Aufgabenblatt 2

Sniffer-Tools: Wireshark Einstieg in die online Testumgebung

Sichern Sie die Aufzeichnungen aus Wireshark zu jeder Teilaufgabe in einer „.pcapng“ Datei mit Aufgabenteil als Name und übertragen Sie diese Dateien zu Ihrem persönlichen Rechner (nicht Cloud).

P.1. Wireshark Einstieg (Gruppenaufgabe)

> 1. Welche Protokolle sehen Sie im Laborbetrieb?

SMB2, TCP, NFS, ARP, IMCP....

> 2. Zeichnen Sie ein „ping“ zu einem benachbarten Rechner Ihrer Gruppe auf. Zeigen Sie die Pakete direkt während der Aufzeichnung an. (Hinweis: Ihre IP-Adressen finden Sie mit „ifconfig“ oder „ip -br a“.)

Man sieht jeweils Pakete als ping request und reply mit ICMP-header

P2. Wireshark Filter (Gruppenaufgabe)

Starten Sie einen neuen Wireshark-Mitschnitt

1. Test des Display-Filters (Tim):

- Display Filter-> http bzw. tcp.port == 80

2. Test des Capture-Filters (Helena):

- Aufzeichnen-> Optionen-> tcp port http

> 3. Vergleichen Sie innerhalb der Gruppe die aufgezeichneten Daten unter Nutzung des Display-Filters und Capture-Filters.

Bei der Nutzung des Capture-Filters werden alle Pakete mit TCP-Protokollen aufgezeichnet, bei der Filterung mit Display-Filter http sehen wir nur die Pakete mit HTTP-Protokoll

> 4. Wann wählen Sie welche Filtermethode in der Praxis?

Der Display-Filter ist sinnvoll, wenn man aus einem Gesamtmitschnitt bestimmte Pakete analysieren möchte oder eine komplette Momentaufnahme betrachten möchte.
Der Capture-Filter eignet sich zum reduzieren des Mitschnitts, wenn man vorher weiß, wonach man sucht und andere Pakete uninteressant sind.

> 5. Suchen Sie in Ihren Mitschnitten nach der User und Passworteingabe

Im Stream des POST-Packages finde ich (Helena) durch Eingabe "login" im Suchfeld:
login_username=hheyen2s und secretkey=projekt

P.3. Web-Datenverkehr analysieren mit Wireshark (Gruppenaufgabe)

heise.de öffnen, Mitschnitt beenden

> 2. Analysieren Sie mit Wireshark, von wie vielen IP-Adressen Daten nach dem Aufruf der Webseite „www.heise.de“ geladen worden sind. Aktivieren Sie unter „Bearbeiten/Einstellungen/Name Resolution“ den Punkt „Resolve Network(IP)-Adresses“. Nutzen Sie dann die Option Endpoints unter dem Menü Statistics in Wireshark. Lassen Sie sich mit „Show address resolution“ die Adressauflösungen der gefundenen Endpunkte mit Wireshark anzeigen.

Insgesamt 10 IP-Adressen, z.B.: 185.54.150.27 (heise02.webtrekk.net)
Bem.: tcp port 80 ist http, port 443 ist https

> 3. Analysieren Sie, mit welchen Endpunkten eine http Kommunikation stattgefunden hat. Analysieren Sie für jeden gefundenen Endpunkt mit http Kommunikation: Welche Aufgabe wurde mit dieser http-Kommunikation verfolgt? Arbeiten Sie in dieser Aufgabe in der Gruppe parallel, d.h. teilen Sie die Analyse der Endpunkte innerhalb Ihrer Gruppe auf und sammeln Sie die Ergebnisse. Hinweis: Nutzen Sie Displayfilter und die Funktionalität „Follow TCP Stream“ bzw „Follow HTTP Stream“von Wireshark.

- Client stellt z.B: Verbindungsanfrage o. Zertifikatanfrage (OSCP)
- bekommt ok/successful vom Server

> 4. Wählen Sie einen Endpunkt mit https Kommunikation aus und analysieren Sie den Beginn der Kommunikation mit diesem Endpunkt. Welche Nachrichten werden ausgetauscht?

Handshake-Nachrichten (TLS 1.2)

P.4. Wireshark in der Cloud-Umgebung (Gruppenaufgabe)

vncviewer 10.20.175.192

> 2. Öffnen sie ein Terminalfenster und lassen Sie sich die Interfaces mit dem Befehl ip -br a anzeigen. Vergleichen Sie die Ausgabe mit den Abbildungen des Sicherheitsnetzwerkes am Anfang dieses Aufgabenblattes.

wir sehen die IP-Adressen aller user auf dem Jumphost

> 3. Starten Sie Wireshark auf dem Jumphost. Starten Sie eine neue Wireshark Aufzeichnung für den srv-Rechner. Starten Sie den Browser auf dem Jumphost und geben Sie die Adresse „srv.itsecnet.de“ ein. Geben sie einen beliebigen User und ein beliebiges Passwort ein. Finden Sie den eingegebenen User und das Passwort im Wiresharkmitschnitt und dokumentieren Sie dies mit einem Screenshot von Wireshark. Speichern Sie den Mitschnitt.
>   Wie können Sie die Menge des aufgezeichneten Verkehrs durch die Wahl
>   - eines passenden Interfaces
>   - durch einen anderen Filter als auf http Pakete reduzieren?
>   Können User und Passwort auch von einem Gruppenmitglied auf dem Jumphost mit Wireshark gefunden werden, das sich nicht bei „srv.itsecnet.de“ angemeldet hat?

Die User in dem Jumphostnetz können den Netzwerktraffic mitschneiden, da sie sich im Selben Rechnernetz bewegen. Das Post-Paket mit dem Klartext-Passwort im Stream kann also von jedem User ausgelesen werden.