Report Programma Cattura Socket di Rete - Azienda Theta

Azienda Theta Committente: Azienda Theta S.r.l.
Fornitore del servizio: Landa Tracker S.p.A.
Progetto: Progettazione e implementazione di un programma in linguaggio Python per la scansione delle porte.
Settore Cliente: Moda
Data: 25 Luglio 2025
Ideazione e progettazione a carico di Falchi Marco (PM), Lucchesi Marco, Matera Cristian, Meloni Alessandro, Mondelci Marco, Saad Patrick

Realizzazione a carico di Falchi Marco, Meloni Alessandro, Matera Cristian

Panoramica della richiesta

Questo documento presenta l'analisi completa di un programma Python progettato per effettuare cattura e monitoraggio in tempo reale del traffico di rete su specifici indirizzi IP e porte.

Obiettivo principale: Implementare un sistema di network monitoring che consenta di intercettare, analizzare e visualizzare il traffico di rete TCP/UDP filtrato per IP e porte specifiche, fornendo visibilità completa sulle comunicazioni di rete per scopi di sicurezza e troubleshooting.

1. Panoramica del Programma

Il programma sviluppato è un network packet sniffer avanzato implementato in Python che permette di monitorare il traffico di rete attraverso la cattura di pacchetti raw a livello Ethernet. Il software utilizza socket RAW e librerie moderne per offrire un'interfaccia utente elegante e funzionalità di monitoring professionale specializzate nell'analisi del traffico di rete.

1.1 Funzionalità

Il programma offre le seguenti funzionalità principali:

Cattura Pacchetti RAW: Utilizza socket AF_PACKET con SOCK_RAW per intercettare tutto il traffico Ethernet, operando a livello di collegamento dati per massima visibilità.

Parsing Protocolli Multi-livello: Implementa decodifica completa degli header Ethernet, IP, TCP e UDP utilizzando **struct.unpack** per interpretazione binaria accurata dei pacchetti.

Filtraggio Avanzato: Consente filtraggio granulare per indirizzo IP specifico e porta target (opzionale), ottimizzando l'analisi su traffico rilevante.
Monitoraggio Bidirezionale: Identifica comunicazioni sia in ingresso che in uscita per l'IP target, fornendo visibilità completa dei flussi di rete.

Supporto Multi-protocollo: Gestisce sia traffico TCP che UDP con parsing specifico degli header per ogni protocollo.

Visualizzazione Real-time: Mostra istantaneamente ogni pacchetto catturato con informazioni dettagliate su sorgente, destinazione e protocolli.

Gestione Privilegi Elevati: Richiede esecuzione con privilegi amministrativi per accesso ai socket RAW, garantendo capacità di cattura completa.

1.2 Utilità

Lo strumento rappresenta una risorsa fondamentale per diverse categorie di utenti:

Network Security Analyst: Possono monitorare traffico sospetto, identificare comunicazioni non autorizzate e analizzare pattern di attacco in tempo reale.

System Administrator: Utilizzano il tool per diagnosticare problemi di connettività, verificare configurazioni di rete e monitorare performance dei servizi.

DevOps: Impiegano lo sniffer per debugging di applicazioni distribuite, analisi di latenza e verifica di comunicazioni tra microservizi.

Incident Response Team: Sfruttano il programma per investigazioni forensi, raccolta di evidenze e analisi del traffico durante security incident.

Network Troubleshooter: Utilizzano il monitoring per identificare problemi di routing e malfunzionamenti dell'infrastruttura di rete.

1.3 Ragioni di Sicurezza

L'implementazione del programma segue principi di sicurezza e responsabilità operativa:

Monitoraggio Passivo: Il programma opera esclusivamente in modalità di ascolto senza generare traffico o interferire con le comunicazioni esistenti.

Filtraggio Mirato: La capacità di filtrare per IP e porta specifici previene la cattura massiva di dati sensibili, dimostrando un approccio focalizzato e responsabile.

Gestione Privilegi: L'utilizzo di socket RAW richiede privilegi elevati, garantendo che solo personale autorizzato possa utilizzare lo strumento.

Trasparenza Operativa: Il codice è completamente documentato e le operazioni sono visibili, facilitando audit e verifiche di conformità.

Scope Limitato: Il focusing su specifici IP/porte previene l'intercettazione non necessaria di comunicazioni non correlate alle attività di monitoring.

Attenzione: è fondamentale utilizzare questo strumento esclusivamente su domini e risorse di proprietà o con autorizzazione esplicita, poiché l'intercettazione non autorizzata del traffico di rete viola policy aziendali, normative sulla privacy e leggi sulla protezione dei dati.

1.4 Implementazioni Grafiche Realizzate

Il programma implementa diverse soluzioni tecniche per migliorare significativamente l'esperienza visiva e l'usabilità, trasformando l'analisi di traffico di rete raw in uno strumento professionale e user-friendly:

Libreria Rich per Output Avanzato: Il programma utilizza **la libreria Rich** (from rich.console import Console, from rich.table import Table) per trasformare l'output testuale grezzo di pacchetti binari in presentazioni grafiche professionali. Questa implementazione sostituisce i tradizionali print() con rendering avanzato che supporta colori, formattazione e layout strutturati.

Tabelle Dinamiche per Network Analysis: La visualizzazione dei pacchetti utilizza **rich.table.Table** per creare tabelle real-time professionali con:

- Intestazioni categorizzate (Protocollo, IP Sorgente, Porta Sorgente, IP Destinazione, Porta Destinazione)
- Colorazione per differenti protocolli
- Allineamento ottimizzato con justification specifica per porte
- Aggiornamento dinamico per ogni pacchetto catturato

Sistema di Colorazione Contestuale: Il codice implementa colorazione intelligente per diversi elementi:

- Header della tabella con colorazione per massima visibilità
- Indirizzi IP colorati in verde per identificazione rapida
- Protocolli evidenziati per una distinzione immediata
- Porte numeriche allineate a destra per comparazione facilitata

Feedback Operativo Intelligente: Il programma fornisce comunicazione visiva continua:

- Conferma dei filtri applicati con formattazione
- Indicatori di stato per IP e porte monitorate
- Gestione elegante dell'interruzione utente con messaggi

Input Validation User-Friendly: L'interfaccia di configurazione implementa:

- Prompts chiari per IP target e porta opzionale
- Gestione intelligente di input vuoti per monitoraggio completo
- Conversione automatica e validazione delle porte numeriche

Parsing Binario Visualizzato: Il programma traduce dati binari complessi in informazioni comprensibili:

- Conversione automatica di byte IP in formato decimale
- Decodifica di protocolli numerici in nomi leggibili (TCP/UDP)
- Estrazione e presentazione di informazioni multi-livello (Ethernet → IP → TCP/UDP)

Real-time Streaming Interface: La visualizzazione continua implementa:

- Aggiornamento istantaneo per ogni pacchetto intercettato
- Tabelle che si rinnovano dinamicamente senza scroll eccessivo
- Layout ottimizzato per sessioni di monitoring prolungate

2. Spiegazione semplificata

Il programma rappresenta una soluzione specializzata per il monitoraggio e l'analisi del traffico di rete in tempo reale. La sua architettura e l'implementazione chiara lo rendono uno strumento potente per professionisti che necessitano di visibilità completa sulle comunicazioni di rete.

Come Funziona in Pratica: il flusso del programma è progettato per essere immediato e completo. L'amministratore di rete inserisce l'indirizzo IP da monitorare (ad esempio, un server critico dell'infrastruttura Theta) e opzionalmente specifica una porta particolare (come 443 per HTTPS o 80 per HTTP). Il sistema inizia immediatamente a catturare tutti i pacchetti che coinvolgono quell'IP, decodificando automaticamente gli header di rete e presentando le informazioni in tabelle colorate e strutturate. Ogni comunicazione viene visualizzata istantaneamente con dettagli completi su sorgente, destinazione, protocollo e porte coinvolte.

Punti di Forza: Il programma opera direttamente sui dati di rete senza limitazioni, catturando tutto il traffico che passa attraverso la scheda di rete. La trasformazione automatica di dati binari complessi in tabelle colorate e leggibili rende immediata la comprensione di ciò che sta accadendo sulla rete. Il sistema di filtri consente di concentrarsi solo su ciò che serve davvero, evitando di perdersi in un mare di informazioni inutili.

Potenziale di Sviluppo: Il codice attuale fornisce una base solida **per espansioni future** verso analisi statistica del traffico, detection di anomalie e integrazione con sistemi SIEM.

Considerazioni Finali

Il programma sviluppato per Theta, marchio di riferimento nel mondo fashion, rappresenta una soluzione personalizzata che fonde potenza tecnica e semplicità d'uso, incarnando i principi di qualità e innovazione che distinguono l'azienda.

Impatto Operativo per Theta: Nel panorama del fashion digitale e delle vendite online, questo strumento diventa un pilastro per la protezione e l'efficienza delle operazioni digitali:

- **Controllo Piattaforme Vendita:** Sorveglianza continua del traffico verso i sistemi di e-commerce per intercettare minacce, sovraccarichi o rallentamenti durante eventi commerciali critici
- **Blindatura Sistemi Pagamento:** Supervisione delle comunicazioni finanziarie per bloccare sul nascere tentativi di frode o compromissioni delle transazioni
- **Vigilanza Catena Logistica:** Controllo delle comunicazioni con magazzini e fornitori per preservare l'accuratezza delle informazioni e la fluidità operativa
- **Risposta Emergenze:** Strumento di investigazione immediata durante crisi di sicurezza per mappare l'origine degli attacchi e valutarne l'estensione

Il Nostro Contributo Distintivo per Theta: Questo programma mette nelle mani del team security e network di Theta un'arma di precisione per il controllo chirurgico del traffico strategico. Il sistema di targeting selettivo per IP e porte trasforma il monitoring da attività generica a operazione mirata sui sistemi vitali, assicurando che nessuna comunicazione cruciale sfugga al controllo e che ogni dato sensibile rimanga sotto protezione totale.
La visualizzazione istantanea permette di cogliere immediatamente segnali di pericolo o irregolarità, garantendo tempi di reazione fulminei per neutralizzare minacce o risolvere malfunzionamenti.

Conclusione

Questo programma rappresenta un baluardo tecnologico nella strategia di difesa digitale di Theta, costruito su misura per salvaguardare l'integrità e la continuità del suo universo digitale.

In un mercato dove un solo minuto di downtime può costare migliaia di clienti e la fiducia acquisita in anni, strumenti di controllo così sofisticati diventano la differenza tra successo e vulnerabilità.

Il software incarna la filosofia Theta: trasformare la complessità in eleganza. Come ogni capo della collezione, unisce funzionalità superiori a un design intuitivo, dimostrando che anche la tecnologia più avanzata può essere resa accessibile e raffinata.
La capacità del programma di vedere l'invisibile - intercettando e decifrando il linguaggio nascosto della rete - permette al team tecnico di Theta di **anticipare i problemi** prima che diventino crisi, mantenendo l'ecosistema digitale sempre un passo avanti rispetto alle minacce. In un settore dove velocità di risposta e affidabilità sono tutto, questo strumento garantisce che Theta rimanga **sempre connessa, sempre protetta, sempre performante.**