Laden Sie Sitzungsschlüssel mit Paket herunter

Veröffentlicht: 2024-07-02

Sie können die PCAP Next Generation (pcapng) -Datei herunterladen, die alle erfassten SSL-Sitzungsschlüssel und verschlüsselten Pakete enthält. Anschließend können Sie die Paketerfassungsdatei in einem Tool wie Wireshark öffnen, das die Sitzungsschlüssel anwenden und die entschlüsselten Pakete anzeigen kann.

Bevor Sie beginnen

- Sie müssen über einen konfigurierten Packetstore oder eine Paketerfassungsdiskette verfügen, bevor Sie Pakete und Sitzungsschlüssel von einem herunterladen können Sensor oder ein Konsole. Sehen Sie unsere Bereitstellungsleitfäden um loszulegen.
- Das Konsole muss für SSL Shared Secrets lizenziert sein.
- Das Speicher für SSL-Sitzungsschlüssel Die Einstellung muss am Sensor aktiviert sein.
- RevealX Enterprise-Benutzer müssen entweder über Systemzugriff und Administration verfügen Privilegien oder eingeschränkte Rechte mit Zugriff auf Pakete und Sitzungsschlüssel. RevealX 360-Benutzer müssen Zugriff auf Pakete und Sitzungsschlüssel haben.

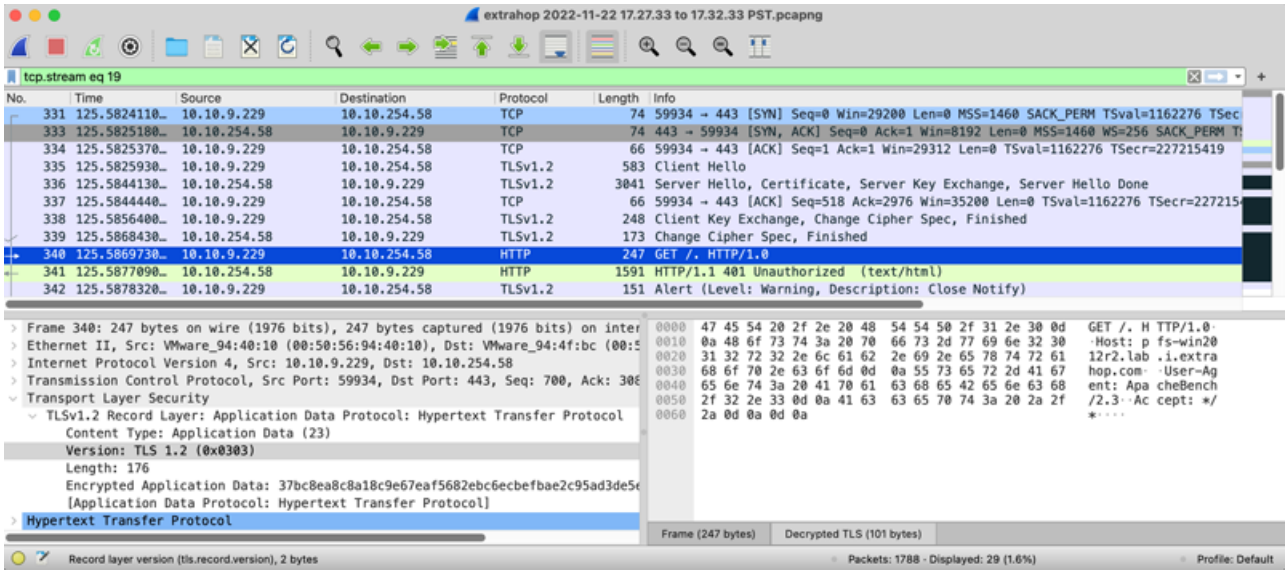
1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Pakete**.
3. Optional: Wenden Sie Filter an, um die Paketabfrage zu verfeinern.
4. Wenn die Abfrage abgeschlossen ist, klicken Sie auf **PCAP+-Sitzungsschlüssel herunterladen**.
5. Klicken Sie **PCAP+-Sitzungsschlüssel herunterladen**.
   Die PCAPNG-Datei wird automatisch auf Ihren Computer heruntergeladen und der Vorgang zum Herunterladen des Sitzungsschlüssels wird im Audit-Log.

   Wenn für die heruntergeladene PCAP keine Sitzungsschlüssel verfügbar sind, wird **PCAP+-Sitzungsschlüssel herunterladen** Die Schaltfläche wird nicht angezeigt.

Sehen Sie sich die entschlüsselte Nutzlast in Wireshark an

1. Starten Sie die Wireshark-Anwendung.
2. Öffnen Sie die heruntergeladene Paketerfassungsdatei (pcapng) in Wireshark.

Wenn ein SSL-verschlüsselter Frame ausgewählt ist, wird **Entschlüsseltes SSL** Die Registerkarte wird am unteren Rand des Wireshark-Fensters angezeigt. Klicken Sie auf die Registerkarte, um die entschlüsselten Informationen in der PCAP als Klartext anzuzeigen.


extrahop 2022-11-22 17.27.33 to 17.32.33 PST.pcapng
tcp.stream eq 19
No. Time Source Destination Protocol Length Info
331 125.5824110… 10.10.9.229 10.10.254.58 TCP 74 59934 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1162276 TSec
333 125.5825180… 10.10.254.58 10.10.9.229 TCP 74 443 → 59934 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM T
334 125.5825370… 10.10.9.229 10.10.254.58 TCP 66 59934 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1162276 TSecr=227215419
335 125.5825930… 10.10.9.229 10.10.254.58 TLSv1.2 583 Client Hello
336 125.5844130… 10.10.254.58 10.10.9.229 TLSv1.2 3041 Server Hello, Certificate, Server Key Exchange, Server Hello Done
337 125.5844440… 10.10.9.229 10.10.254.58 TCP 66 59934 → 443 [ACK] Seq=518 Ack=2976 Win=35200 Len=0 TSval=1162276 TSecr=227215
338 125.5856400… 10.10.9.229 10.10.254.58 TLSv1.2 248 Client Key Exchange, Change Cipher Spec, Finished
339 125.5868430… 10.10.254.58 10.10.9.229 TLSv1.2 173 Change Cipher Spec, Finished
340 125.5869730… 10.10.9.229 10.10.254.58 HTTP 247 GET /. HTTP/1.0
341 125.5877090… 10.10.254.58 10.10.9.229 HTTP 1591 HTTP/1.1 401 Unauthorized (text/html)
342 125.5878320… 10.10.9.229 10.10.254.58 TLSv1.2 151 Alert (Level: Warning, Description: Close Notify)
Frame 340: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on inter
Ethernet II, Src: VMware_94:40:10 (00:50:56:94:40:10), Dst: VMware_94:4f:bc (00:5
Internet Protocol Version 4, Src: 10.10.9.229, Dst: 10.10.254.58
Transmission Control Protocol, Src Port: 59934, Dst Port: 443, Seq: 700, Ack: 308
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 176
Encrypted Application Data: 37bc8ea8c8a18c9e67eaf5682ebc6ecbefbae2c95ad3de5
[Application Data Protocol: Hypertext Transfer Protocol]
Hypertext Transfer Protocol
0000 47 45 54 20 2f 2e 20 48 54 54 50 2f 31 2e 30 0d GET /. H TTP/1.0·
0010 0a 48 6f 73 74 3a 20 70 66 73 2d 77 69 6e 32 30 ·Host: p fs-win20
0020 31 32 72 32 2e 6c 61 62 2e 69 2e 65 78 74 72 61 12r2.lab .i.extra
0030 68 6f 70 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 hop.com· ·User-Ag
0040 65 6e 74 3a 20 41 70 61 63 68 65 42 65 6e 63 68 ent: Apa cheBench
0050 2f 32 2e 33 0d 0a 41 63 63 65 70 74 3a 20 2a 2f /2.3·· Ac cept: */
0060 2a 0d 0a 0d 0a *····
Frame (247 bytes)
Decrypted TLS (101 bytes)
Record layer version (tls.record.version), 2 bytes
Packets: 1788 · Displayed: 29 (1.6%)
Profile: Default