Laboratorul 7 – Analiza Jurnalului de evenimente Windows

**Scopul** acestui laborator este să învețe studenții să analizeze jurnalele de evenimente Windows pentru identificarea artefactelor care prezintă interes.

**Sarcina:**

1. Completați câmpurile libere de mai jos cu informația corespunzătoare și cu ***capturile de ecran*** pentru fiecare întrebare, obținută în urma analizei fișierelor!

**Rezolvarea sarcinilor:**

Deschideți jurnalul de evenimente “Security.evtx” (și altele) selectând File>Open Log File>Standard…

1. Câte evenimente au fost înregistrate?
2. Care este ID-ul evenimentului și tipul de autentificare pentru un logon de consolă reușit?
3. Când a fost prima conectare la consola folosind contul Rock Hammerfist?
4. Câte autentificări succesive au fost?
5. Au fost evenimente de conectare de tip 10?
   1. Câte?
   2. Care cont a fost folosit?
   3. Care a fost adresa IP?
   4. Care au fost cele mai vechi și cele mai recente mărci de timp? (Sugestie: adăugați la cronologie.)

Folosiți jurnalul de evenimente “Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx” și răspundeți la următoarele întrebări. Puteți folosi fie Event Log Explorer sau Microsoft’s Event Viewer (double-click pe fișierul jurnal).

1. Sesiunea (sesiunile) RDP pe care am văzut-o în jurnalul evenimentelor de securitate apare aici?
2. Care este ID-ul Evenimentului?
3. Câte astfel de evenimente au fost?

**Deși am văzut aceste logări în jurnalul de evenimente de securitate, amintiți-vă că jurnalul de evenimente de securitate are multe, multe alte evenimente care se înregistrează mai frecvent. Dacă rulajul este mai mic, acest jurnal conține de obicei înregistrări mult mai vechi ale accesului RDP la sistem.**

Folosiți jurnalul de evenimente “Application.evtx” și răspundeți la următoarele întrebări. Puteți folosi fie Event Log Explorer sau Microsoft’s Event Viewer (double-click pe fișierul jurnal).

1. Au fost înregistrate alte evenimente în jurul perioadei în care a fost inițiată prima sesiune RDP? (Sugestie: Adăugați la cronologie.)
2. La ce oră a fost Windows Defender amânat pentru prima dată? Când a fost acesta oprit pentru ultima dată?

**\*Acum reveniți la Lab 5 - Analiza Prefetch și răspundeți la întrebarea 4.**