S11L4

Relazione tecnica: Analisi del traffico DNS con Wireshark

Introduzione e contesto

Il Domain Name System (DNS) come un elemento cruciale per il funzionamento delle reti. Il DNS traduce i nomi di dominio, facilmente leggibili dagli esseri umani (come www.cisco.com), in indirizzi IP (ad esempio, 192.0.2.1) che i computer utilizzano per comunicare.

L'importanza del DNS risiede nel suo ruolo centrale nella risoluzione dei nomi, ma presenta una vulnerabilità significativa: il traffico DNS non è crittografato di default. Ciò lo rende suscettibile a intercettazioni, manipolazioni e attacchi come lo spoofing. Questo esercizio si concentra sull'uso di Wireshark per catturare e analizzare le comunicazioni DNS, consentendo di comprendere le dinamiche del protocollo e di identificare i potenziali rischi associati.

Obiettivi dell'esercizio

L'esercizio mira a:
1. Configurare Wireshark per catturare il traffico DNS in tempo reale.
2. Analizzare i dettagli delle query e delle risposte DNS per comprendere il funzionamento del protocollo.
3. Identificare i rischi di sicurezza legati alla mancanza di crittografia nel traffico DNS.

Fasi dell'esercizio

Fase 1: Preparazione e configurazione

1. Avvio di Wireshark:
   - L'utente apre Wireshark e seleziona l'interfaccia di rete appropriata (ad esempio, Wi-Fi o Ethernet) per iniziare la cattura dei pacchetti.
   - È necessario applicare un filtro DNS per ridurre il rumore del traffico non pertinente. Questo viene fatto inserendo `dns` nella barra dei filtri. In alternativa, si può usare il filtro `udp.port == 53`, che mostra solo il traffico DNS trasmesso su UDP.

Fase 2: Generazione del traffico DNS

1. Navigazione web:
   - L'utente apre un browser e visita un sito web, ad esempio www.example.com.
   - Durante questa operazione, vengono inviate query DNS al server DNS configurato nella rete, richiedendo la risoluzione del nome di dominio.

2. Cattura in tempo reale:
   - Wireshark registra ogni pacchetto trasmesso, comprese le query DNS e le eventuali risposte ricevute.

Fase 3: Analisi del traffico DNS

1. Esplorazione delle query DNS:
   - In Wireshark, si possono visualizzare i dettagli delle query DNS catturate.
   - Ogni query contiene campi come:
     - Name: Il dominio richiesto dall'utente.
     - Transaction ID: Un identificatore univoco per la richiesta DNS.
     - Flags: Indicano se si tratta di una query o di una risposta.

2. Analisi delle risposte DNS:
   - Le risposte forniscono l'indirizzo IP corrispondente al dominio richiesto. Ad esempio, la query per www.example.com potrebbe restituire un indirizzo IPv4 (record A) o un IPv6 (record AAAA).
   - È possibile osservare i dettagli delle risorse restituite, come il Time to Live (TTL), che specifica la durata di validità della risposta.

Fase 4: Identificazione delle vulnerabilità

1. Traffico in chiaro:
   - Il traffico DNS catturato con Wireshark non è crittografato, quindi è facilmente leggibile. Questo consente a un potenziale attaccante di intercettare le query e monitorare i siti visitati dagli utenti.

2. Manipolazione dei dati:
   - Senza crittografia, le risposte DNS possono essere alterate, ad esempio per reindirizzare gli utenti verso siti fraudolenti o malevoli (DNS spoofing o poisoning).

Mitigazione dei rischi

Il documento suggerisce che per mitigare i rischi associati al traffico DNS non crittografato, si può ricorrere a tecnologie come DNS over HTTPS (DoH) o DNS over TLS (DoT). Entrambi i protocolli garantiscono la crittografia del traffico DNS:
1. **DNS over HTTPS (DoH):** Utilizza il protocollo HTTPS per proteggere le query DNS, rendendole indistinguibili dal normale traffico web.
2. **DNS over TLS (DoT):** Impiega il protocollo TLS per crittografare le comunicazioni DNS, aumentando la sicurezza.

Conclusioni

Questo esercizio fornisce una comprensione pratica del funzionamento del DNS attraverso l'uso di Wireshark. Permette di acquisire competenze utili per analizzare il traffico di rete e identificare potenziali vulnerabilità. La mancanza di crittografia nel traffico DNS rappresenta una minaccia significativa alla privacy e alla sicurezza degli utenti. Adottare protocolli avanzati come DoH e DoT è fondamentale per proteggere le comunicazioni DNS e migliorare la sicurezza complessiva delle reti.