Practicum 5 – deel 1 - Netwerk forensics voor AlbusLux

Tijdens het practicum zal er een grote hoeveelheid aan tapbestanden worden gegenereerd. Het is ondoenlijk om deze bestanden één voor één te analyseren in Wireshark. Het is ook niet werkbaar om al deze bestanden samen te voegen om het samengevoegde bestand vervolgens in Wireshark te openen. In dit practicum gaan we eerst python scripts schrijven waarmee de tapbestanden kunnen worden gefilterd, bijv op datum en andere kenmerken. Hierbij maken we gebruik van de commandline versie van Wireshark: tshark. Als filter kun je daarom dezelfde filters toepassen als je tijdens eerdere practica in wireshark hebt gedaan.

Download het archief “tapbestanden.7z” met tapbestanden van Blackboard.

Opdracht 1: Python script voor wijzigen van naam van tapbestand

De tapbestanden zoals die in het Albuslux netwerk worden hebben een unieke naam, bijv capture.pcap35 en capture.pcap36. Omdat deze bestanden niet de extensie pcap hebben, kunnen ze zonder aanpassing niet door tshark worden verwerkt. Schrijf daarom een python script waarmee je de extensie van de tapbestanden wijzigt in .pcap en de namen van tapbestanden uniek blijven.

Tip: een eenvoudige manier is om de naam “capture.pcap35” te wijzigen in ”capture35.pcap”. je kunt natuurlijk ook iets verder gaan en ook de datum van het bestand in de naam plaatsen.

Opdracht 2: Python script voor filteren van tapbestanden

Bijgevoegd is het script “shark_filter_run_student_v3.py” waarmee alle bestanden in een bepaalde map kunnen worden gefilterd op tijd en andere kenmerken, zoals ip bronadres of MAC adres.

Pas de variabelen in de regels volgens op “#### init variables” aan en test het script vervolgens op een aantal pcap bestanden.

Opdracht 2: Analyse tapbestanden

Medewerker emp39 heeft op 6 oktober diverse handelingen uitgevoerd op de laptop. In het bestand “Laptop-acties v1.pdf” staat beschreven welke acties zijn uitgevoerd. Probeer elk van de acties terug te vinden in de tapbestanden. Als er mail is verstuurd bepaal dan ook de inhoud van de mailberichten.