

Report - Analisi del traffico di rete multi-protocollo tramite Raw Socket

Questo strumento permette di osservare il traffico di rete intercettando i pacchetti direttamente a livello Ethernet, prima che vengano elaborati dallo stack di rete del sistema operativo.

L'approccio consente una visione diretta e dettagliata delle comunicazioni che attraversano l'interfaccia di rete.

Ogni pacchetto catturato viene registrato in un file di log con un identificativo progressivo e un timestamp ad alta precisione. Questa struttura rende possibile ricostruire con accuratezza la sequenza temporale del traffico osservato.

Dopo la fase di cattura, il traffico IPv4 viene analizzato estraendo le informazioni principali dall'header IP.

In base al protocollo di livello superiore, il programma esegue un'analisi specifica per TCP, UDP o ICMP.

Per TCP e UDP vengono registrate le porte sorgente e destinazione e la dimensione del payload, mentre per ICMP vengono analizzati tipo e codice del messaggio, anche protocolli IP non gestiti esplicitamente vengono comunque tracciati.

Il programma funziona in tempo reale, richiede privilegi di amministratore e può essere interrotto manualmente in modo sicuro.

Nel complesso, rappresenta uno strumento efficace per monitoraggio, troubleshooting e analisi di sicurezza a basso livello.