Министерство образования республики Молдова

Технический Университет Молдовы

Департамент Программной Инженерии и Автоматики

О т ч ё т

Лабораторная работа №7

По предмету: Infractiuni informatice si tehnici de investigare

Выполнил студ. гр. SI-202 Абабий Эдуард

Проверил Масютин Максим

Кишинёв – 2023

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:

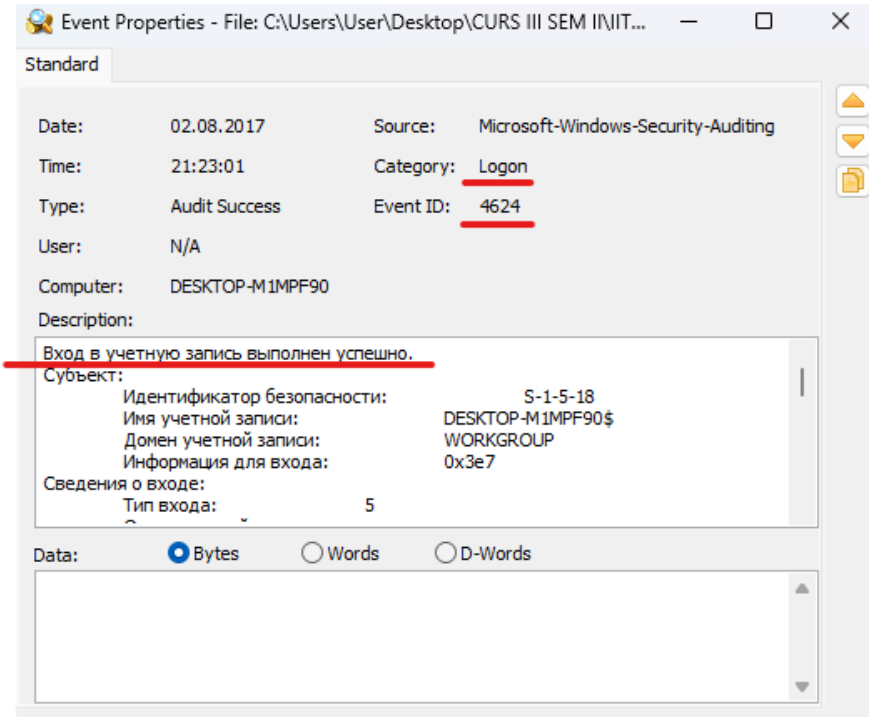
Deschideți jurnalul de evenimente “Security.evtx” (și altele) selectând File>Open Log File>Standard…

1. Câte evenimente au fost înregistrate?

   17245

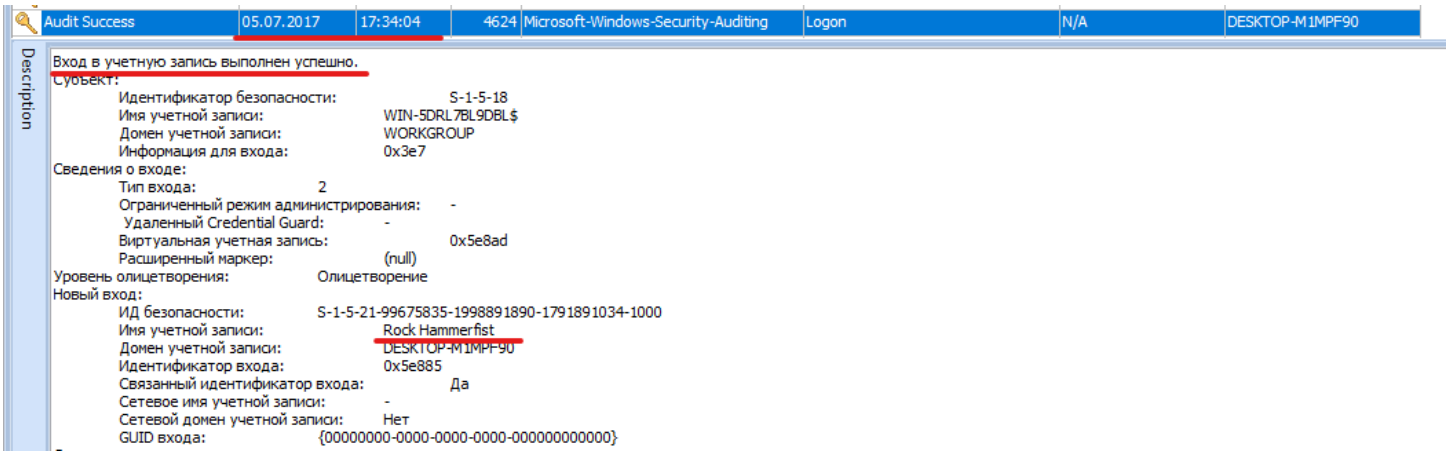
2. Care este ID-ul evenimentului și tipul de autentificare pentru un logon de consolă reușit?

   Event ID: 4624



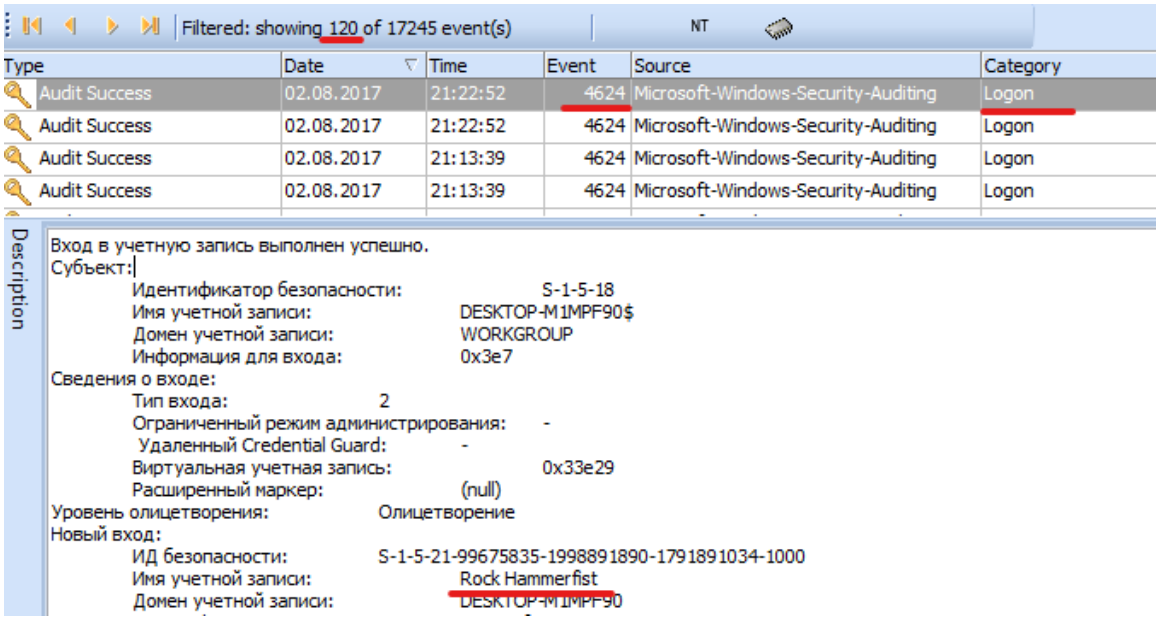
3. Când a fost prima conectare la consola folosind contul Rock Hammerfist?

Первое подключение было 05.07.2017 в 17:34:04



4. Câte autentificări succesive au fost?

120

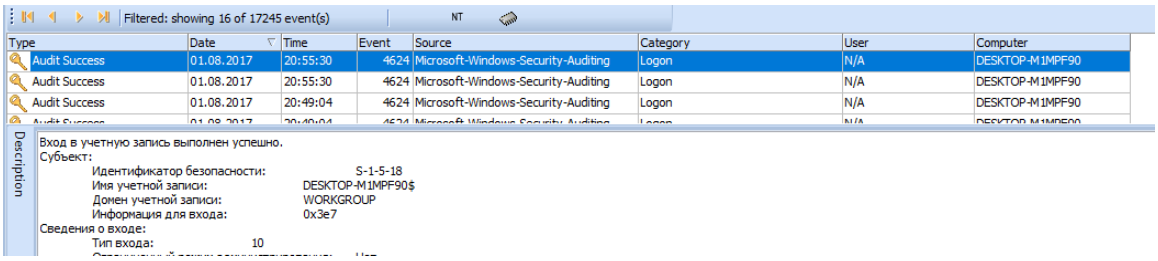


5. Au fost evenimente de conectare de tip 10?

Да

a. Câte?

16

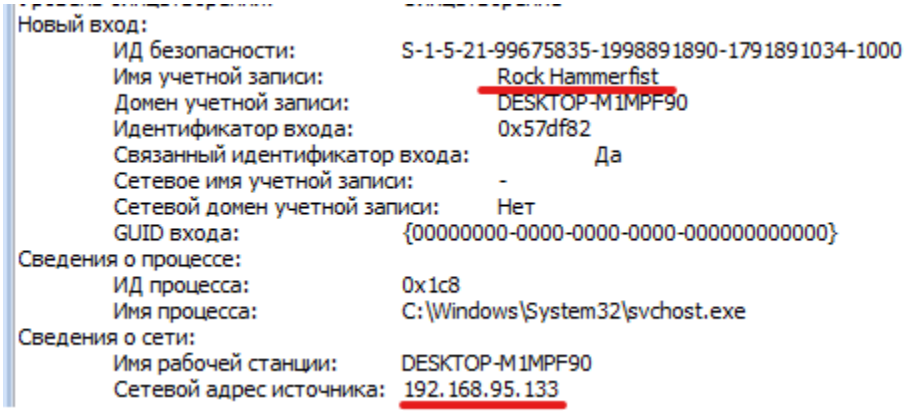


b. Care cont a fost folosit?

Была использован только учетная запись только Rock Hammerfist

c. Care a fost adresa IP?

192.168.95.133



d. Care au fost cele mai vechi și cele mai recente mărci de timp? (Sugestie: adăugați la cronologie.)

Первый вход был в 18:45:39 / Последний вход в 20:55:30
Оба в один и тот же день 01.08.2017 года

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	01.08.2017	18:48:39	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	18:48:39	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	18:56:40	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	18:56:40	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	19:21:56	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	19:21:56	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:12:30	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:12:30	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:26:54	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:26:54	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:40:43	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:40:43	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:49:04	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:49:04	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:55:30	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90
Audit Success	01.08.2017	20:55:30	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	DESKTOP-M1MPF90

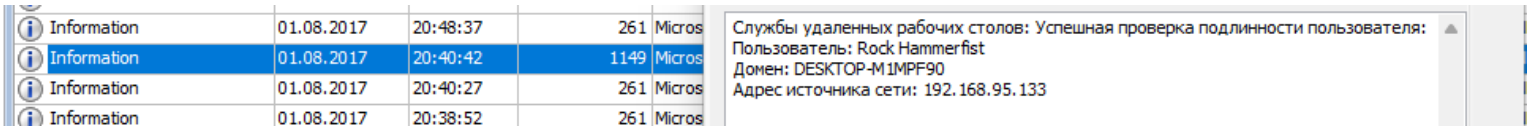
Folosiți jurnalul de evenimente “Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx” și răspundeți la următoarele întrebări. Puteți folosi fie Event Log Explorer sau Microsoft’s Event Viewer (double-click pe fișierul jurnal).

1. Sesiunea (sesiunile) RDP pe care am văzut-o în jurnalul evenimentelor de securitate apare aici?

   Да

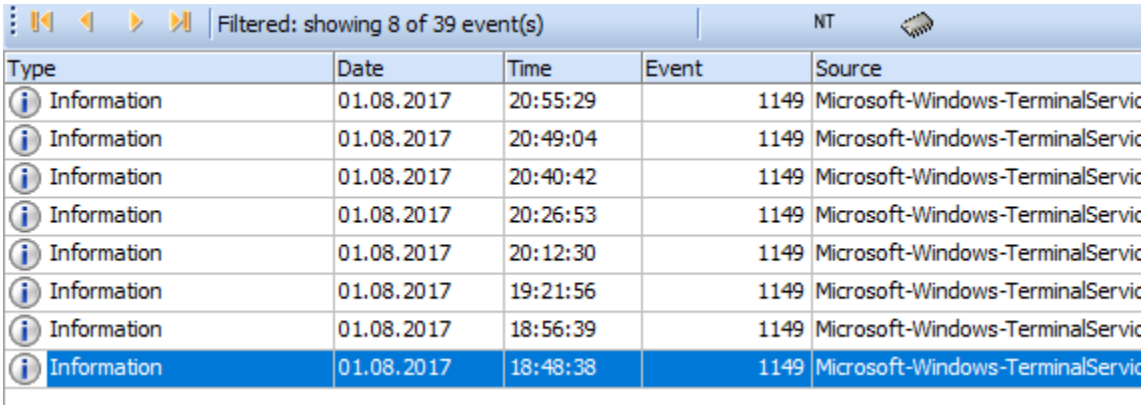
2. Care este ID-ul Evenimentului?

   1149



3. Câte astfel de evenimente au fost?

   8



Filtered: showing 8 of 39 event(s)

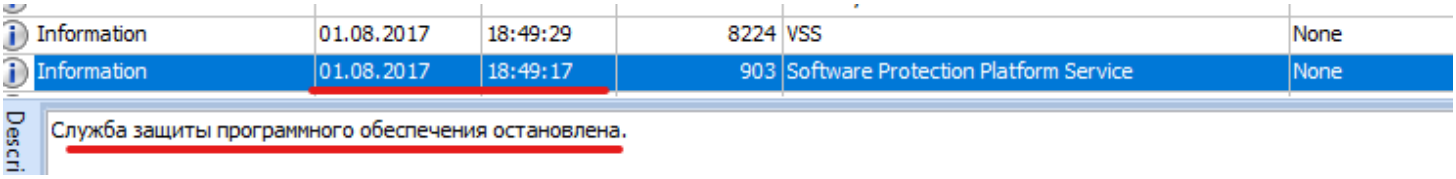
Type	Date	Time	Event	Source
Information	01.08.2017	20:55:29	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	20:49:04	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	20:40:42	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	20:26:53	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	20:12:30	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	19:21:56	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	18:56:39	1149	Microsoft-Windows-TerminalServic
Information	01.08.2017	18:48:38	1149	Microsoft-Windows-TerminalServic

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.)

   Да, была приостановлена служба защиты Windows



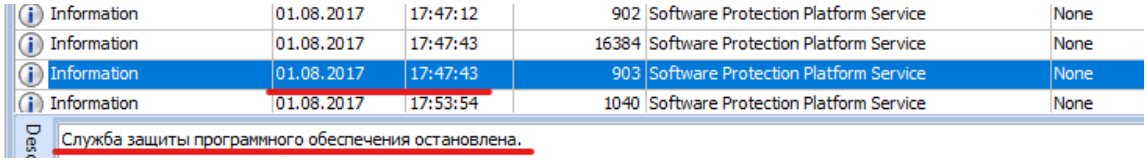
Information	01.08.2017	18:49:29	8224	VSS	None
Information	01.08.2017	18:49:17	903	Software Protection Platform Service	None

Descri

Служба защиты программного обеспечения остановлена.

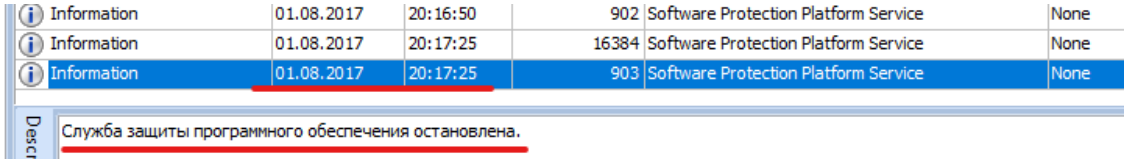
2. La ce oră a fost Windows Defender amânat pentru prima dată? Când a fost acesta oprit pentru ultima dată?

   01.08.2017 17:47:43 был приостановлен в первый раз
   01.08.2017 20:17:25 был приостановлен в последний раз



Information	01.08.2017	17:47:12	902	Software Protection Platform Service	None
Information	01.08.2017	17:47:43	16384	Software Protection Platform Service	None
Information	01.08.2017	17:47:43	903	Software Protection Platform Service	None
Information	01.08.2017	17:53:54	1040	Software Protection Platform Service	None

Служба защиты программного обеспечения остановлена.



Information	01.08.2017	20:16:50	902	Software Protection Platform Service	None
Information	01.08.2017	20:17:25	16384	Software Protection Platform Service	None
Information	01.08.2017	20:17:25	903	Software Protection Platform Service	None

Служба защиты программного обеспечения остановлена.

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

Вывод: В данной лабораторной работе я научился анализировать журналы событий Windows, чтобы отслеживать все события, которые произошли в системе. Такие как вход в систему, выход из системы, отключение определённых компонентов системы и др. Что позволяет отследить действия злоумышленника и узнать откуда и как произошло проникновениею.