuova **regola in entrata** che consente il traffico tramite **procotollo ICMP** da macchina remota, indicando l'indirizzo IP della macchina Linux (**192.168.50.100**) come consentito per il ping.







Cybersecurity Analyst / **Week3** - W3D4 Pratica

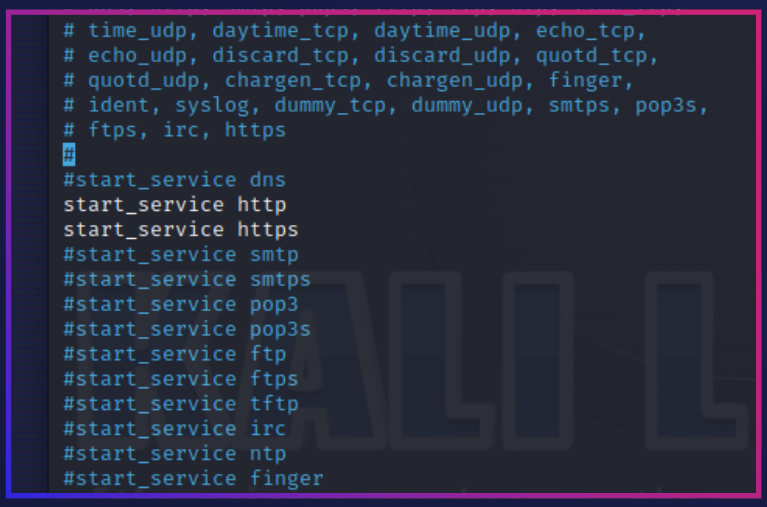
Pre-requisiti: Network 3

EPICODE

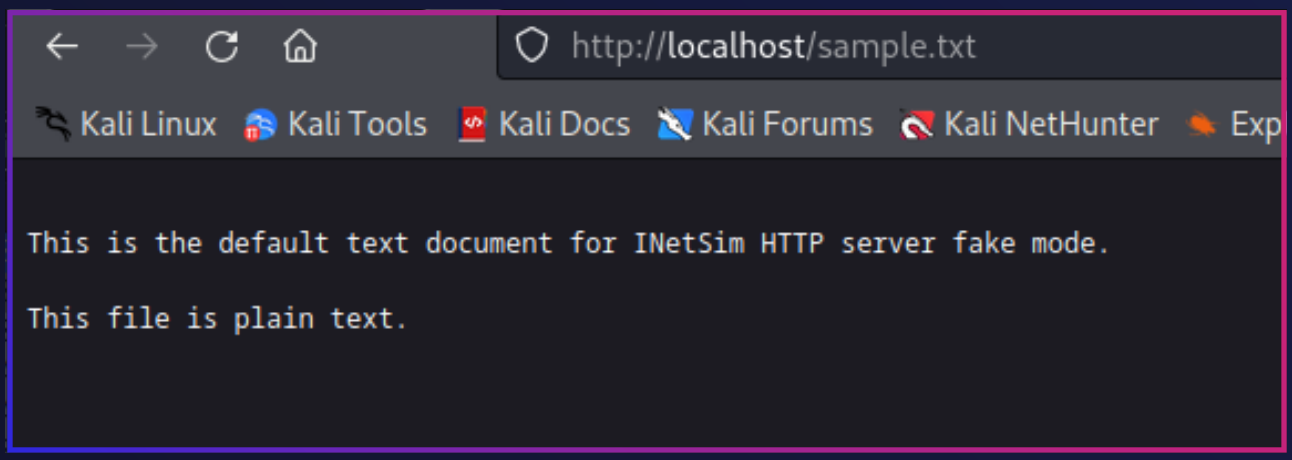
Andrea Rocca
CSPT0323

CONFIGURAZIONE E AVVIO INETSIN

Da terminale su macchina Kali Linux, è stato configurato il file relativo alle impostazioni di INetSim (**inetsim.conf**) escludendo tutti i servizi ad **eccezione di quelli HTTP e HTTPS**; avviando in seguito la simulazione del server web virtuale tramite comando "**sudo inetsim**".



APERTURA FILE .txt SU SERVER VIRTUALE

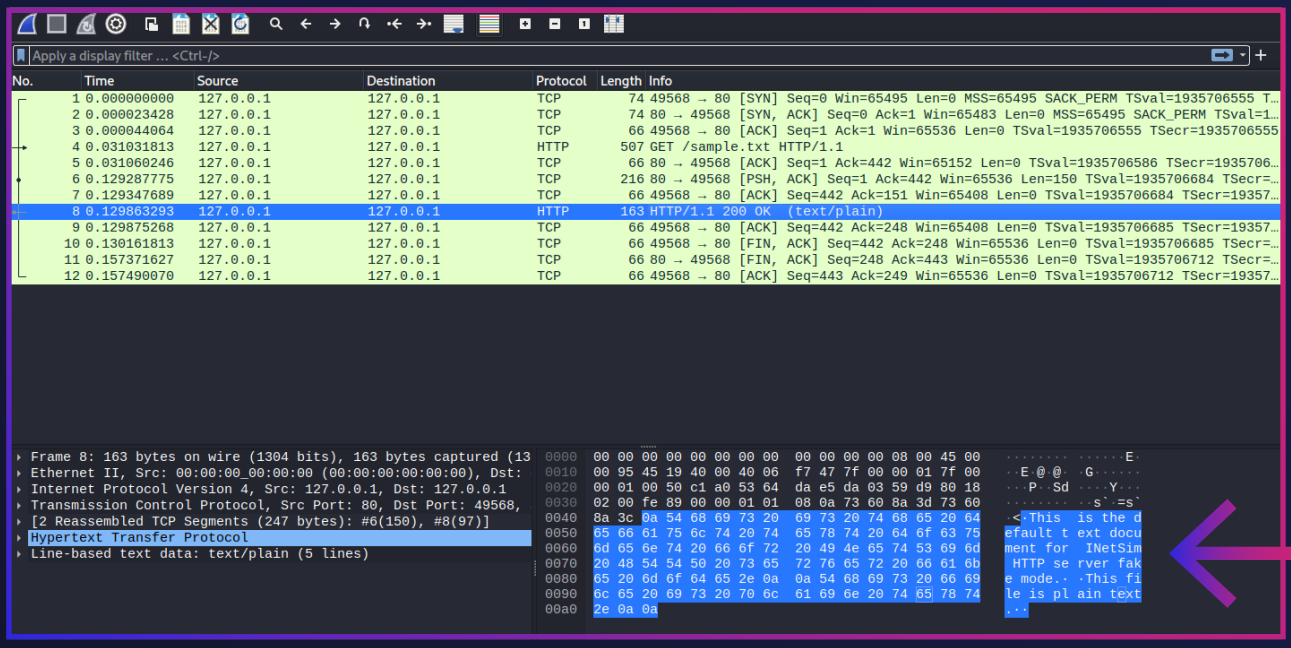


EPICODE

Andrea Rocca
CSPT0323

UTILIZZO DI WIRESHARK

Utilizzando Wireshark, uno strumento di analisi del traffico di rete, sono stati **catturati e esaminati i pacchetti** inviati durante questo processo su rete **loopback**. Trattandosi di processo su servizio **HTTP (quindi non cifrato)**, attraverso l'analisi, è stato possibile visualizzare il testo in chiaro (**text plain**) contenuto nel file .txt, dimostrando la possibilità di intercettare e leggere il contenuto del traffico dati durante la trasmissione attraverso la rete simulata.



Cybersecurity Analyst / **Week3** - W3D4 Pratica

Pre-requisiti: Network 3