Erfassen und Analysieren von Netzwerkverkehr mit Wireshark für Diagnosen

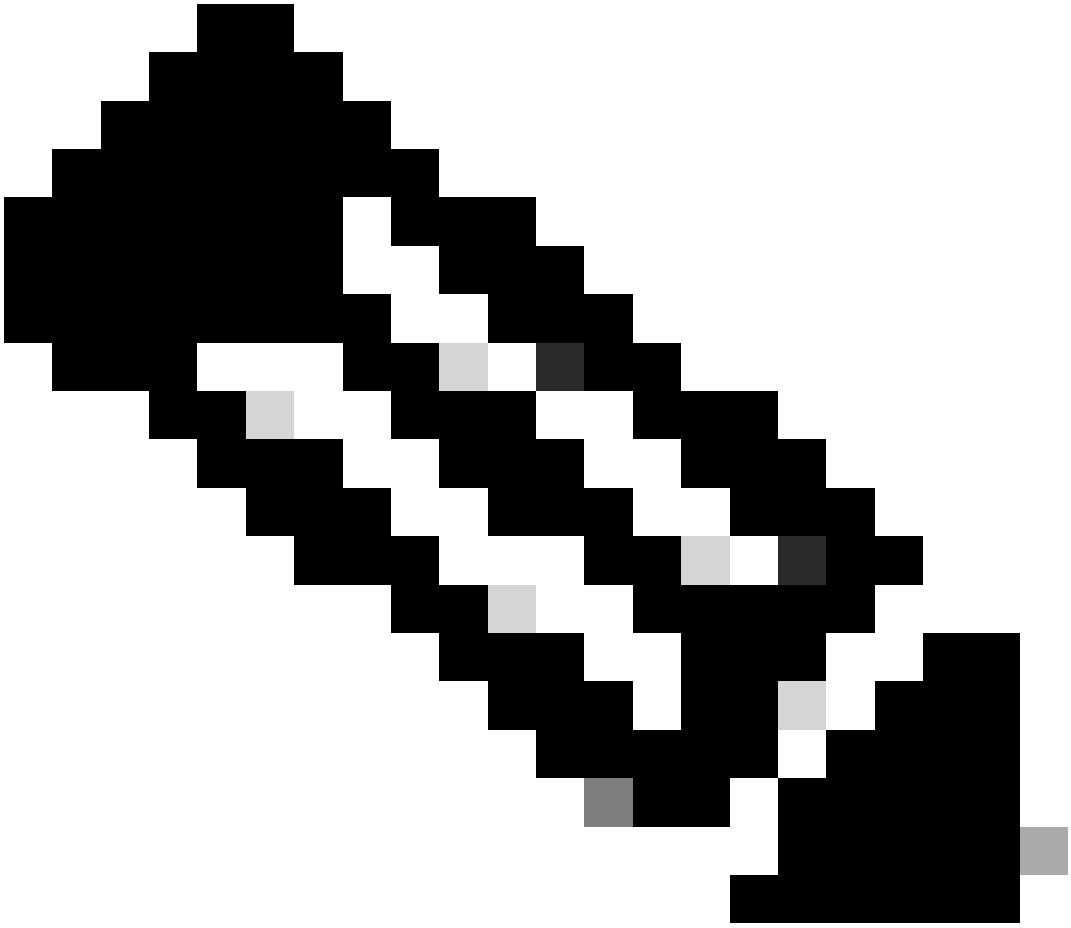
Inhalt

Einleitung

In diesem Dokument wird die Verwendung von Wireshark zur Erfassung und Analyse des Netzwerkverkehrs zu Diagnosezwecken beschrieben.

Überblick

Wireshark ist eine kostenlose Anwendung, mit der Sie Paketerfassungen lesen und analysieren können (auch "TCP-Dumps" genannt). Bei der Paketerfassung wird die gesamte Kommunikation über einen Netzwerkadapter auf Paketebene aufgedeckt, sodass DNS-, HTTP-, Ping- und andere Datenverkehrstypen angezeigt werden können. Paketerfassungen sind besonders wertvoll als diagnostischer Schritt für eine tief greifende Fehlerbehebung und mit der Einführung von SIG nun ein grundlegender Bestandteil des Diagnoseprozesses.



Anmerkung: Wireshark erfasst den gesamten Datenverkehr auf dem ausgewählten Adapter. Da Paketerfassungen häufig personenbezogene Daten (PII) enthalten, sollten Sie stets eine sichere Methode, z. B. eine Box-Verbindung, verwenden, um Erfassungsdateien mit Unterstützung gemeinsam zu nutzen.

Wireshark herunterladen

Sie können Wireshark für Windows, MacOS oder Linux herunterladen unter: https://www.wireshark.org/

Erfassen einer Paketerfassung

1. Wählen Sie den mit dem Internet verbundenen Netzwerkadapter aus, und starten Sie die Erfassung in Wireshark.
2. Reproduzieren Sie während der Erfassung das Problem, das Sie diagnostizieren möchten.

3. Beenden Sie die Erfassung, wenn Sie fertig sind, und speichern Sie die Datei als `.pcap`.

Grundlegende Ports und Protokolle

- Die meisten Pakete kommunizieren auf Transportschichtprotokollen TCP oder UDP
  - "DNS" wird z. B. standardmäßig "auf" UDP ausgeführt. Bei TCP-Fehlern wird auf UDP umgeschaltet.
- HTTP und DNS sind gängige Protokolle, die auf einer Kombination aus Transportprotokoll und Ports ausgeführt werden.

Transportschichtprotokoll	Anschluss	Protokollname	Nutzung
TCP	22	SSH	Remote-VA-Zugriff
TCP	25	SMTP	VA-Überwachung
IP	50	ESP (Encapsulating Security Payload)	Vertraulichkeit, Datenintegrität, Ursprungsauthentifizierung
IP	51	AH (Authentifizierungs-Header)	Datenintegrität, Ursprungsauthentifizierung
UDP	53	DNS	DNS-Standard
TCP	53	DNS	DNS-Failover
TCP	80	HTTP	Webdatenverkehr (unverschlüsselt), APIs
UDP	123	NTP	VA-Zeitsynchronisierung
TCP	443	HTTPS	Verschlüsselter Web-Datenverkehr, APIs, AD-Verbindungen zu VAs
UDP	443	HTTPS	RC Verschlüsselte DNS-Abfragen
UDP	500	IKE	IPsec-Tunnelaushandlung
UDP	4500	NAT-T	NAT-Traversal für IPsec-Tunnel
TCP	8080	HTTP	AD-Anschlüsse für VAs und Kommunikation

Die Kenntnis von Protokollnamen, Ports und deren Verwendung hilft Ihnen, relevanten Datenverkehr in Wireshark zu identifizieren und zu analysieren.

Grundlegende Operatoren

Verwenden Sie beim Erstellen von Filterzeichenfolgen in Wireshark folgende Operatoren:

- `==`: Equals (Beispiel:`ip.dst==1.2.3.4`)
- `!=`: Ungleich (Beispiel:`ip.dst!=1.2.3.4`)

- `&`: und (Beispiel:`ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`: oder (Beispiel:`ip.dst==1.2.3.4 | ip.dst==1.2.3.5`)

Erweiterte Filteroptionen finden Sie in der Wireshark-Dokumentation: [6.4. Erstellen von Anzeigefilterausdrücken]

Filter

Paketerfassungen können Tausende von Paketen enthalten. Mithilfe von Filtern können Sie sich auf bestimmte Datenverkehrstypen konzentrieren:

- Nach Protokoll:
  - `dns` - Nur DNS-Verkehr anzeigen
  - `http || dns` - Zeigt HTTP- oder DNS-Datenverkehr an
- Nach IP-Adresse:
  - `ip.addr==<IP>`— Gesamter Datenverkehr von/zu`<IP>`
  - `ip.src==<IP>` - Gesamter Datenverkehr von`<IP>`
  - `ip.dst==<IP>` - Gesamter Datenverkehr zu`<IP>`
- Verschiedenes:
  - `tcp.flags.reset==1`— Überprüfen Sie, ob TCP zurückgesetzt wurde (Timeouts).
  - `dns.qry.name enthält "[domain]"` — DNS-Abfragen, die mit einer Domäne übereinstimmen
  - `TCP-Port==80 | udp.port==80` - TCP- oder UDP-Datenverkehr an Port 80

Anzeigen und Analysieren von Paketen

Nachdem Sie ein Paket gefunden haben, erweitern Sie die Segmente in Wireshark, um Details zu analysieren. Wenn Sie mit der Protokollstruktur vertraut sind, können Sie diese Details interpretieren und bei Bedarf sogar Daten rekonstruieren.

Einem Datenstrom folgen

Verwenden Sie die Paketliste, um nach Anforderungs- und Antwortpaaren zu suchen. Klicken Sie mit der rechten Maustaste auf ein Paket, und wählen Sie Follow > TCP-Stream, UDP-Stream, TLS-Stream oder HTTP-Stream aus, um die zugehörige Anforderungs- und Antwortsequenz anzuzeigen.

- Dies ist bei Protokollen mit mehreren Austauschverbindungen (z. B. HTTP) nützlicher als bei Einzelanforderungsprotokollen (z. B. DNS).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.