Acquisire e analizzare il traffico di rete con Wireshark per la diagnostica

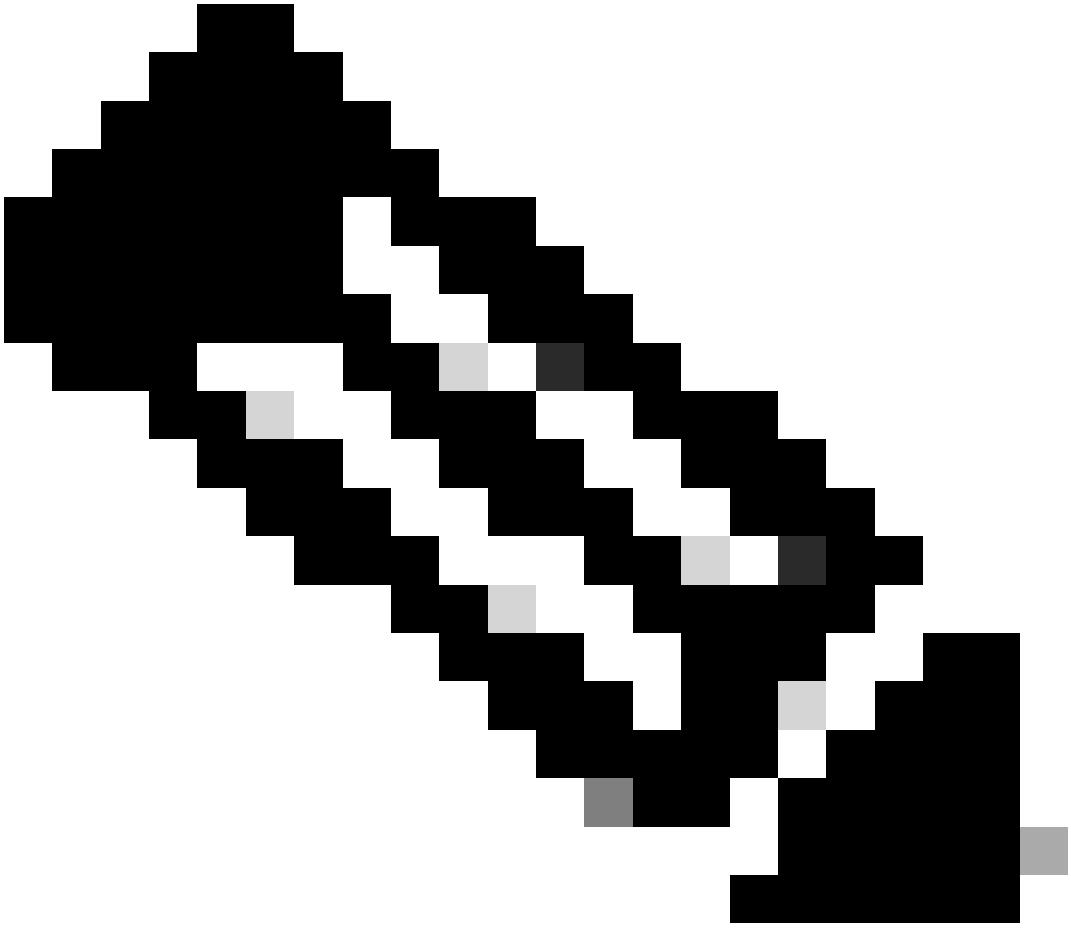
Sommario

Introduzione

In questo documento viene descritto come utilizzare Wireshark per acquisire e analizzare il traffico di rete a scopo diagnostico.

Panoramica

Wireshark è un'applicazione gratuita che può essere utilizzata per leggere e analizzare le acquisizioni dei pacchetti (chiamate anche "dump TCP"). Le acquisizioni dei pacchetti rivelano tutte le comunicazioni tramite una scheda di rete a livello di pacchetto, rendendo possibile la visualizzazione di DNS, HTTP, ping e altri tipi di traffico. L'acquisizione dei pacchetti è particolarmente utile come fase diagnostica per la risoluzione dei problemi e, con l'introduzione del SIG, è ora una parte fondamentale del processo diagnostico.



Nota: Wireshark acquisisce tutto il traffico sulla scheda selezionata. Poiché le acquisizioni di pacchetti spesso contengono informazioni che consentono l'identificazione personale dell'utente (PII), per condividere i file di acquisizione con il supporto utilizzare sempre un metodo sicuro, ad esempio un collegamento Box.

Scarica Wireshark

È possibile scaricare Wireshark per Windows, macOS o Linux all'indirizzo: https://www.wireshark.org/

Raccogliere un'acquisizione pacchetto

1. Scegliere la scheda di rete connessa a Internet e avviare la cattura in Wireshark.
2. Durante l'acquisizione, riprodurre il problema da diagnosticare.
3. Al termine dell'operazione, interrompete la cattura e salvate il file con il nome `.pcap`.

Porte e protocolli di base

- La maggior parte dei pacchetti comunica sui protocolli del livello trasporto TCP o UDP
  - Per impostazione predefinita, ad esempio, "DNS" viene eseguito "su" UDP. In caso di guasto del protocollo TCP, il sistema passa a UDP.
- HTTP e DNS sono protocolli comuni eseguiti su una combinazione di protocollo di trasporto + porte.

Transport Layer Protocol	Port	Nome protocollo	Utilizzo
TCP	22	SSH	Accesso VA remoto
TCP	25	SMTP	Monitoraggio VA
IP	50	ESP (Encapsulating Security Payload)	Riservatezza, integrità dei dati, autenticazione dell'origine
IP	51	AH (Authentication Header)	Integrità dei dati, autenticazione dell'origine
UDP	53	DNS	Predefinito DNS
TCP	53	DNS	Failover DNS
TCP	80	HTTP	Traffico Web (non crittografato), API
UDP	123	NTP	Sincronizzazione ora VA
TCP	443	HTTPS	Traffico Web crittografato, API, connettori AD a VA
UDP	443	HTTPS	Query DNS crittografate RC
UDP	500	IKE	Negoziazioni tunnel IPsec
UDP	4500	NAT-T	Attraversamento NAT per tunnel IPsec
TCP	8080	HTTP	Connettori AD per comunicazioni VA

La conoscenza dei nomi di protocollo, delle porte e dei relativi utilizzi consente di identificare e analizzare il traffico rilevante in Wireshark.

Operatori di base

Per creare stringhe di filtro in Wireshark, utilizzare i seguenti operatori:

- `==`: Uguale a (esempio:`ip.dst==1.2.3.4`)
- `!=`: Diverso da (esempio:`ip.dst!=1.2.3.4`)
- `&`: And (Esempio:`ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`: Oppure (Esempio:`ip.dst==1.2.3.4) || ip.dst==1.2.3.5`)

Per le opzioni di filtro avanzate, consultare la documentazione di Wireshark: 6.4. Creazione di espressioni di filtro di visualizzazione

Filtri

Le acquisizioni di pacchetti possono contenere migliaia di pacchetti. I filtri consentono di focalizzare l'attenzione su tipi di traffico specifici:

- Per protocollo:
    - `dns`: visualizza solo il traffico DNS
    - `http || dns`— Mostra traffico HTTP o DNS
- Per indirizzo IP:
    - `ip.addr==<IP>`— Tutto il traffico da/verso`<IP>`
    - `ip.src==<IP>`— Tutto il traffico proveniente da`<IP>`
    - `ip.dst==<IP>`— Tutto il traffico diretto a`<IP>`
- Varie:
    - `tcp.flags.reset==1`— Verifica la presenza di reimpostazioni TCP (timeout)
    - `dns.qry.name contiene "[dominio]"`— Query DNS corrispondenti a un dominio
    - `tcp.port==80 || udp.port==80`— traffico TCP o UDP sulla porta 80

Visualizzazione e analisi dei pacchetti

Dopo aver individuato un pacchetto, espandere i segmenti all'interno di Wireshark per analizzarne i dettagli. La familiarità con la struttura del protocollo consente di interpretare questi dettagli e di ricostruire i dati se necessario.

Seguire un flusso di dati

Utilizzare l'elenco dei pacchetti per individuare le coppie di richiesta e risposta. Fare clic con il pulsante destro del mouse su un pacchetto e selezionare Segui **>** Flusso TCP, Flusso UDP, Flusso TLS o Flusso HTTP per visualizzare la richiesta e la sequenza di risposta correlate.

- Ciò è più utile con i protocolli che hanno scambi multipli (ad esempio, HTTP) che con i protocolli a richiesta singola (ad esempio, DNS).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).