Gerren Jerome - Malware Threats

Malware Analysis and Enumeration Project

Introduction

In my role as an ethical hacker with the EC-Council, I conducted an extensive project focused on malware analysis and enumeration techniques. This project was designed to demonstrate my capabilities in identifying, creating, and analyzing malware, as well as extracting critical information from target networks to enhance security measures.

Objectives

The primary objectives of this project were:

- **Malware Creation and Exploitation:**
  - Creating a Trojan and exploiting a target machine.
  - Developing a virus to infect the target machine.
  - Conducting malware analysis to determine origin, functionality, and potential impact.
  - Detecting malware within a network.
- **Enumeration:**
  - Extracting various pieces of information about the target, such as machine names, ports, operating systems, services, network resources and shares, usernames, user groups, policies, passwords, routing tables, audit settings, and service configurations.

Tasks and Techniques

This project involved performing a series of tasks using a variety of tools and techniques to achieve thorough malware analysis and enumeration. The tasks included:

1. **Creating and Exploiting Malware:**
   - **Trojan Creation and Exploitation:** Gaining access to and control over victim machines using tools like njRAT and Theef RAT Trojan.
   - **Virus Creation:** Using the JPS Virus Maker Tool to develop a virus and infect target systems.
2. **Static Malware Analysis:**
   - Using tools like Hybrid Analysis, BinText, PeID, Detect It Easy (DIE), PE Explorer, Dependency Walker, IDA, OllyDbg, and Ghidra to perform static analysis of malware samples.
3. **Dynamic Malware Analysis:**
   - Employing tools like TCPView, CurrPorts, Process Monitor, Reg Organizer, Windows Service Manager, Autoruns for Windows, WinPatrol, Mirekusoft Install Monitor, PA File Sight, DriverView, Driver Reviver, and DNSQuerySniffer to perform dynamic analysis of malware behavior and system interactions.
4. **Enumeration Techniques:**
   - **NetBIOS Enumeration:** Using Windows command line tools and NetBIOS Enumerator.
   - **SNMP Enumeration:** Utilizing tools like snmp-check, SoftPerfect Network Scanner, and snmpwalk.
   - **LDAP Enumeration:** Using Active Directory Explorer, Python (ldap3), and Nmap for LDAP exploration.

- **NFS Enumeration:** Conducting scans using RPCScan and SuperEnum.
- **DNS Enumeration:** Performing DNS zone transfers, DNSSEC zone walking, and service discovery with tools like dig, dnsrecon, and Nmap.
- **SMTP Enumeration:** Listing mail users and open SMTP relays with Nmap.
- **General Enumeration Tools:** Employing Global Network Inventory, Advanced IP Scanner, and Enum4linux for comprehensive network resource enumeration.

Tools Utilized

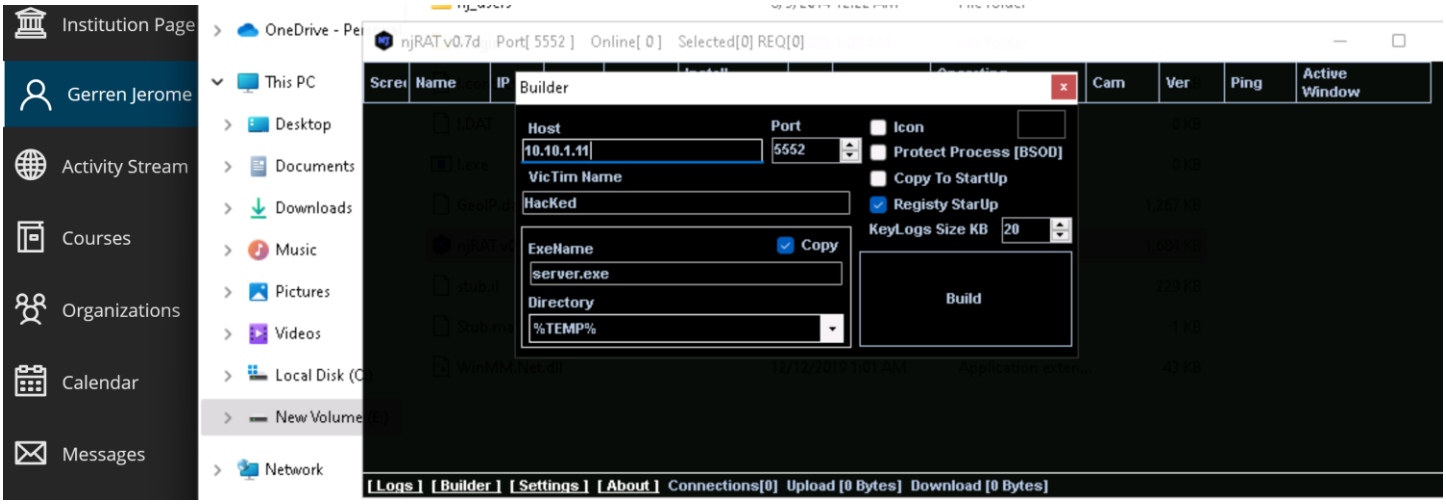
Throughout this project, I utilized several key tools to perform malware analysis and enumeration tasks, including:

- **njRAT** and **Theef RAT**: For creating and exploiting Trojans.
- **JPS Virus Maker Tool:** For creating viruses.
- Hybrid Analysis, BinText, PeID, DIE, PE Explorer, Dependency Walker, IDA, OllyDbg, Ghidra: For static malware analysis.
- TCPView, CurrPorts, Process Monitor, Reg Organizer, Windows Service Manager, Autoruns, WinPatrol, Mirekusoft Install Monitor, PA File Sight, DriverView, Driver Reviver, DNSQuerySniffer: For dynamic malware analysis.
- NetBIOS Enumerator, snmp-check, SoftPerfect Network Scanner, snmpwalk, Active Directory Explorer, Nmap, RPCScan, SuperEnum, dig, dnsrecon, Global Network Inventory, Advanced IP Scanner, Enum4linux: For enumeration tasks.

Gain access to the target system using Trojans.

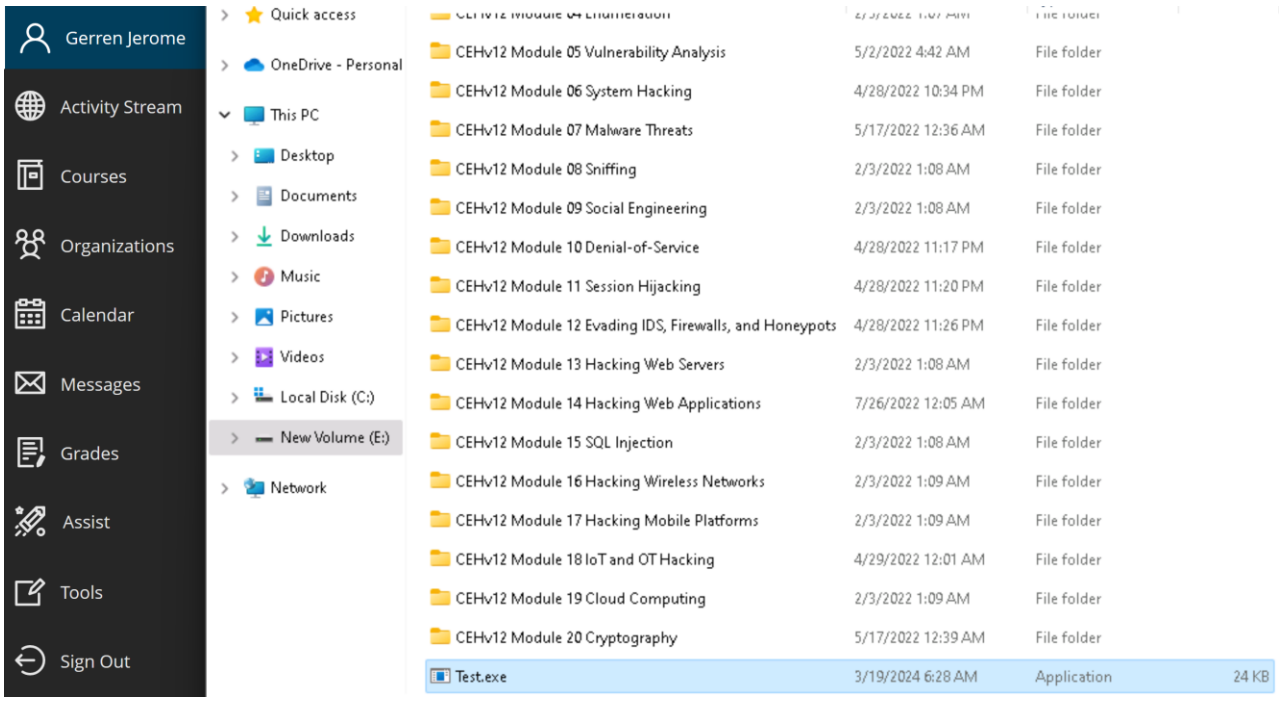
Gain control over a victim machine using the njRAT RAT Trojan

Confirm install with port (5552) and listener host (WIN_11; 10.10.1.11)

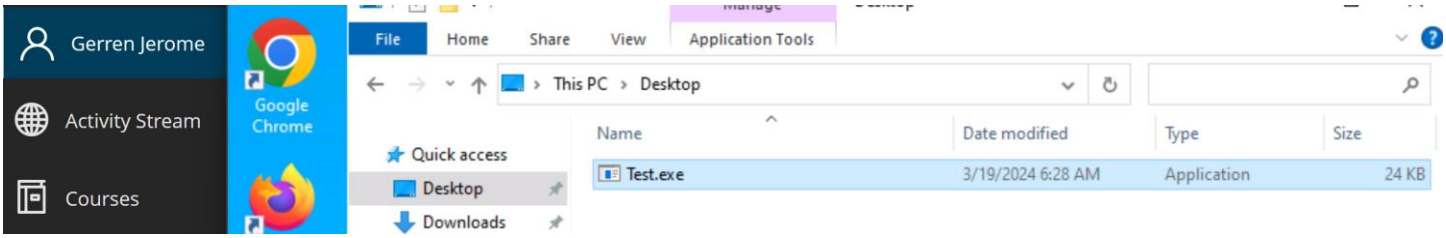


Gerren Jerome - Malware Threats

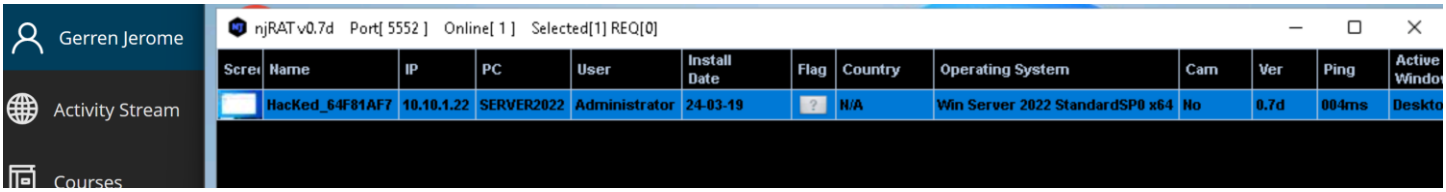
Confirm creation and upload of Test.exe to share folder.



Launch Test.exe on WIN_SVR_22

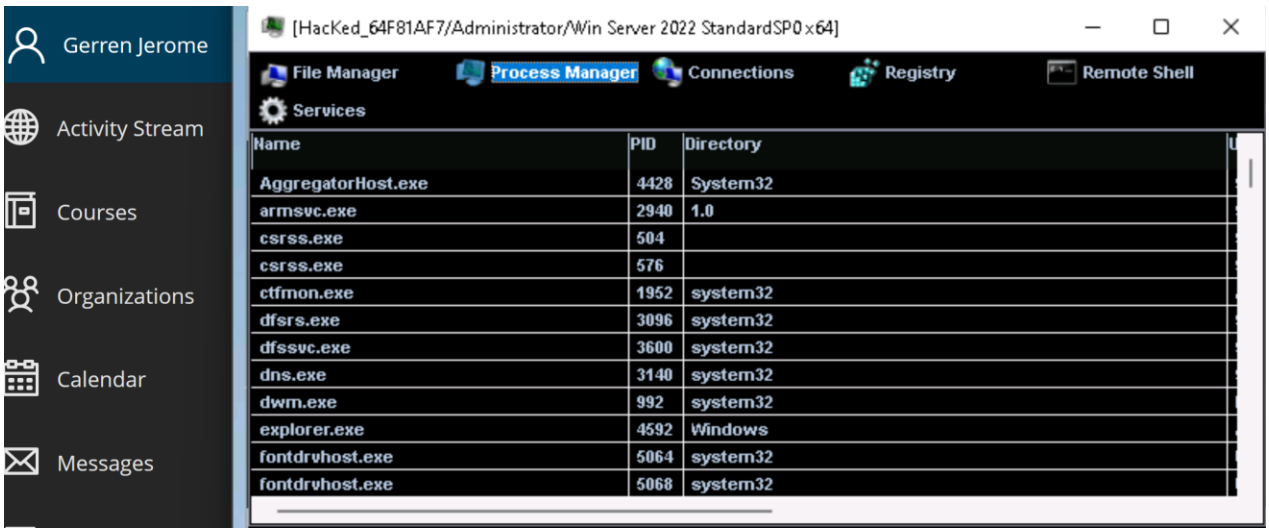


Confirm control session between WIN_11 and WIN_SVR_22

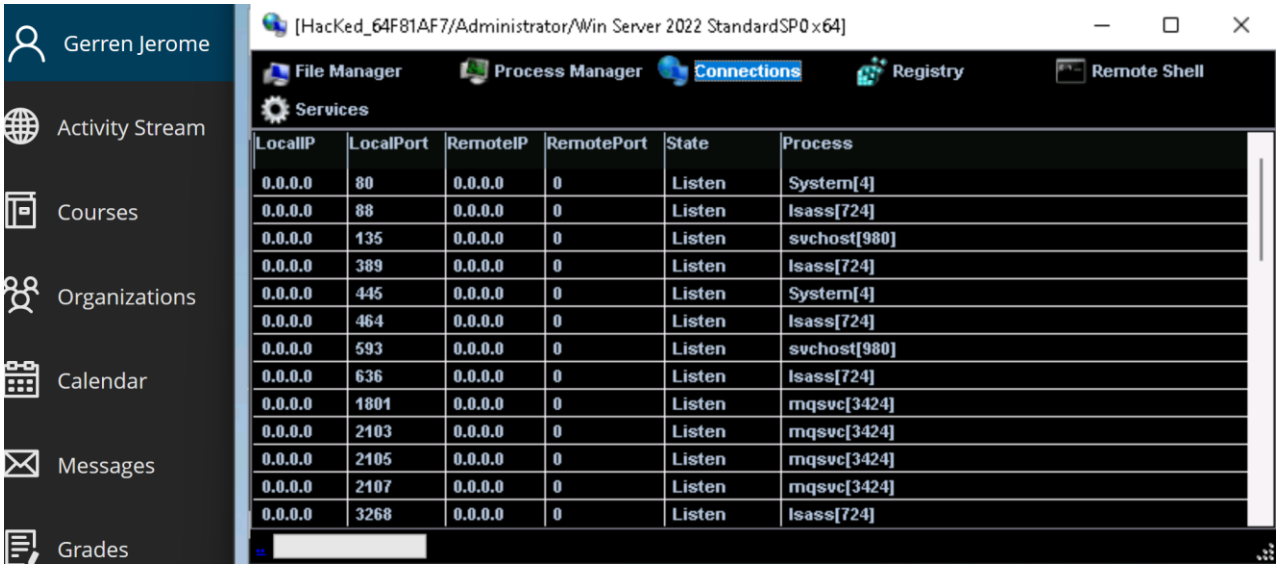


Gerren Jerome - Malware Threats

Show Process Manager in njRAT control panel.



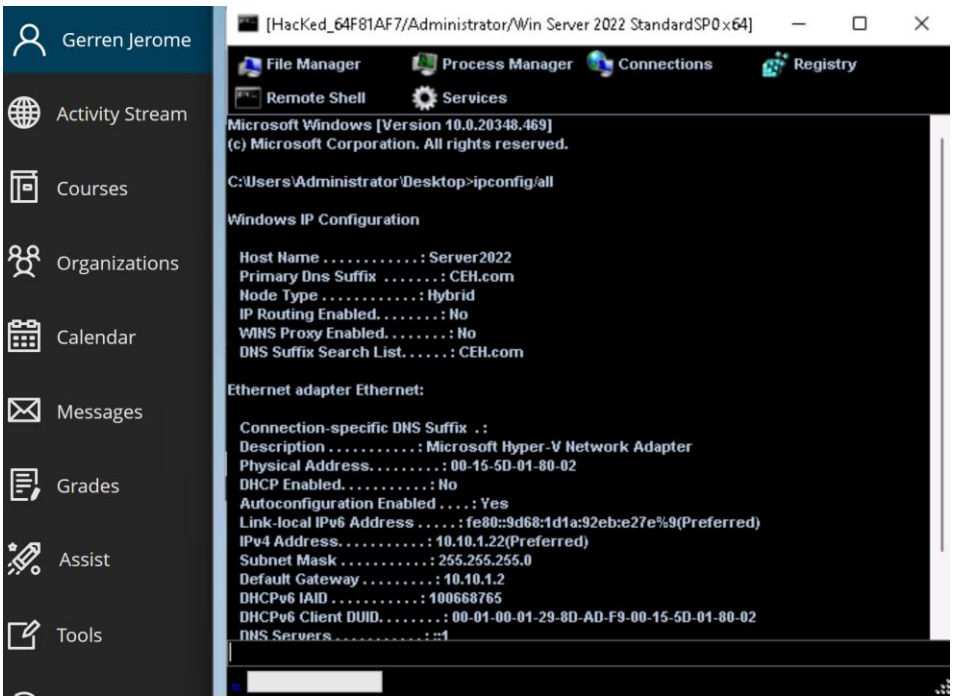
Show network connections.



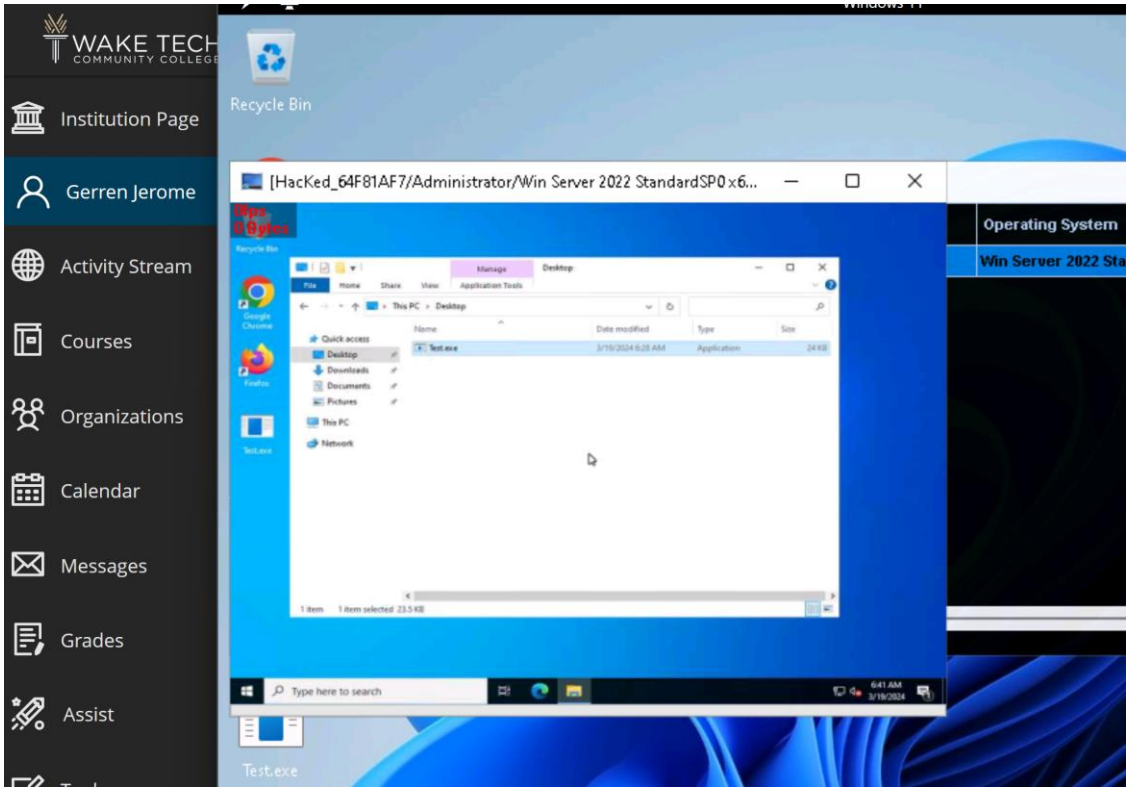
Show registry.

Gerren Jerome - Malware Threats

Show remote shell, confirm connection using ipconfig.

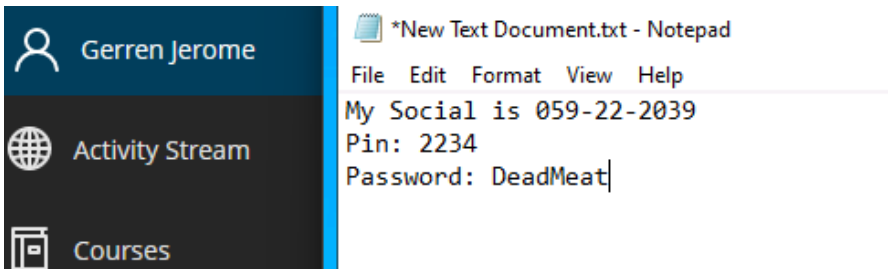


Show remote desktop.

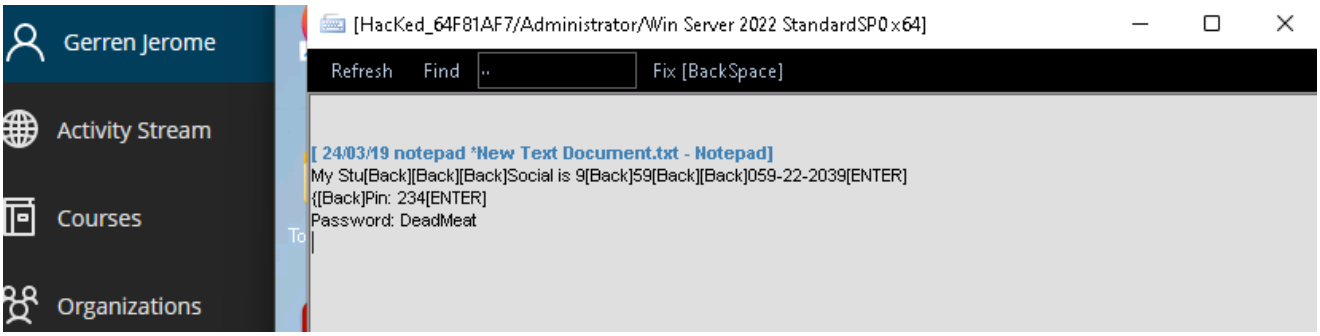


Gerren Jerome - Malware Threats

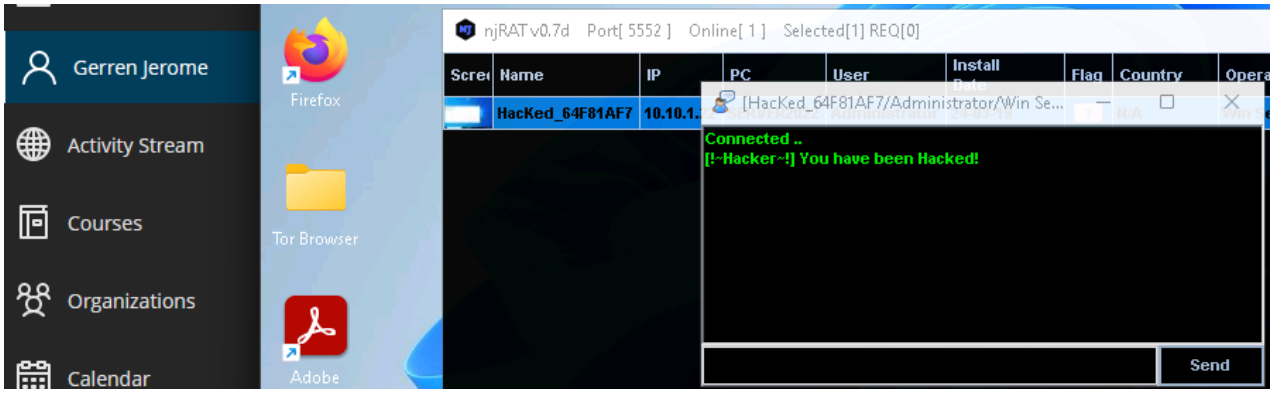
Create dummy text/actions on victim (WIN_SVR_22) machine.



Confirm surveillance on WIN_11 machine in njRAT.



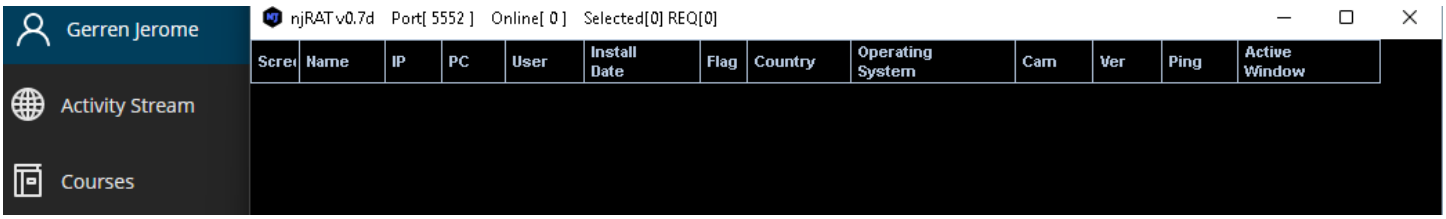
Send chat message (WIN_11)

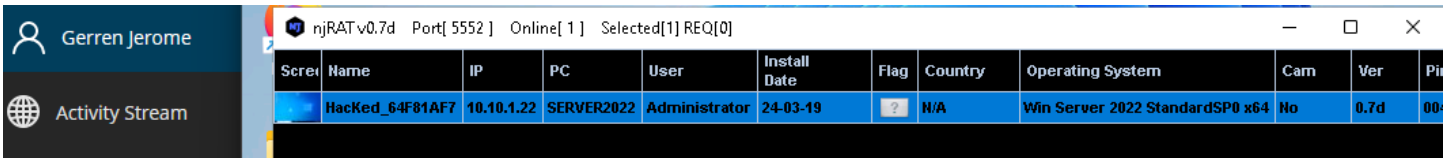


Display chat message (WIN_SVR_22)

Gerren Jerome - [Malware Threats]

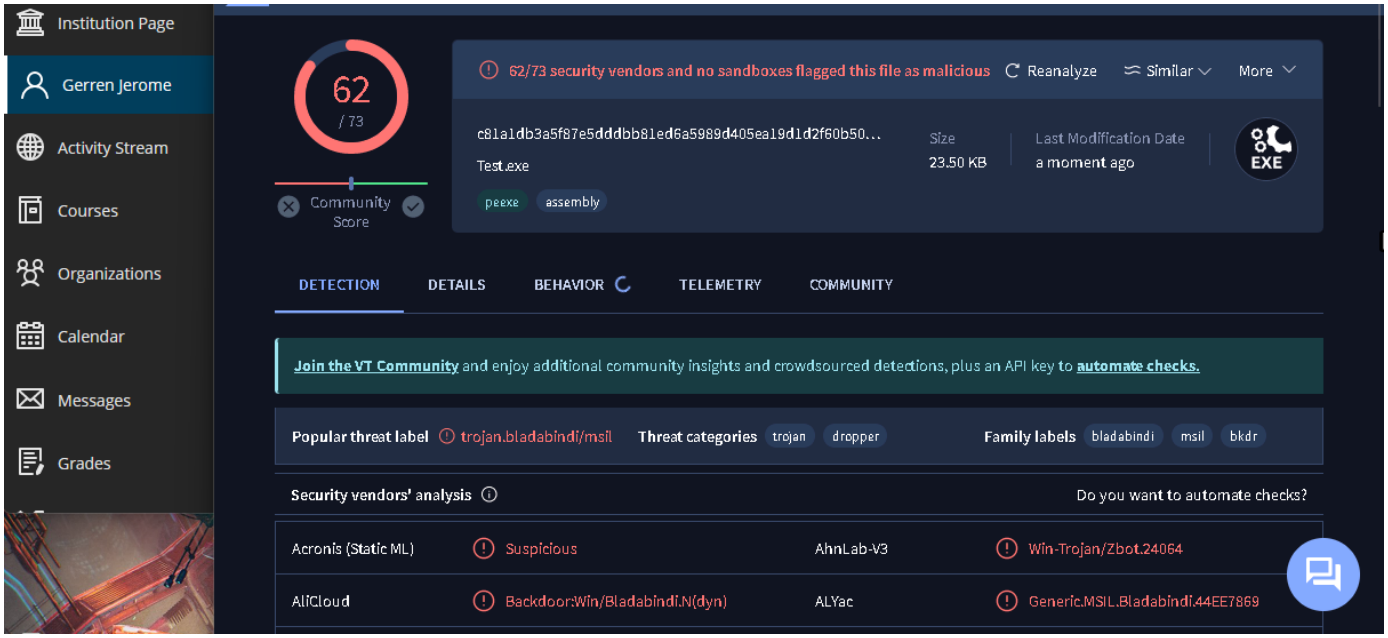
Show automatic recapture of connection with victim.



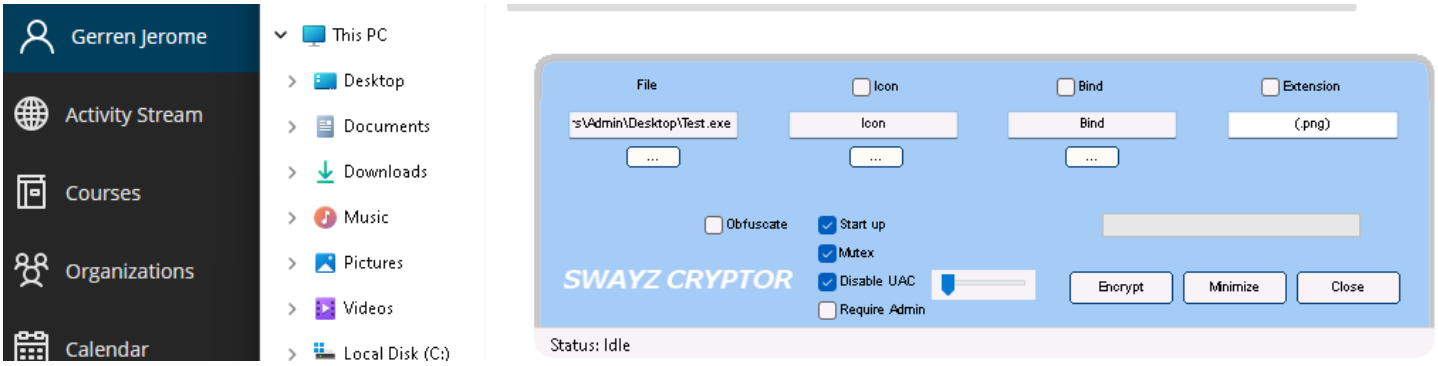


Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs

Results of VirusTotal scan for Test.exe

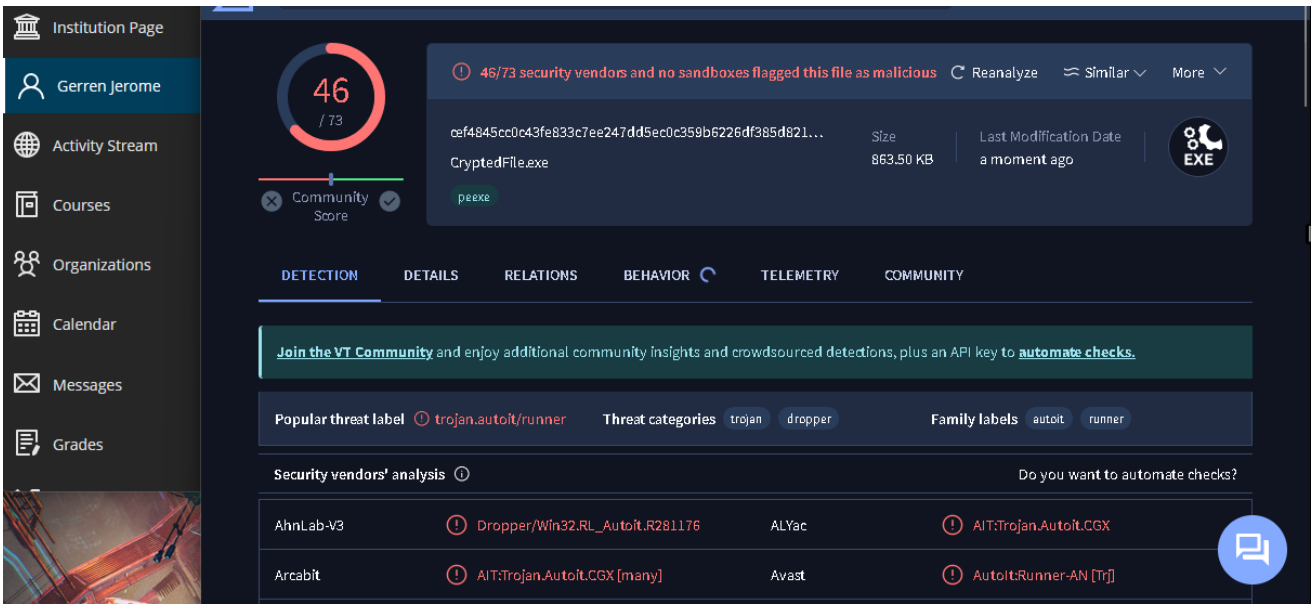


Confirm encryption options in SwayzCryptor

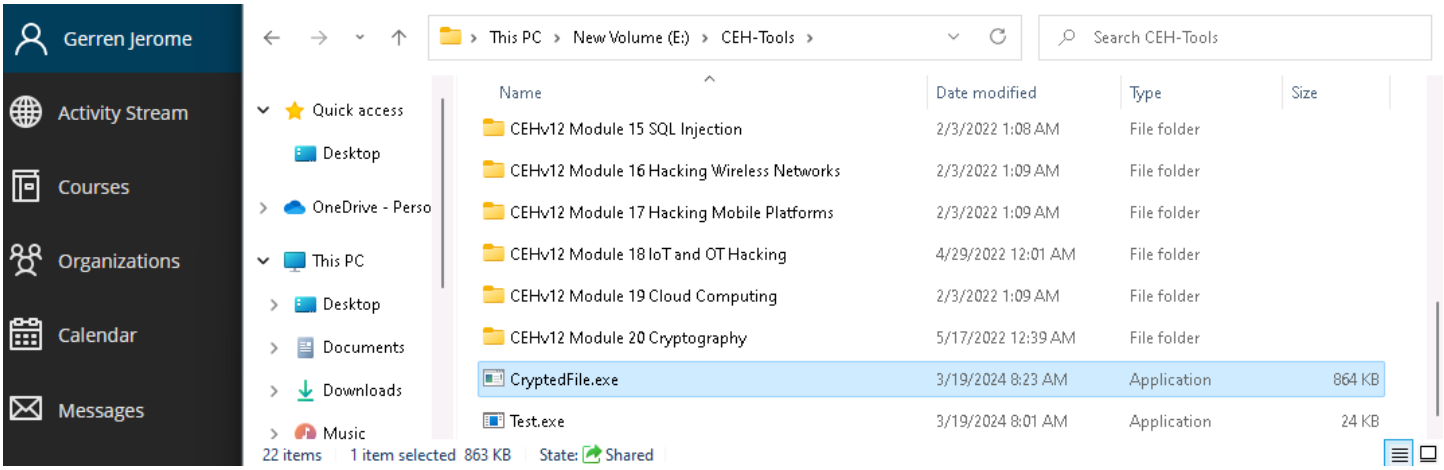


Gerren Jerome - [Malware Threats]

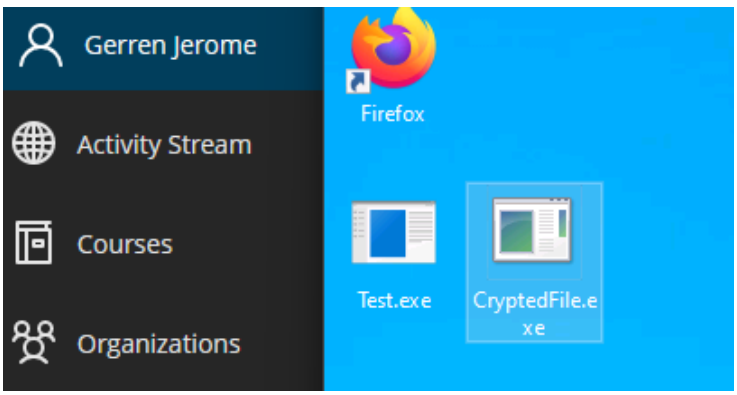
Upload CryptedFile.exe to VirusTotal and compare results



Upload CryptedFile to the CEH-Tools folder.

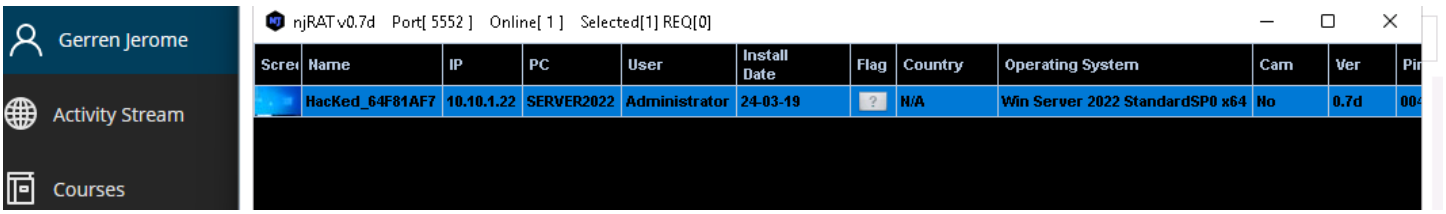


Copy CryptedFile to Desktop of WIN_SVR_22 and run.



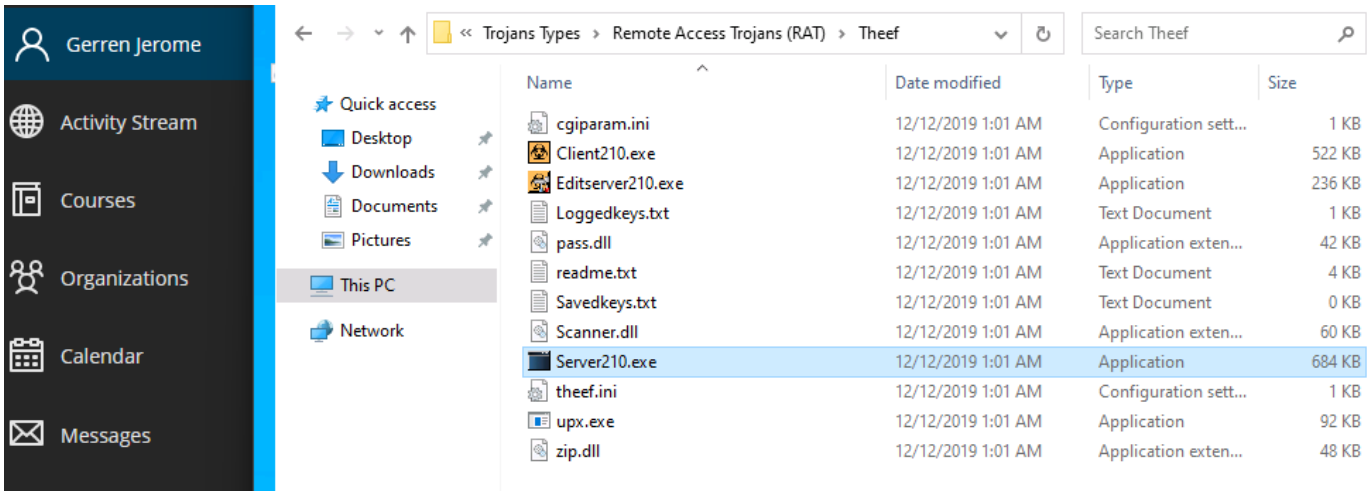
Gerren Jerome - [Malware Threats]

Confirm session in njRAT between WIN_SVR_22 and WIN_11

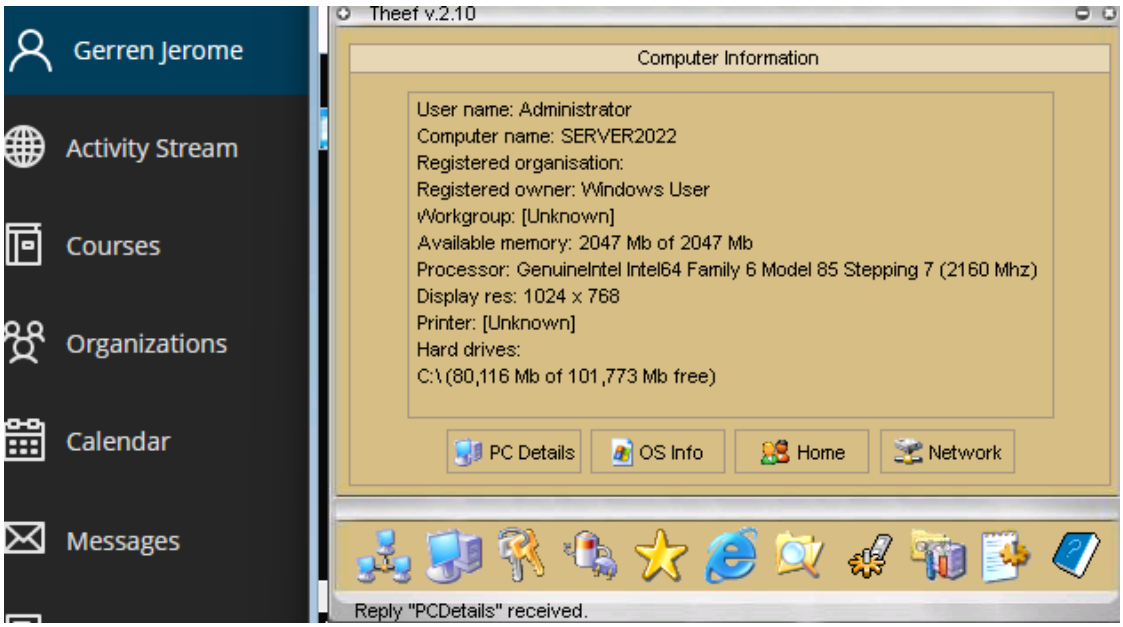


Create a Trojan server using Theef RAT Trojan

Run Server210 (Theef) on WIN_SVR_22

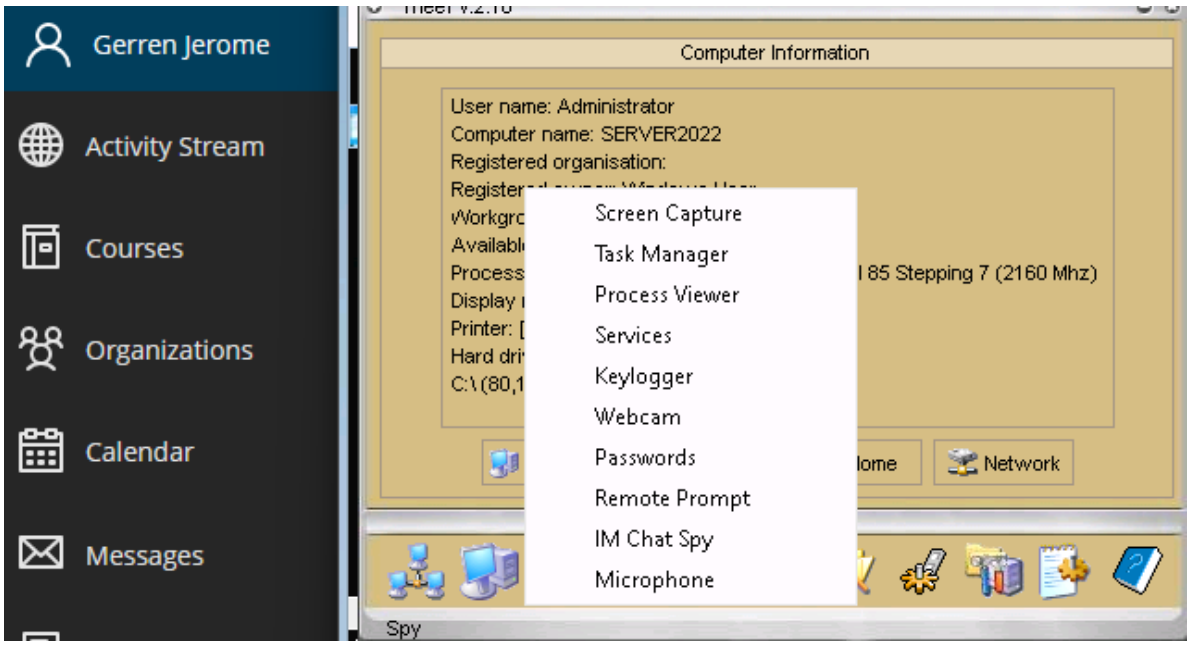


Run Client210 on WIN_11 and view WIN_SVR_22's info in Theef's menu

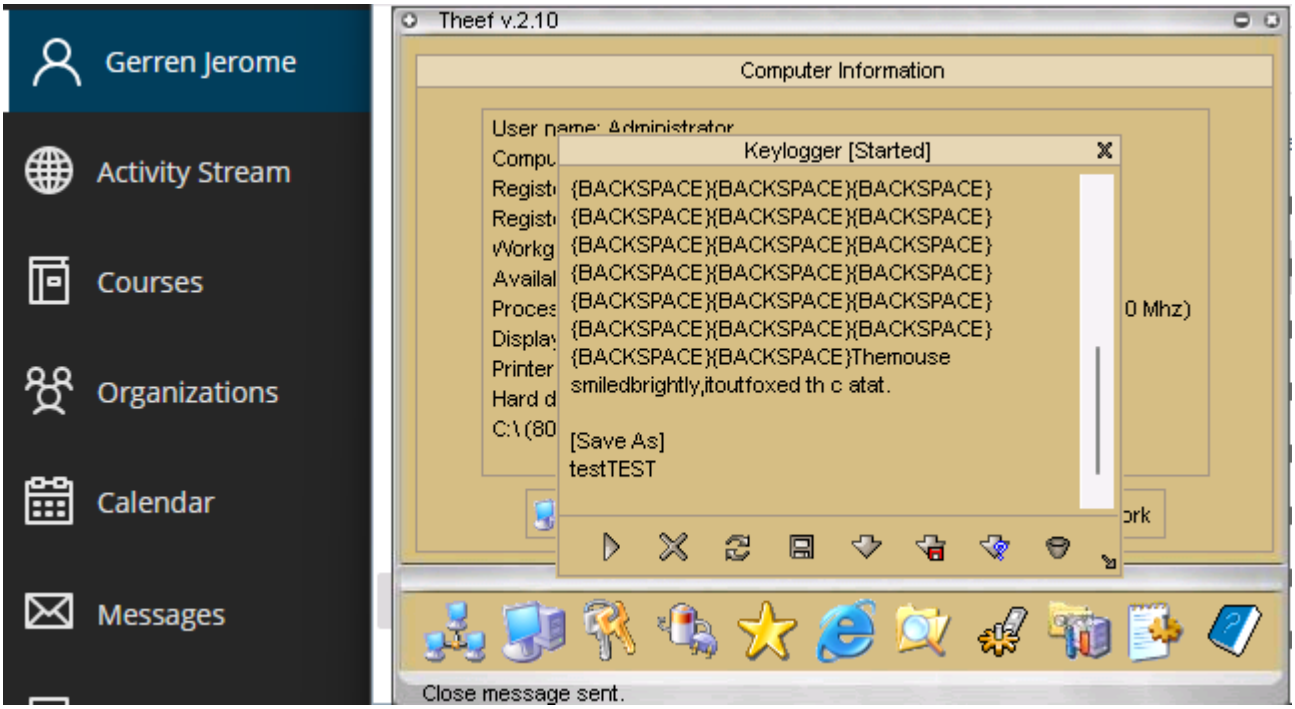


Gerren Jerome - [Malware Threats]

Show results of Spy screen in Theef



Launch keylogger in Theef, write some stuff on WIN_SVR_22, then confirm on WIN_11

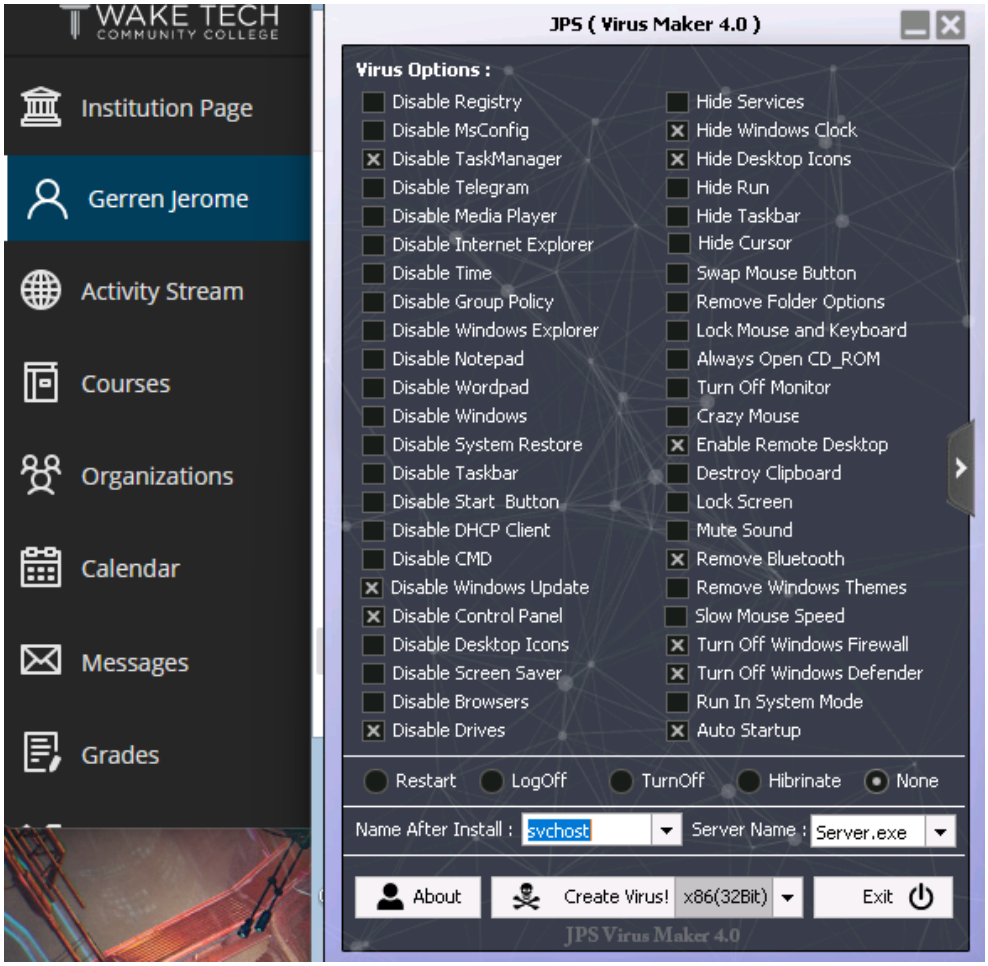


Gerren Jerome - Malware Threats

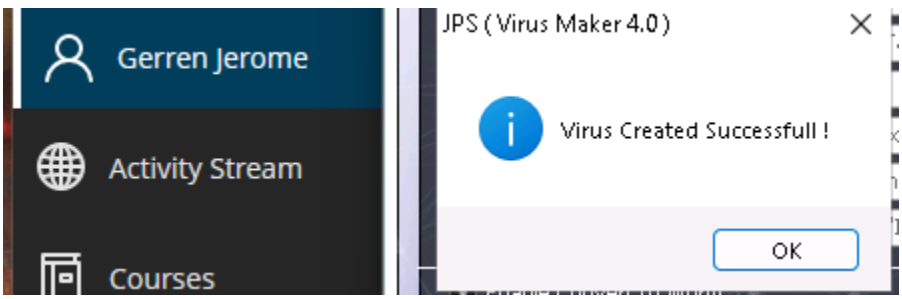
Infect the target system using a virus.

Create a virus using the JPS Virus Maker Tool and infect the target system.

Create and config virus, part 1 (Virus Options – Left hand menu)

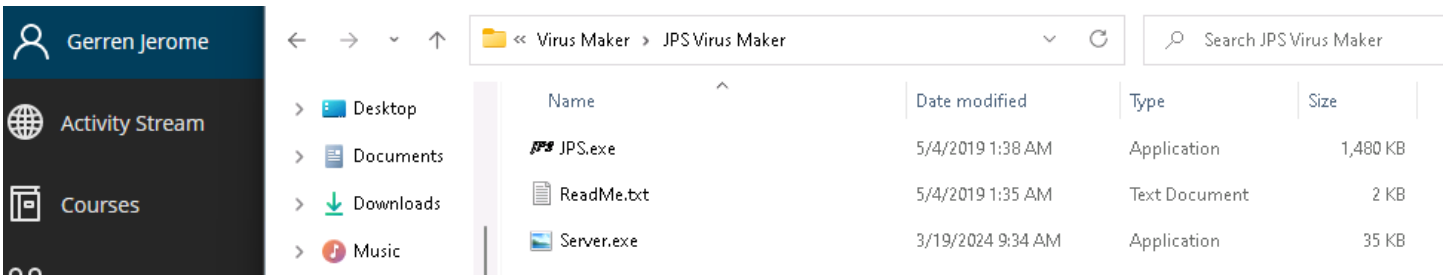


Create and config virus, part 2 (Virus Options – Right hand menu)

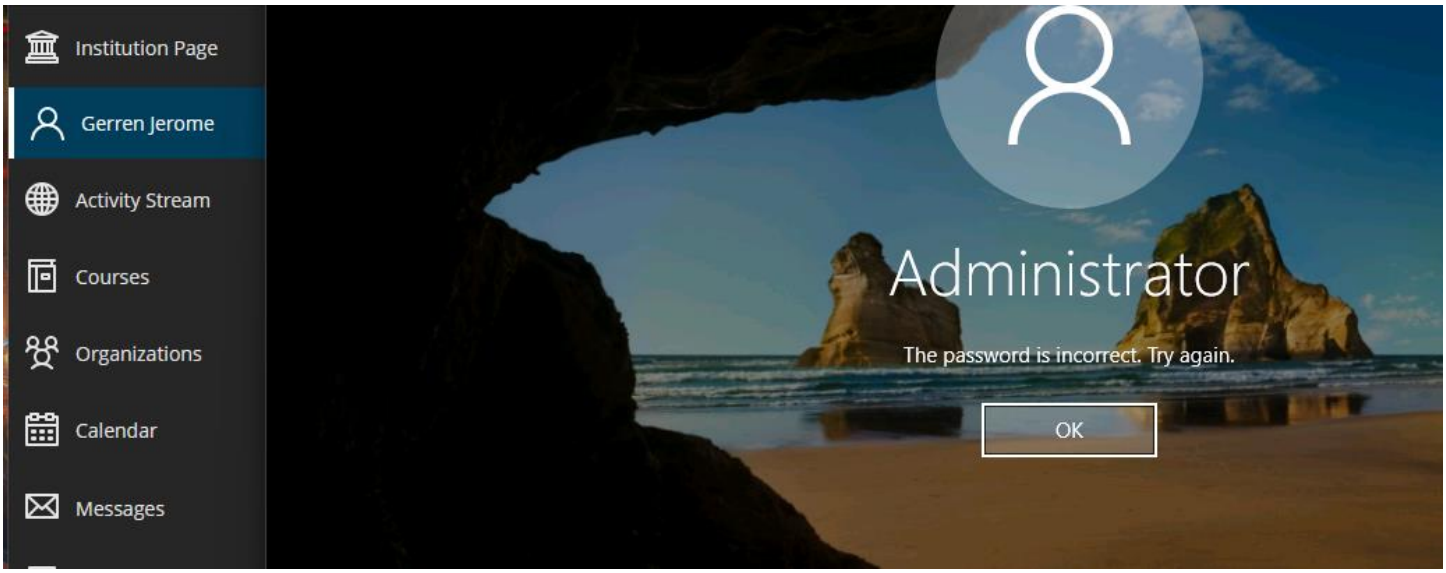


Gerren Jerome - [Malware Threats]

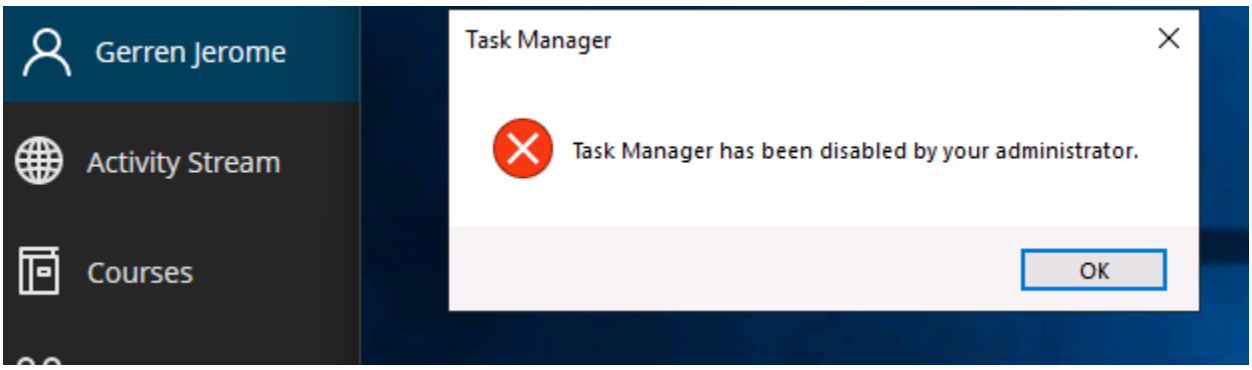
Confirm server.exe is in the JPS Virus Maker folder.



Launch server.exe on WIN_SVR_19, attempt to restart and login.



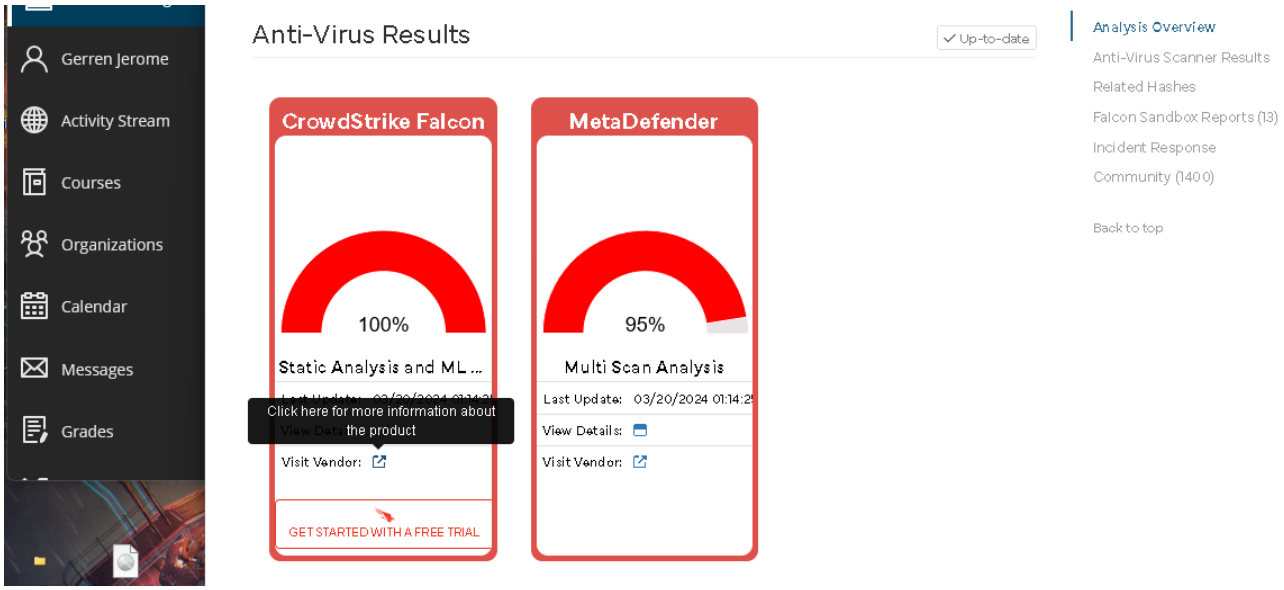
After using new password from Step 9, show Task Manager is disabled.



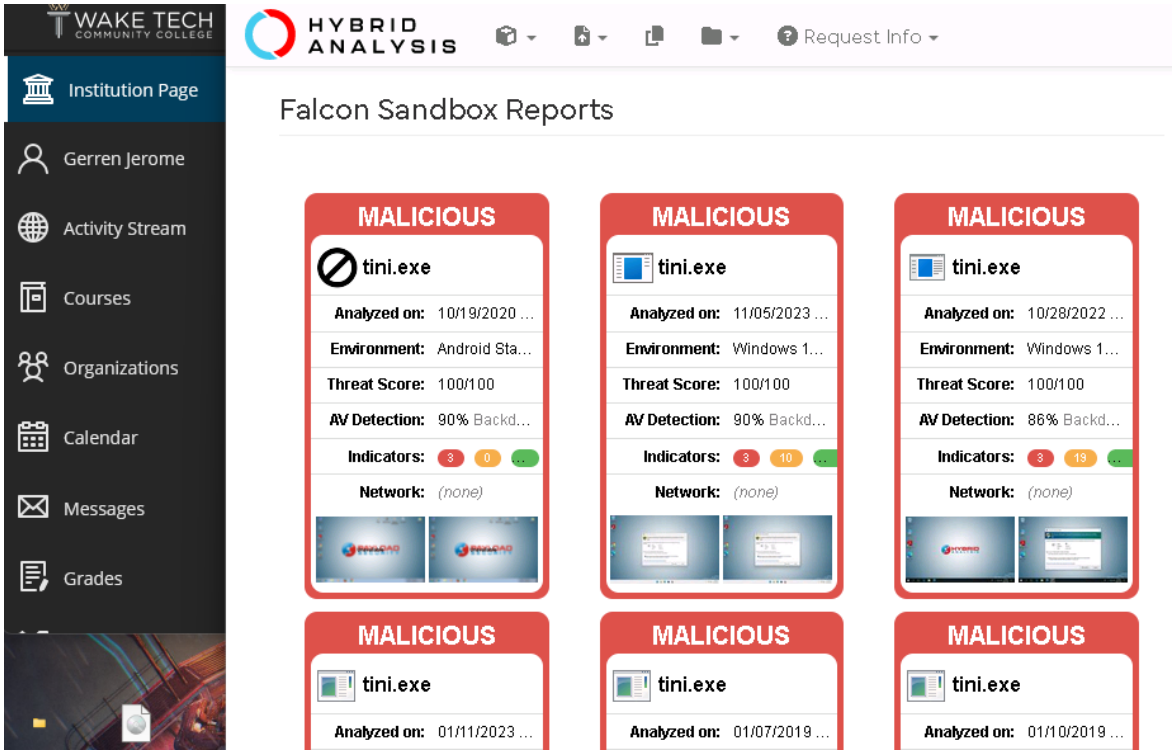
Gerren Jerome - [Malware Threats]

Perform static malware analysis

Perform malware scanning using Hybrid Analysis



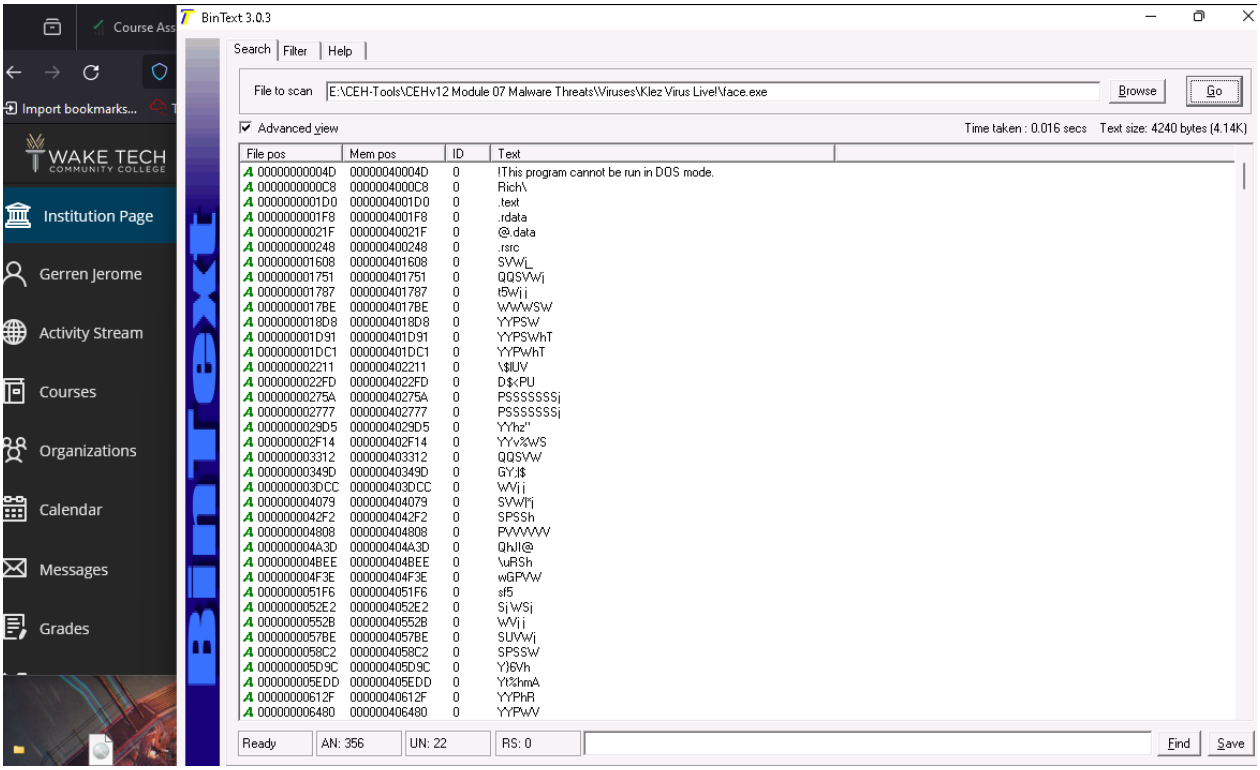
Information from Falcon Sandbox Reports



Gerren Jerome - [Malware Threats]

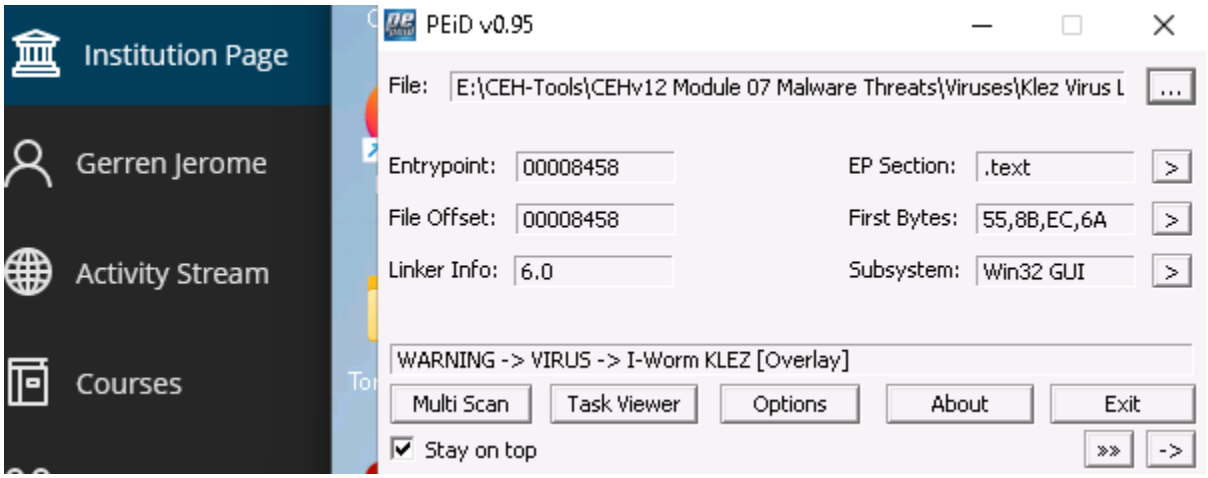
Perform a strings search using BinText.

Extracted information from face.exe in BinText.



Identify packaging and obfuscation methods using Peid

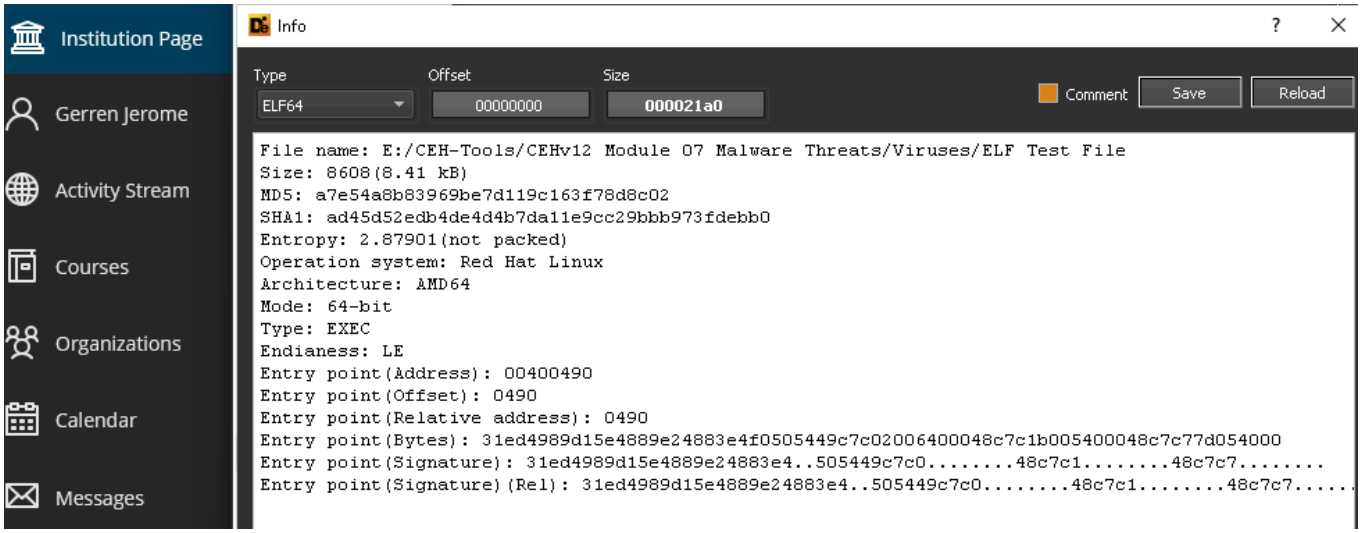
Analysis information from PeID of face.exe



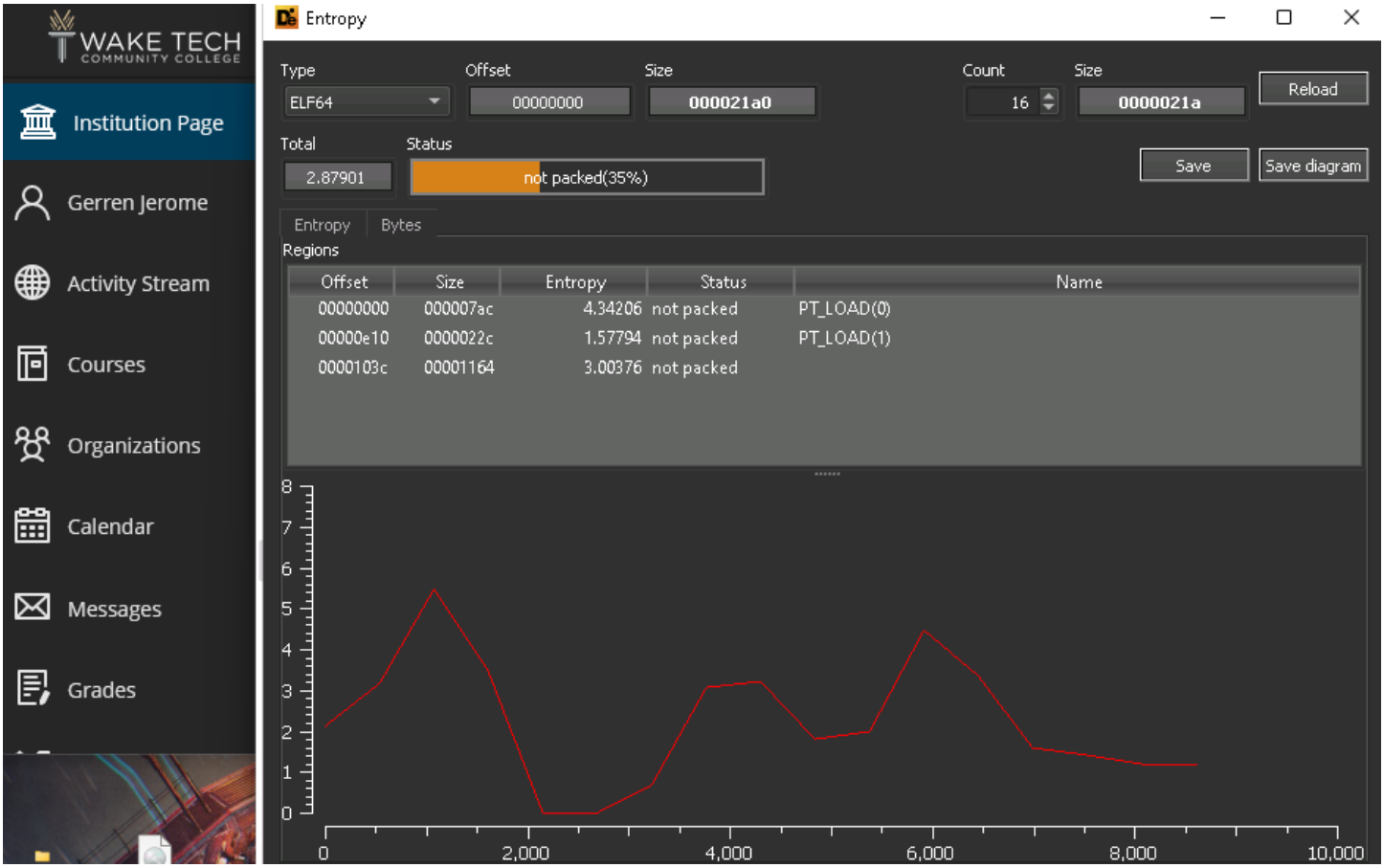
Gerren Jerome - Malware Threats

Analyze ELF executable file using Detect It Easy (DIE)

File info of ELF test file



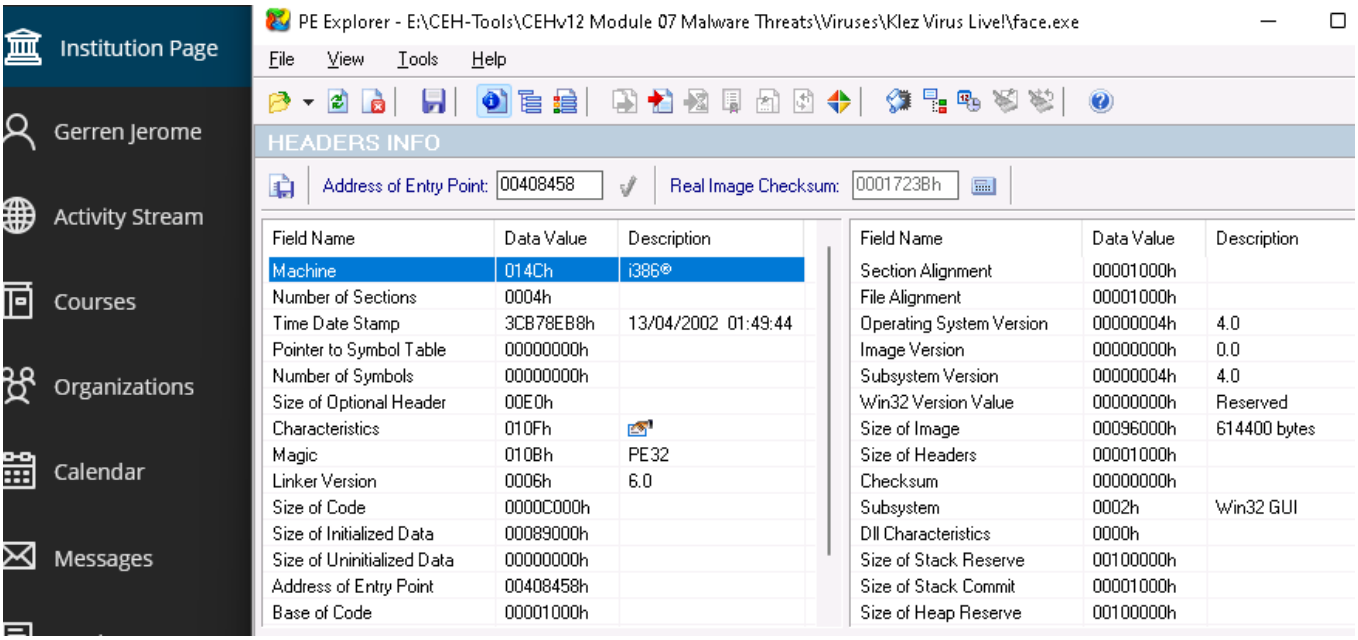
Entropy graph of ELF test file



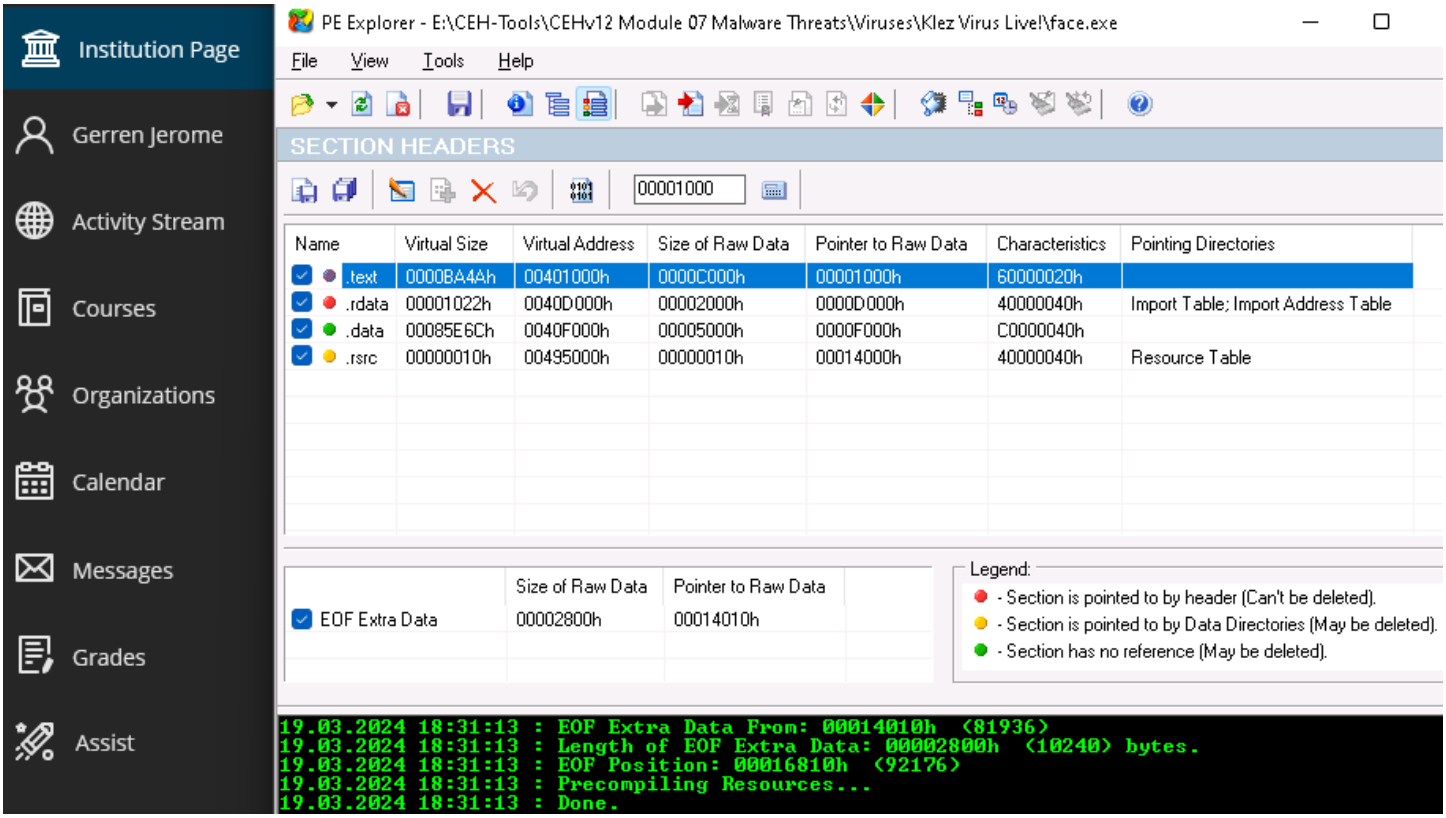
Gerren Jerome - Malware Threats

Find the portable executable (PE) info of a malware executable file using PE Explorer

Scan result (Headers Info) for face.exe in PE Explorer



Scan result (Section Headers) for face.exe in PE Explorer

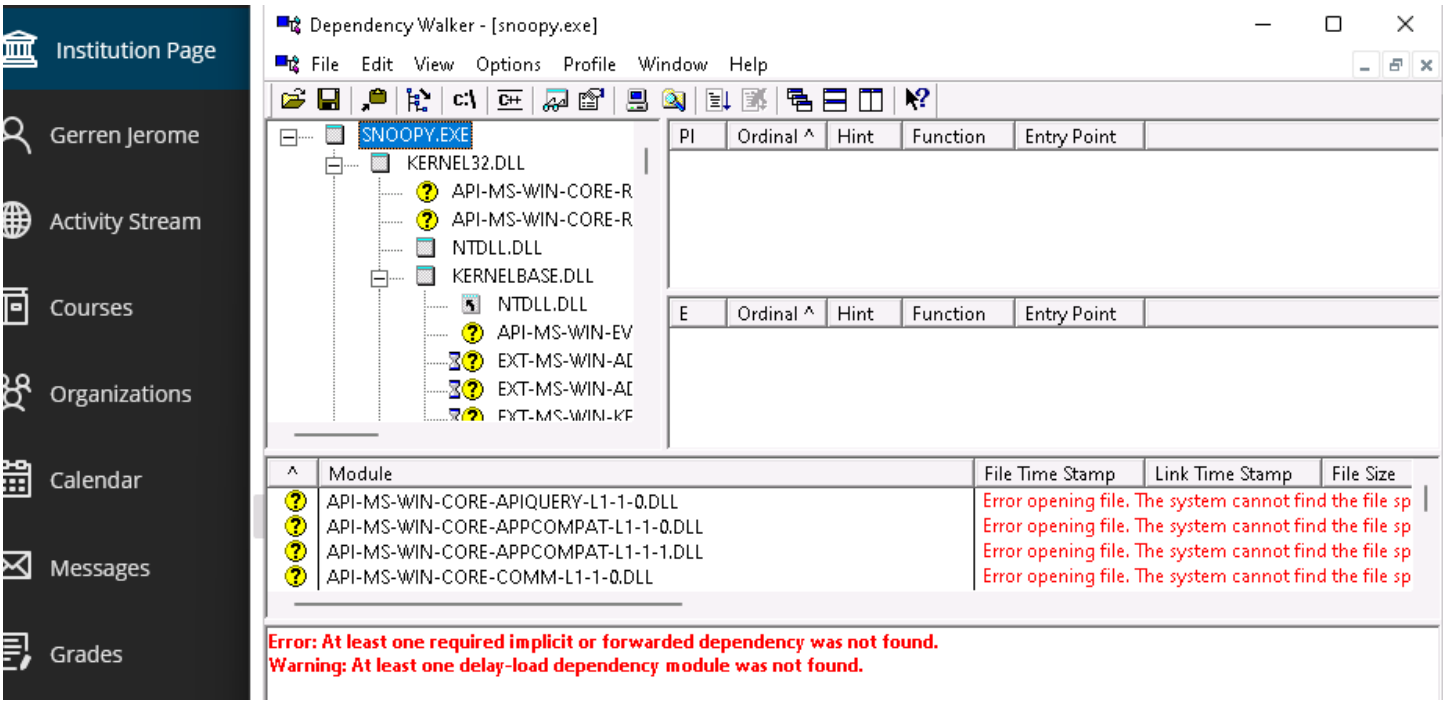


Gerren Jerome - [Malware Threats]

Hex viewer before closing.

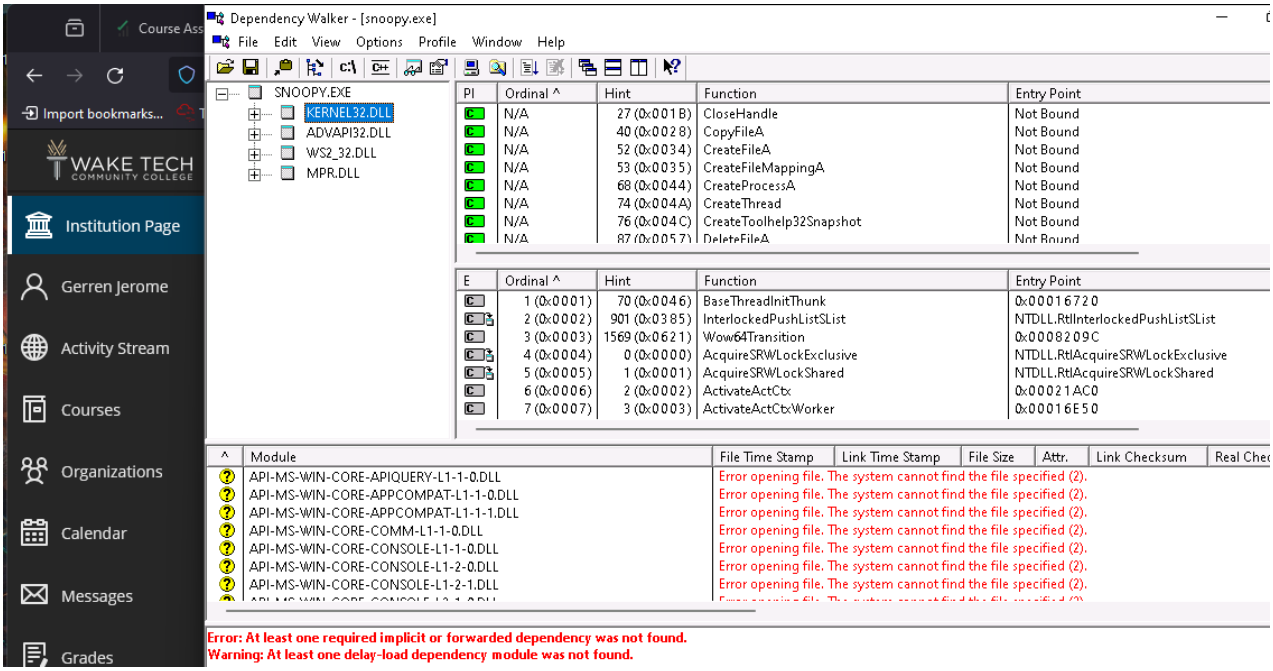
Identify file dependencies using Dependency Walker

Confirm import (Snoopy.exe) in DW



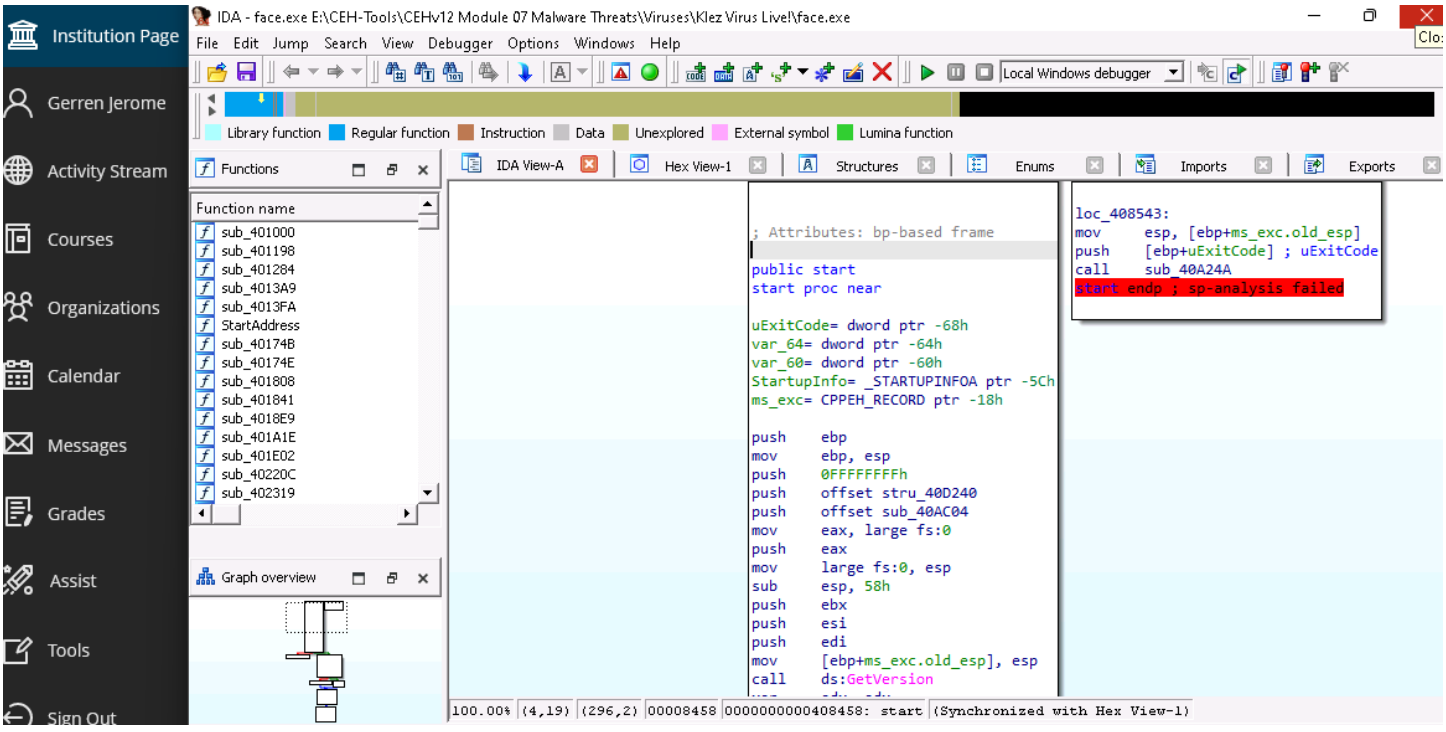
Gerren Jerome - Malware Threats

Display DLL details in DW for KERNEL32.dll



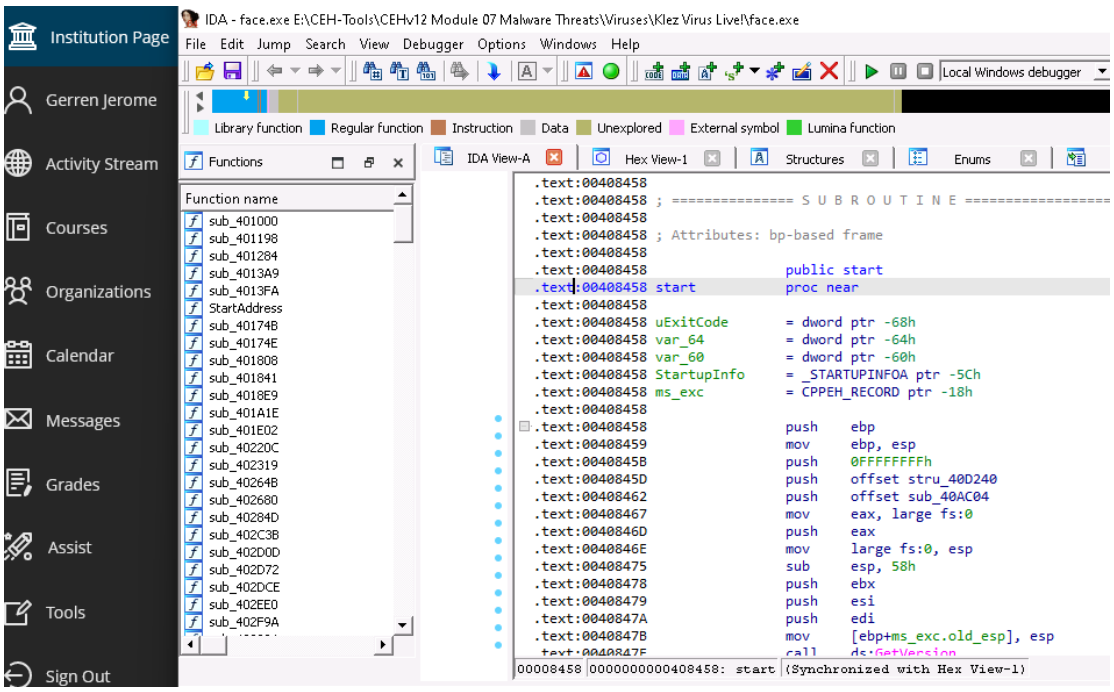
Perform malware disassembly using IDA and OllyDbg

Results of analysis (face.exe) in IDA

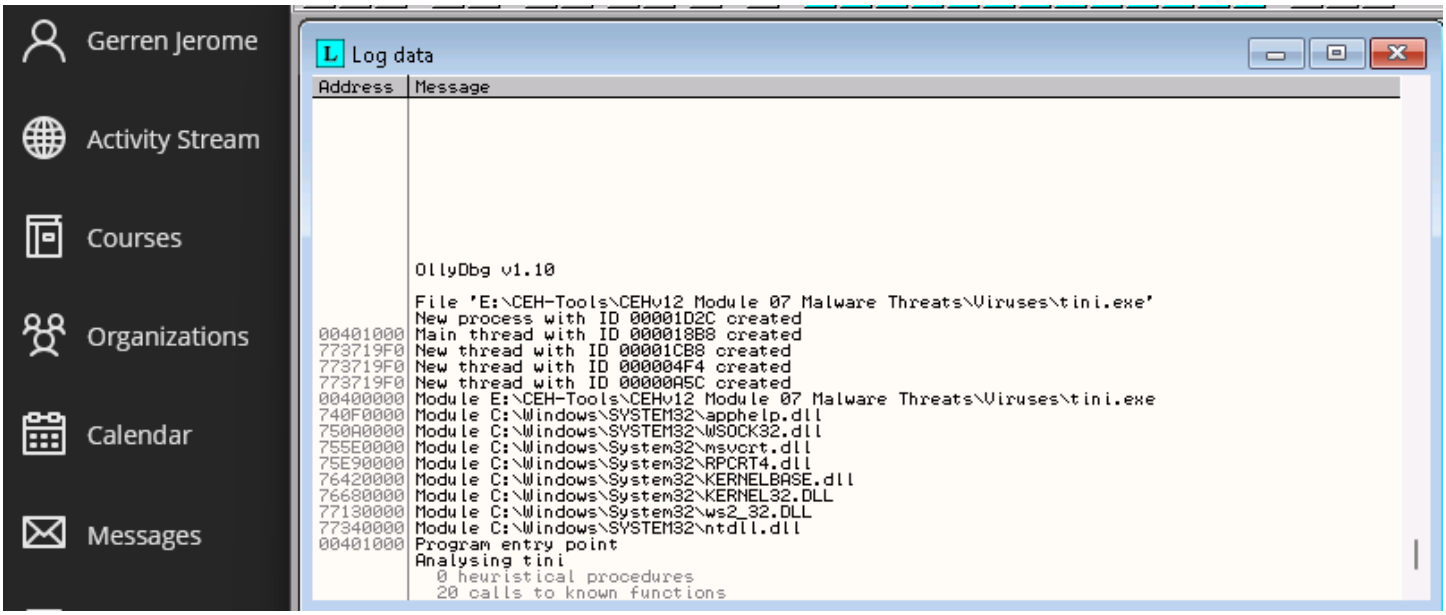


Gerren Jerome - Malware Threats

Text view of face.exe in IDA

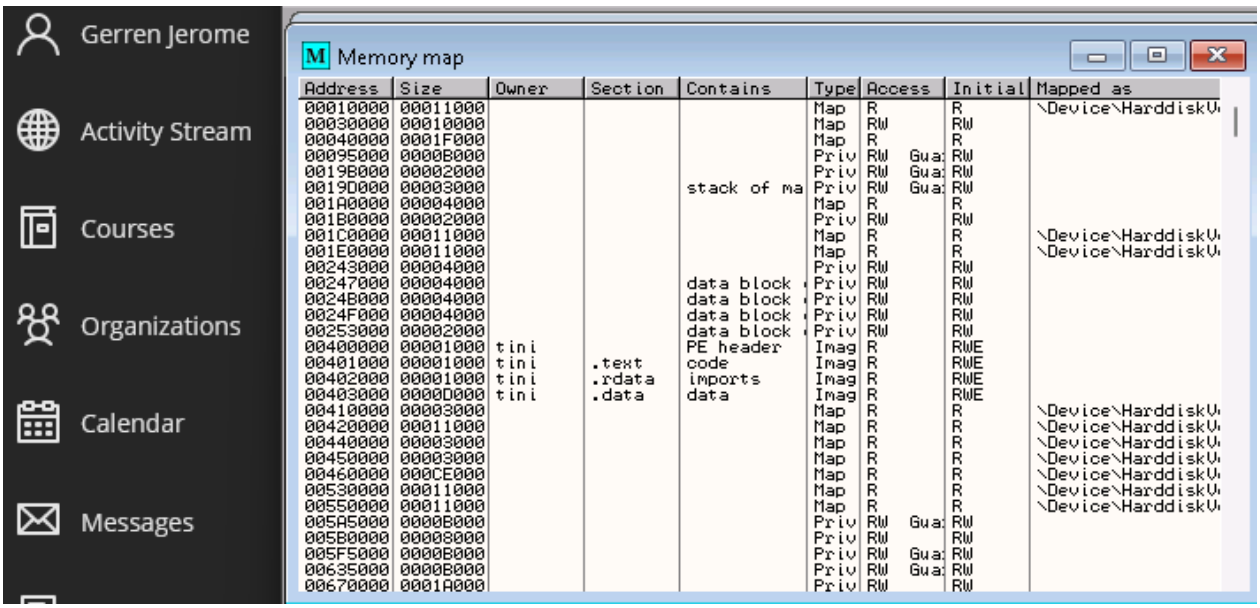


view log data of tini.exe in OllyDBG



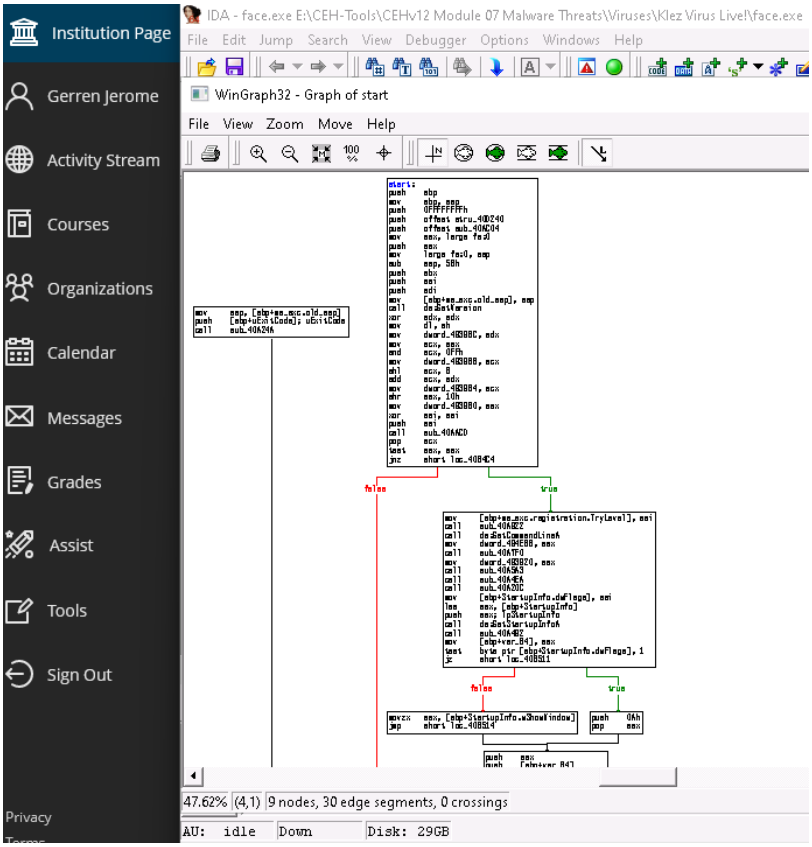
Gerren Jerome - [Malware Threats]

Memory map in OllyDBG



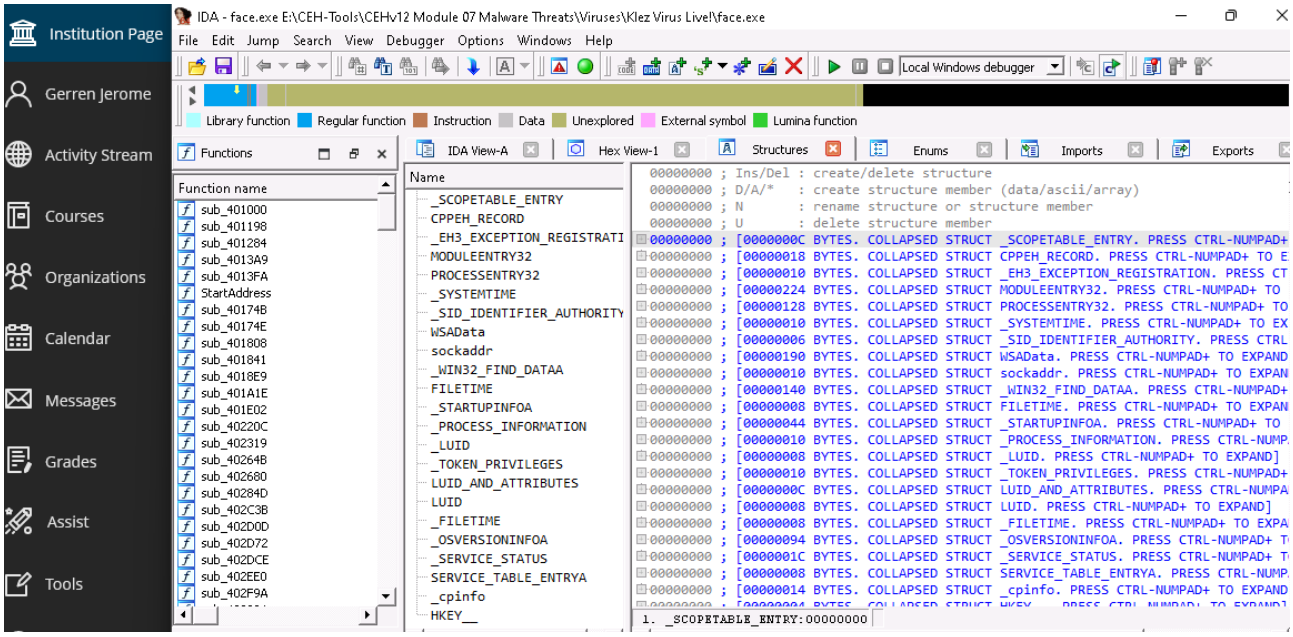
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00011000				Map	R	R	\Device\HarddiskV
00030000	00010000				Map	RW	RW	
00040000	0001F000				Map	R	R	
00095000	0000B000				Priv	RW Gua	RW	
0019B000	00002000				Priv	RW Gua	RW	
0019D000	00003000			stack of ma	Priv	RW Gua	RW	
001A0000	00004000				Map	R	R	
001B0000	00002000				Priv	RW	RW	
001C0000	00011000				Map	R	R	\Device\HarddiskV
001E0000	00011000				Map	R	R	\Device\HarddiskV
00243000	00004000				Priv	RW	RW	
00247000	00004000			data block	Priv	RW	RW	
0024B000	00004000			data block	Priv	RW	RW	
0024F000	00004000			data block	Priv	RW	RW	
00253000	00002000			data block	Priv	RW	RW	
00400000	00001000	tini		PE header	Imag	R	RWE	
00401000	00001000	tini	.text	code	Imag	R	RWE	
00402000	00001000	tini	.rdata	imports	Imag	R	RWE	
00403000	0000D000	tini	.data	data	Imag	R	RWE	
00410000	00003000				Map	R	R	\Device\HarddiskV
00420000	00011000				Map	R	R	\Device\HarddiskV
00440000	00003000				Map	R	R	\Device\HarddiskV
00450000	00003000				Map	R	R	\Device\HarddiskV
00460000	000CE000				Map	R	R	\Device\HarddiskV
00530000	00011000				Map	R	R	\Device\HarddiskV
00550000	00011000				Map	R	R	\Device\HarddiskV
005A5000	0000B000				Priv	RW Gua	RW	
005B0000	00008000				Priv	RW	RW	
005F5000	0000B000				Priv	RW Gua	RW	
00635000	0000B000				Priv	RW Gua	RW	
00670000	0001A000				Priv	RW	RW	

Graph view in IDA.



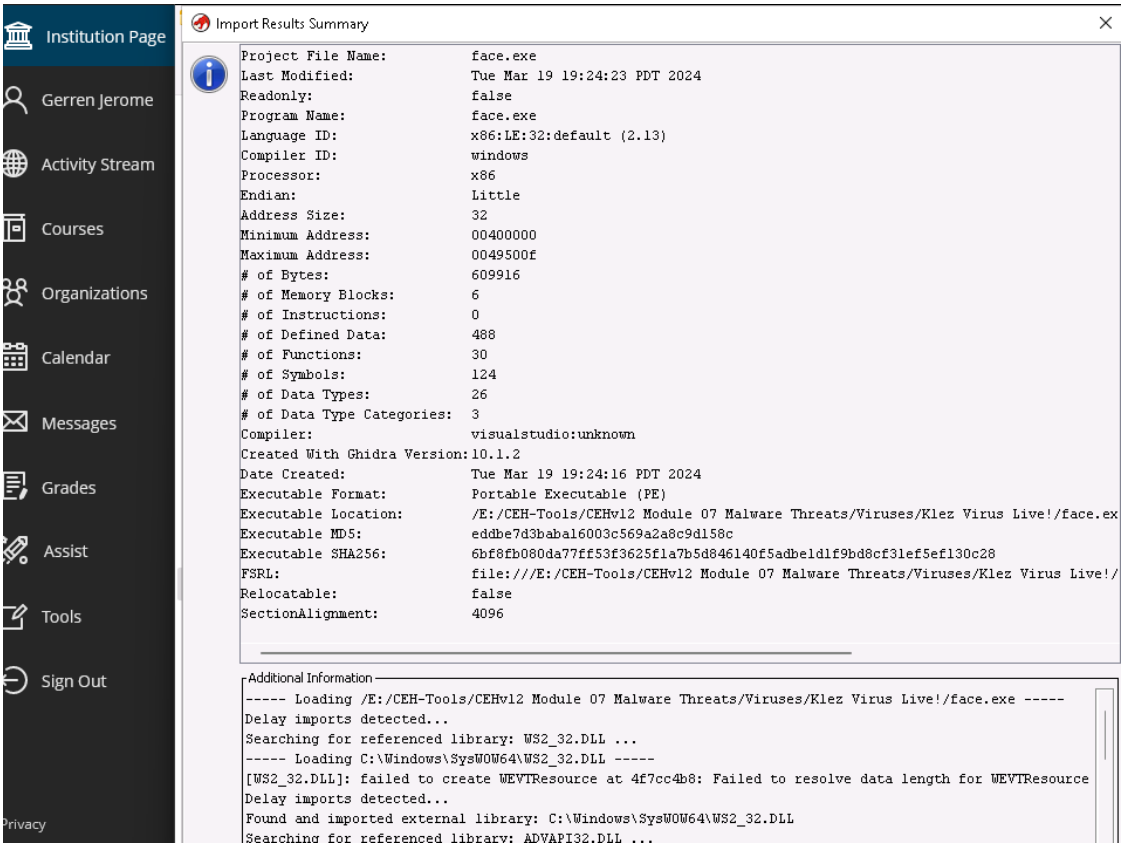
Gerren Jerome - Malware Threats

Structures view in IDA



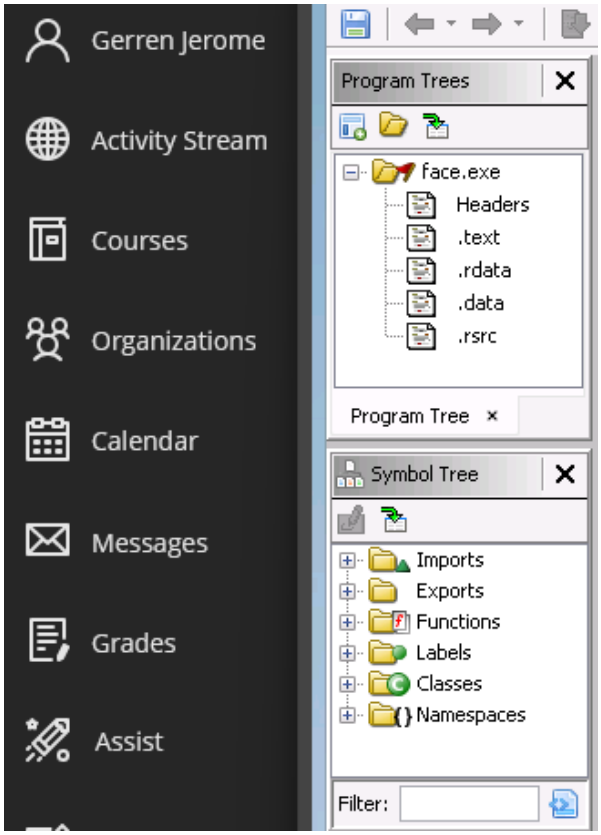
Perform malware disassembly using Ghidra.

Import Results Summary window in Ghidra.

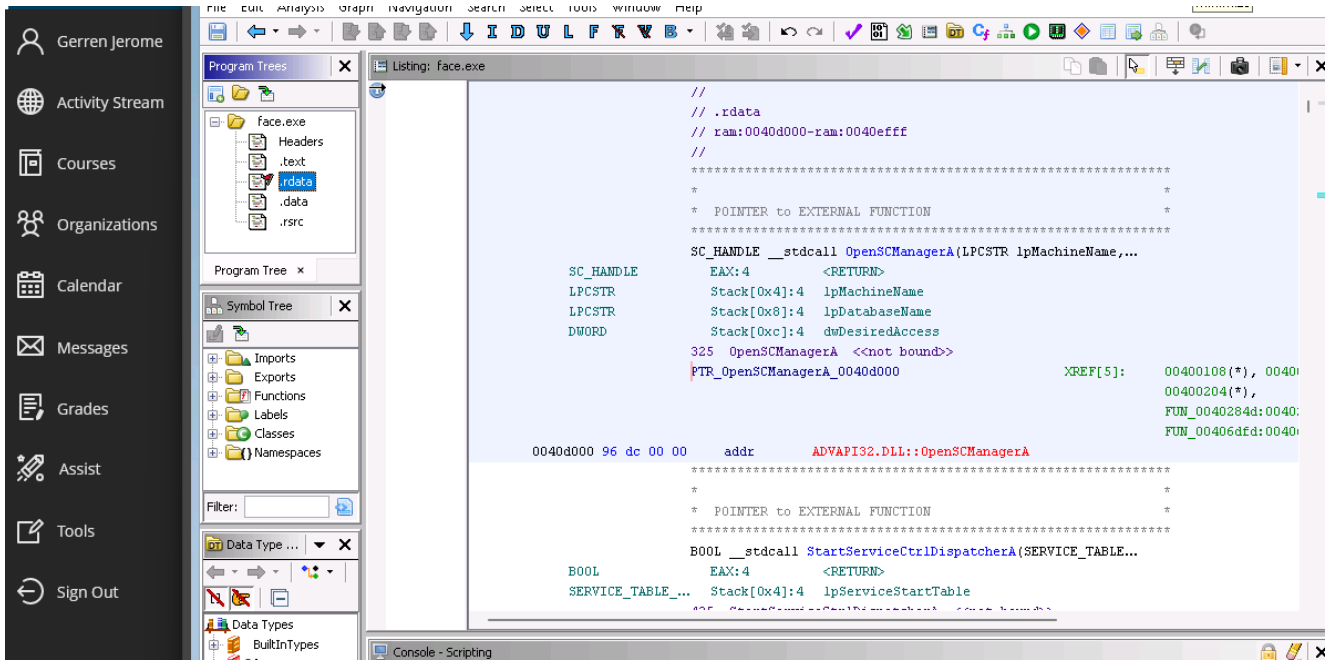


Gerren Jerome - [Malware Threats]

Symbol tree for face.exe in Ghidra



.rdata node for face.exe in Ghidra

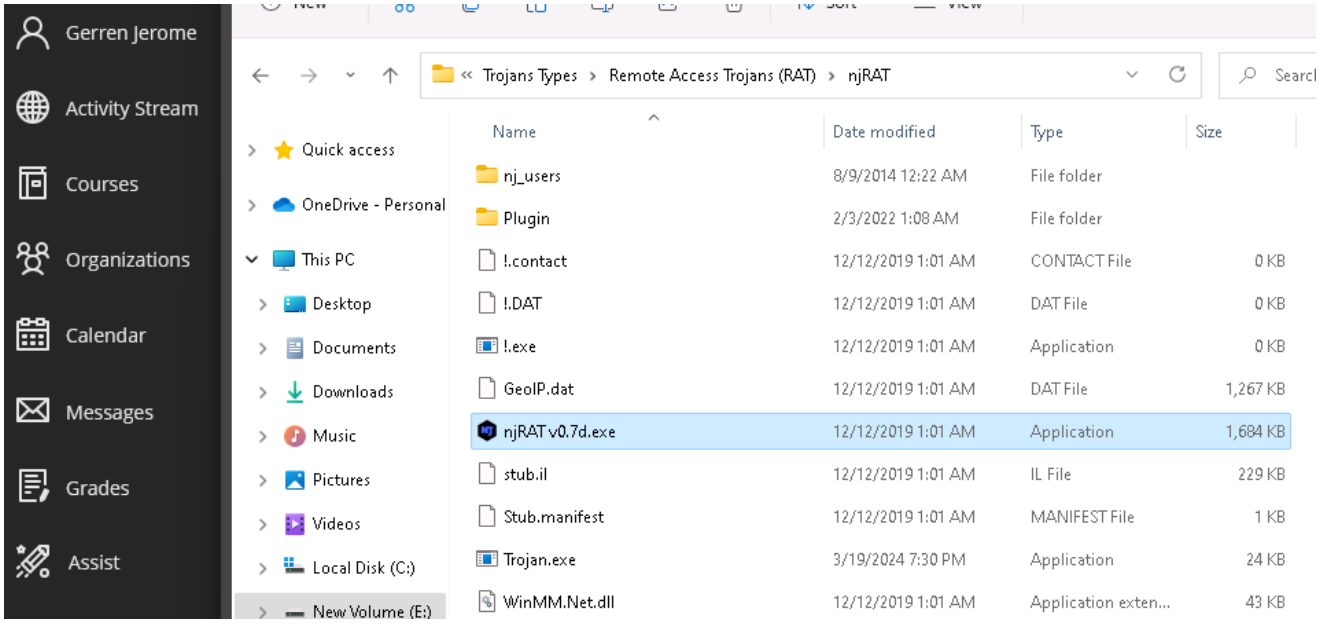


Gerren Jerome - [Malware Threats]

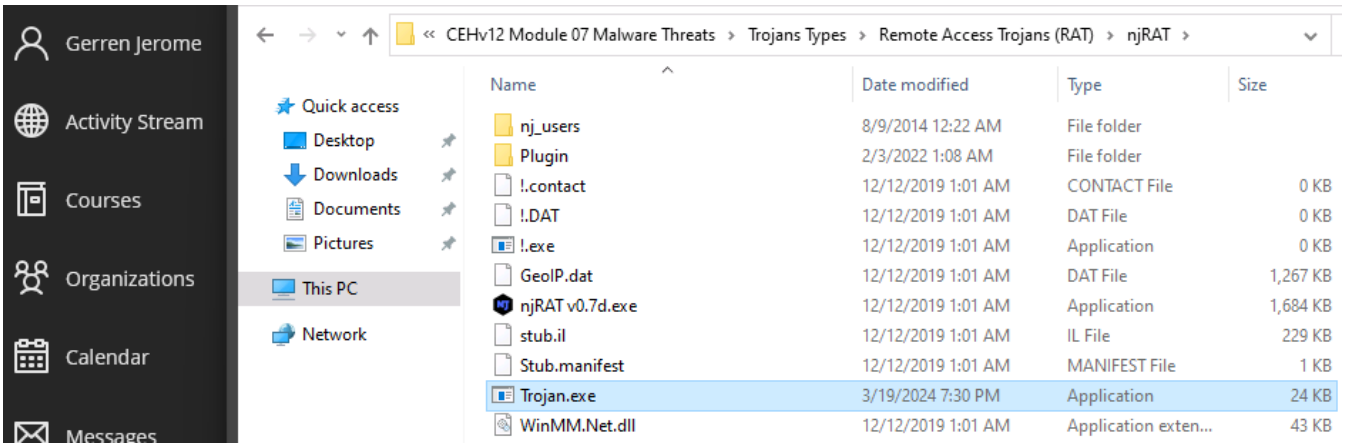
Perform dynamic malware analysis.

Perform port monitoring using TCPView and CurrPorts

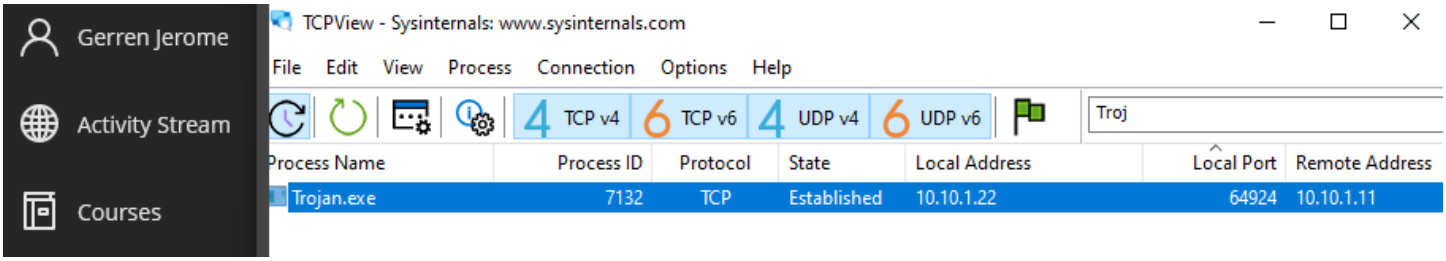
confirm creation of Trojan.exe in CEH-Tools with njRAT



launch Trojan.exe on WIN_SVR_22

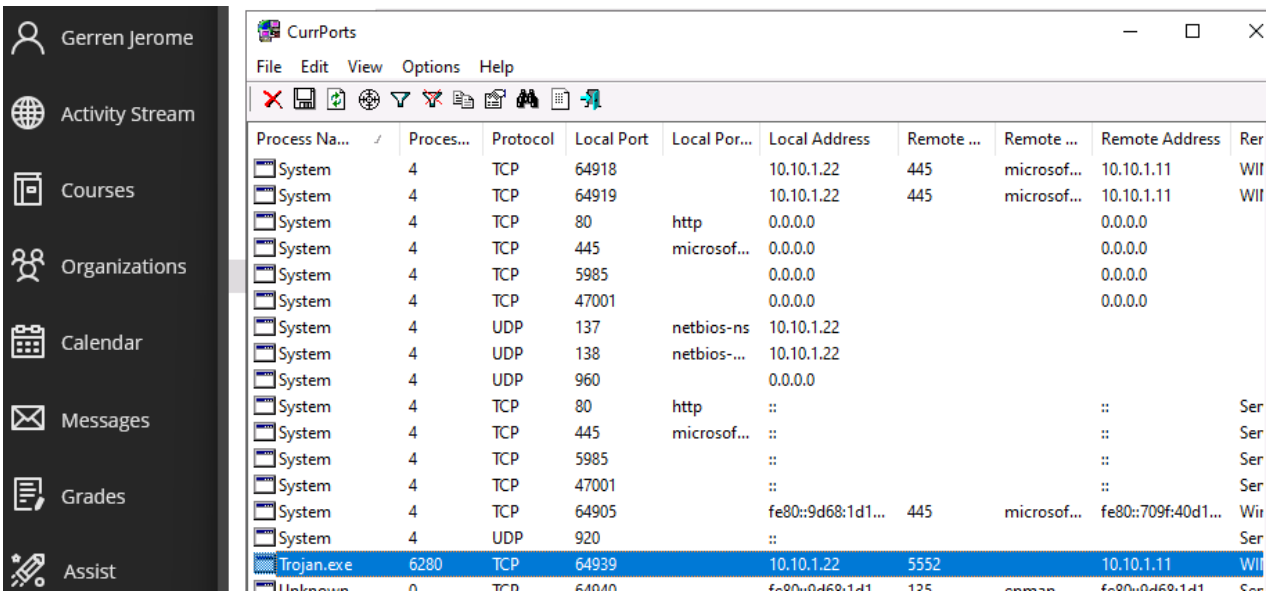


filter TCPview scan results to find Trojan.exe

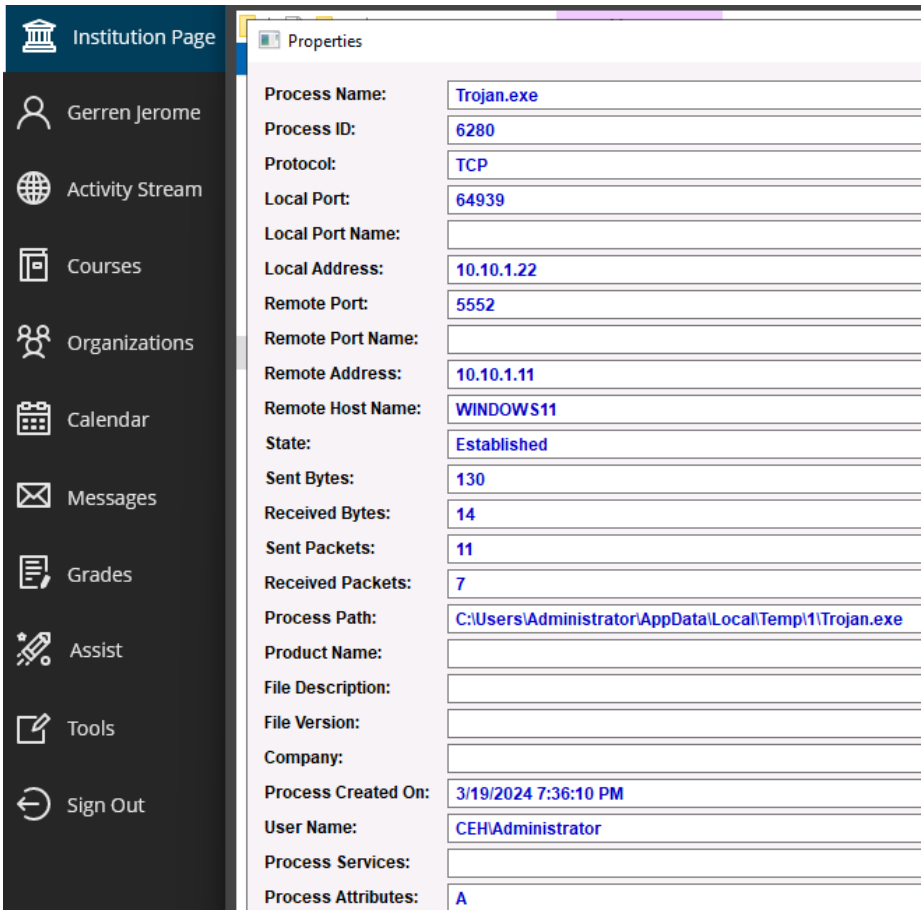


Gerren Jerome - Malware Threats

filter scan results in CurrPorts to find Trojan.exe.



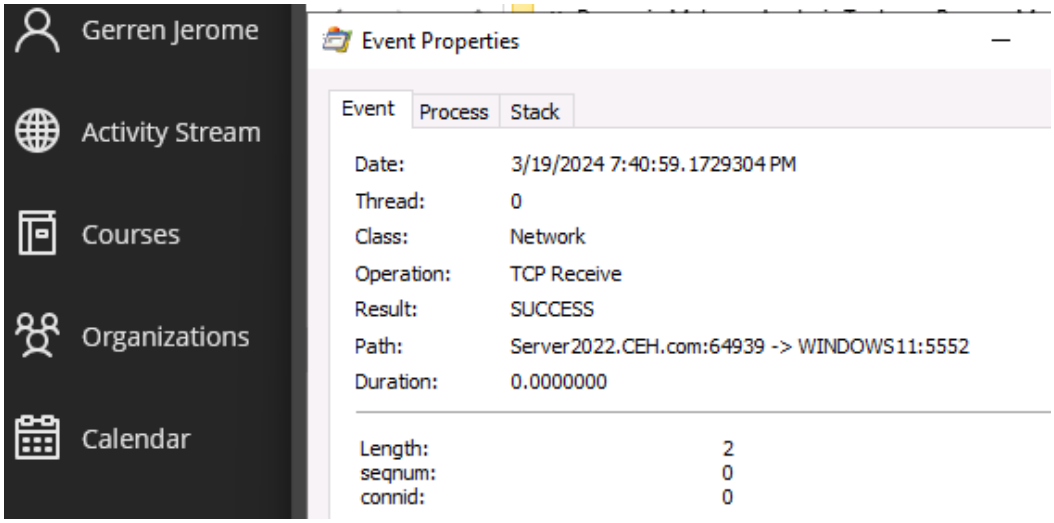
Examine Trojan.exe's Properties (didn't kill process yet)



Gerren Jerome - Malware Threats

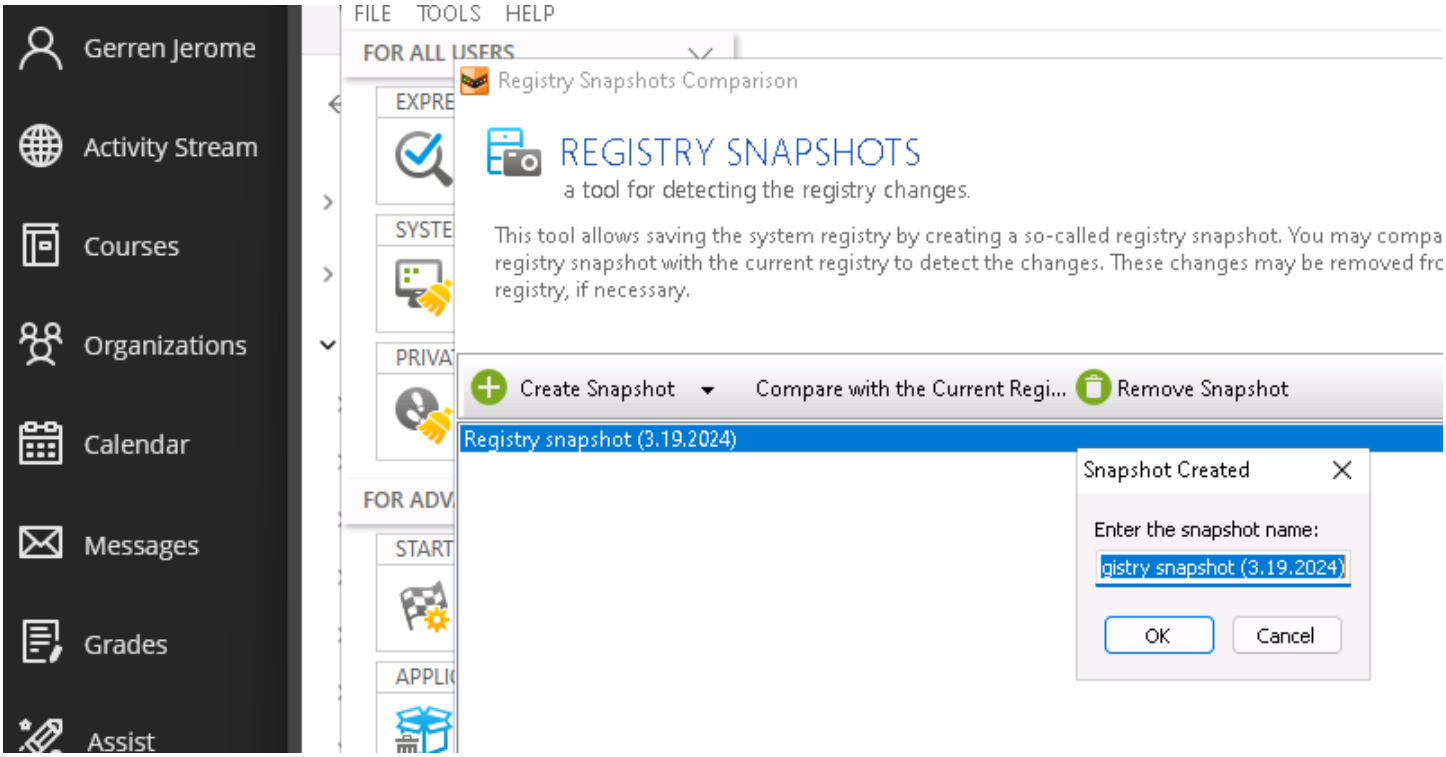
Perform process monitoring using Process Monitor

Identify properties of Trojan.exe from 4a in Process Monitor



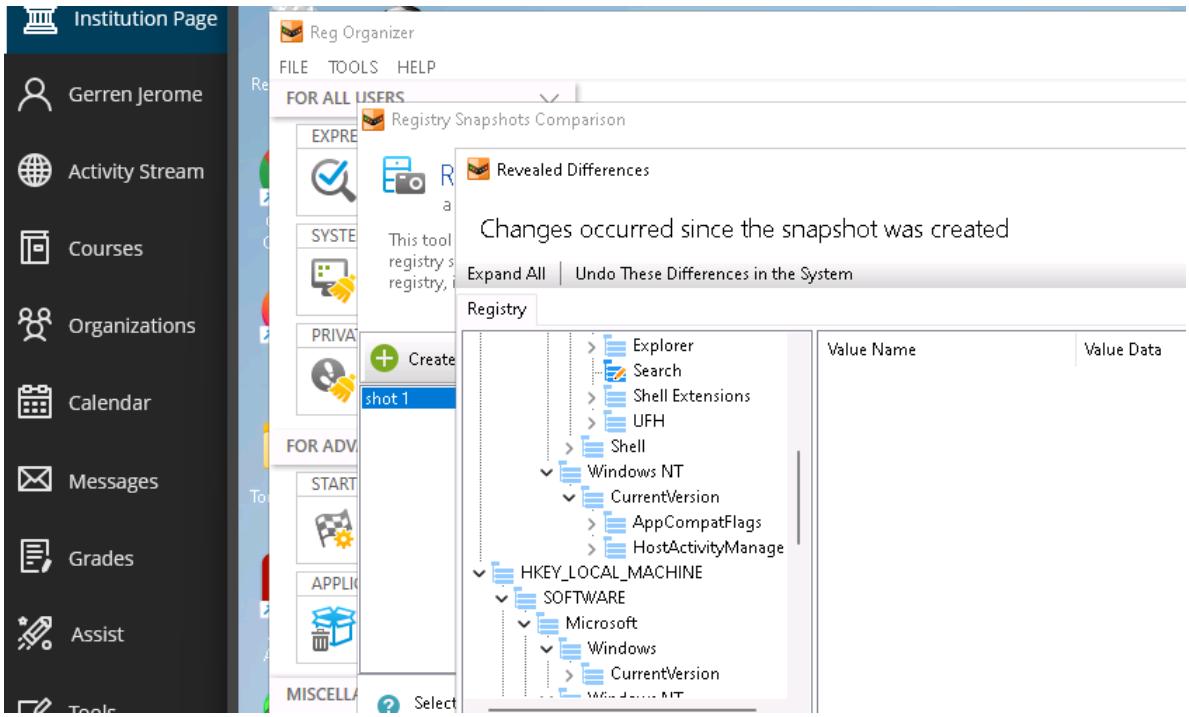
Perform registry monitoring using Reg Organizer

Create snapshot in Reg Organizer



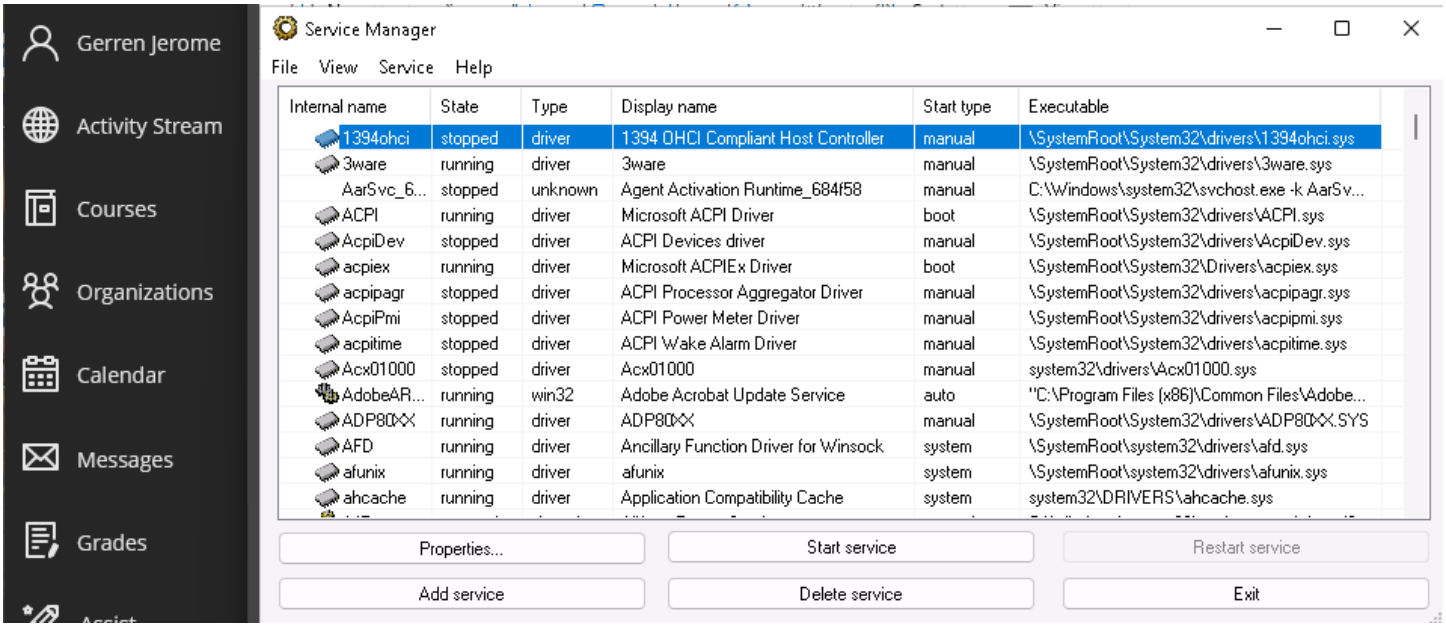
Gerren Jerome - [Malware Threats]

Identify changes in Registry post-install of SoftPerfect Network Scanner



Perform Windows services monitoring using Windows Service Manager (SrvMan) *(1 task)*

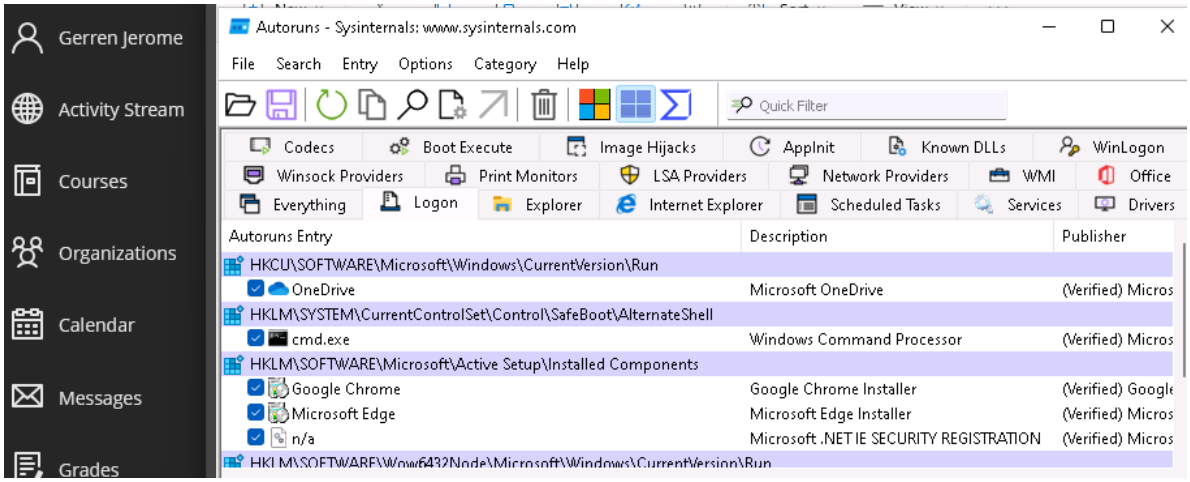
Service Manager main window.



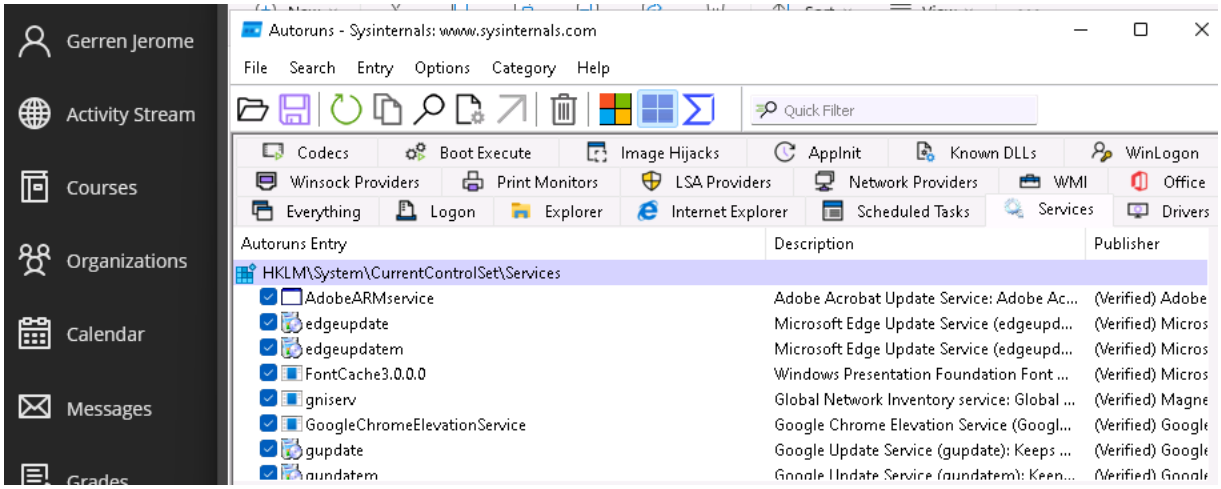
Gerren Jerome - Malware Threats

Perform startup program monitoring using Autoruns for Windows and WinPatrol

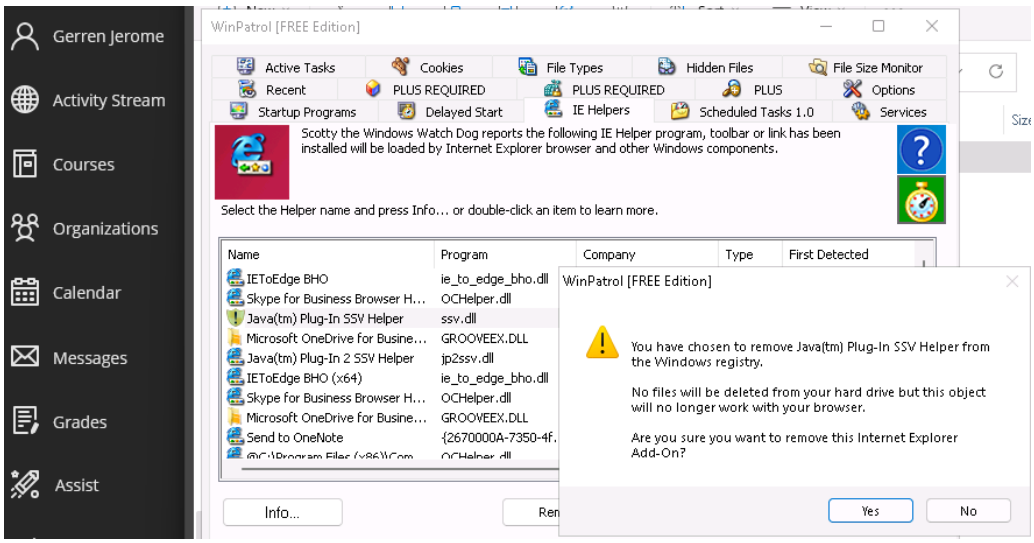
Identify login processes in Autoruns.



Identify services at startup in Autoruns.



View IE Helpers tab in WinPatrol

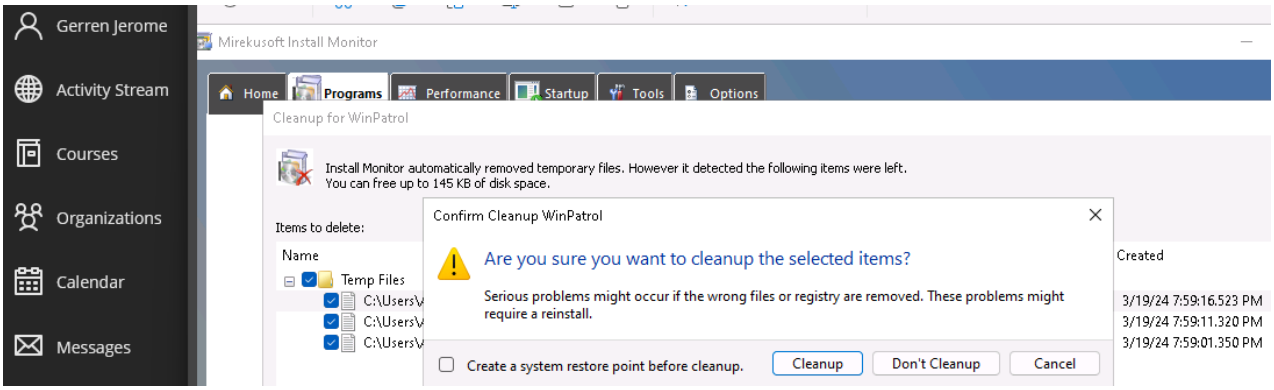


Gerren Jerome - [Malware Threats]

Show expanded view of Windows Batch File information.

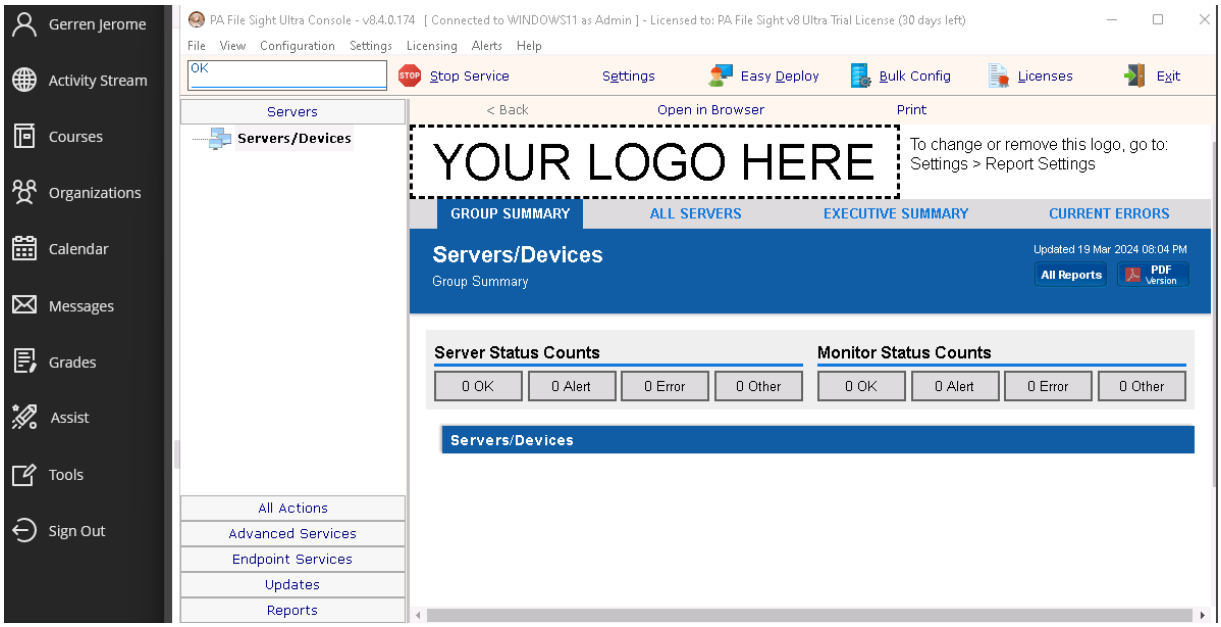
Perform installation monitoring using Mirekusoft Install Monitor

confirm cleanup of WinPatrol



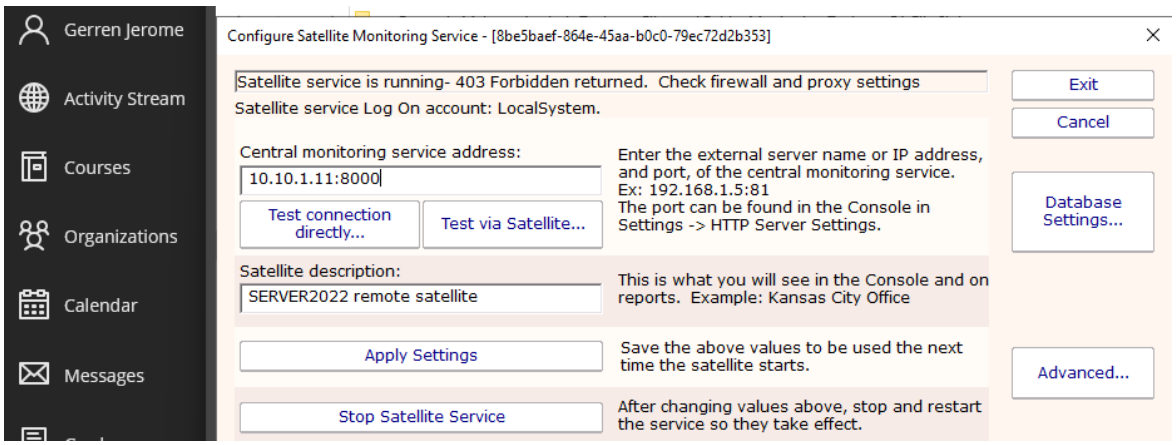
Perform files and folder monitoring using PA File Sight

Install and load up PA File Sight Ultra's console.

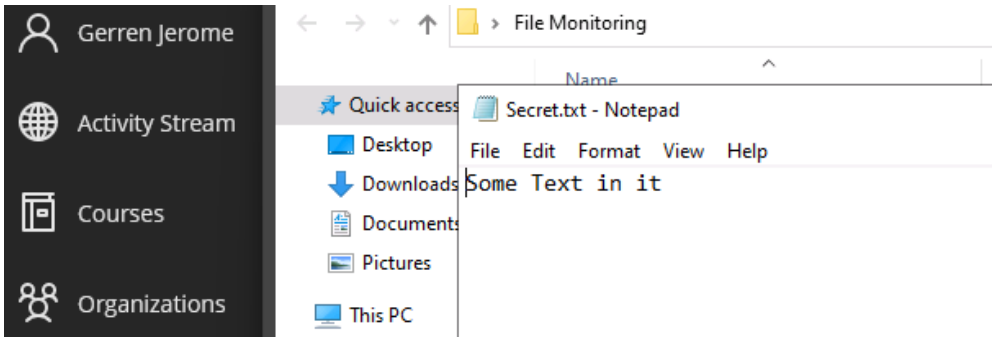


Gerren Jerome - [Malware Threats]

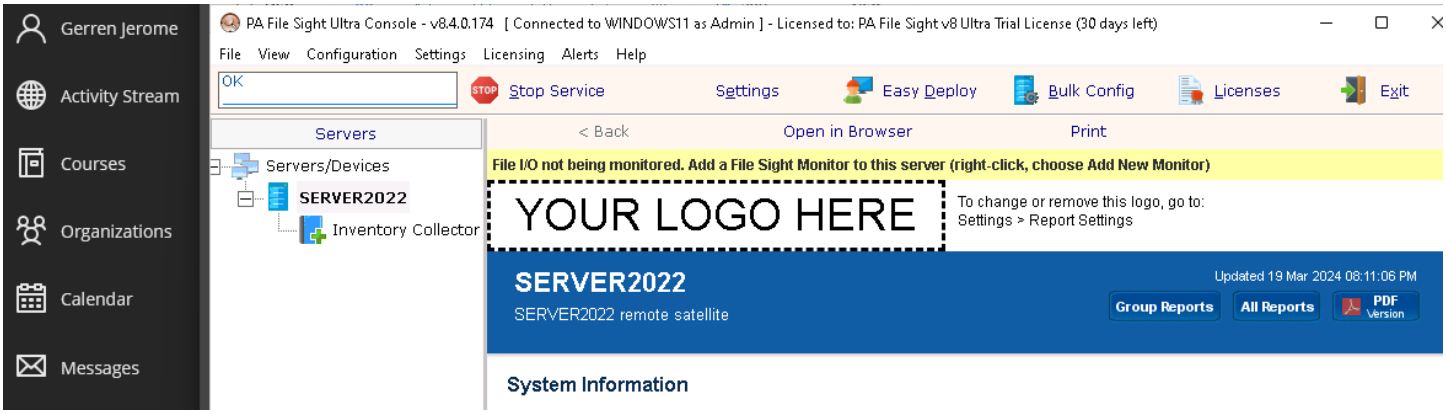
Configure satellite monitoring service.



i) Screengrab: Step 21 – Create secret.txt on WIN_SVR_22

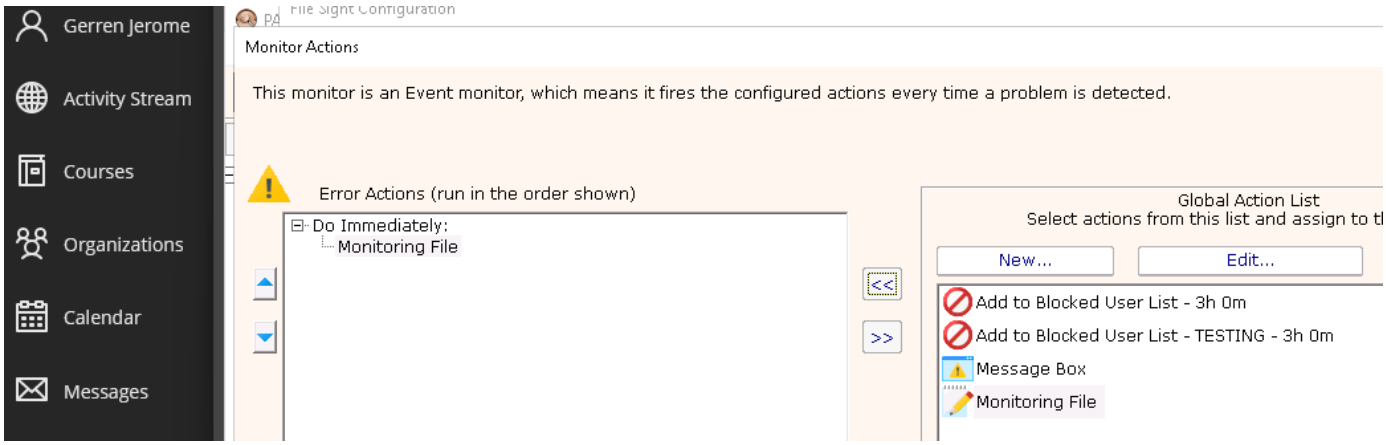


Confirm remote monitoring on Server2022.

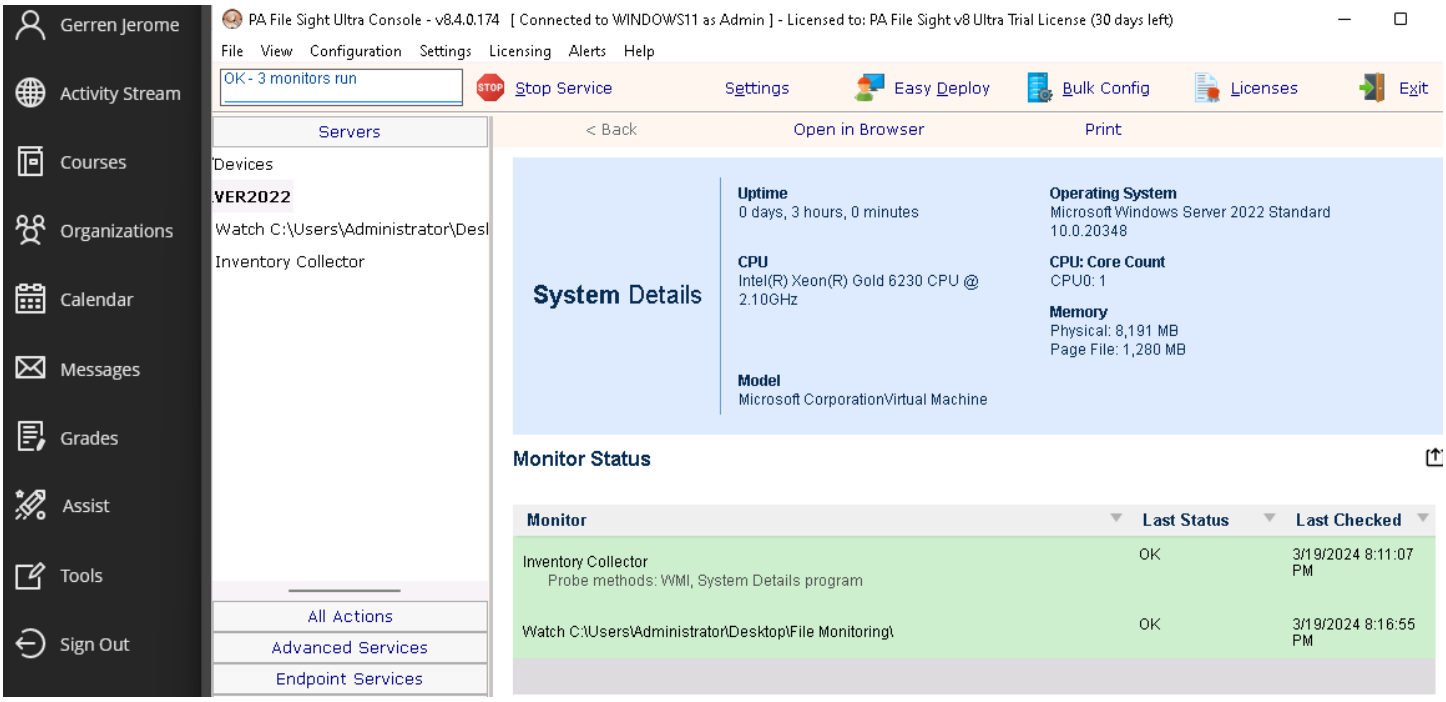


Gerren Jerome - [Malware Threats]

Create ruleset and instantiate Monitoring File action in Monitor Actions

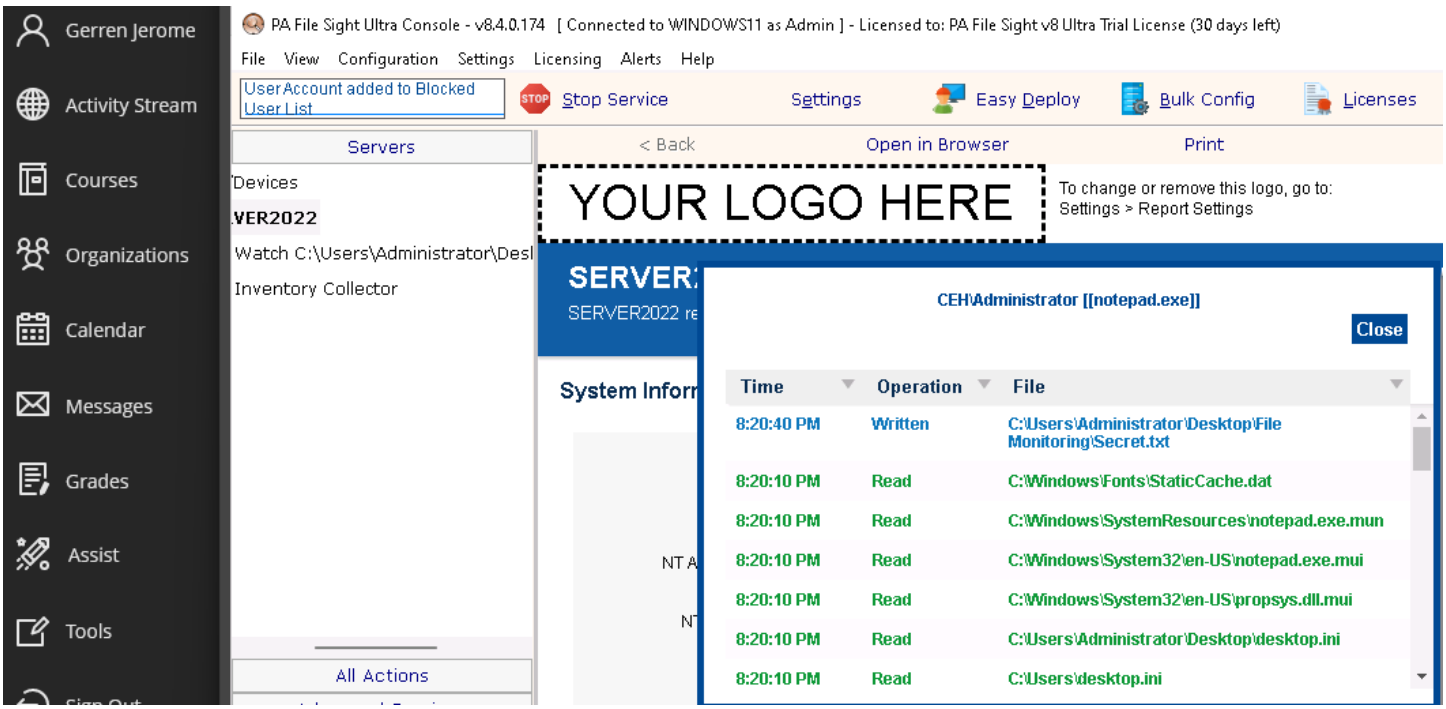


View Server2022 dashboard



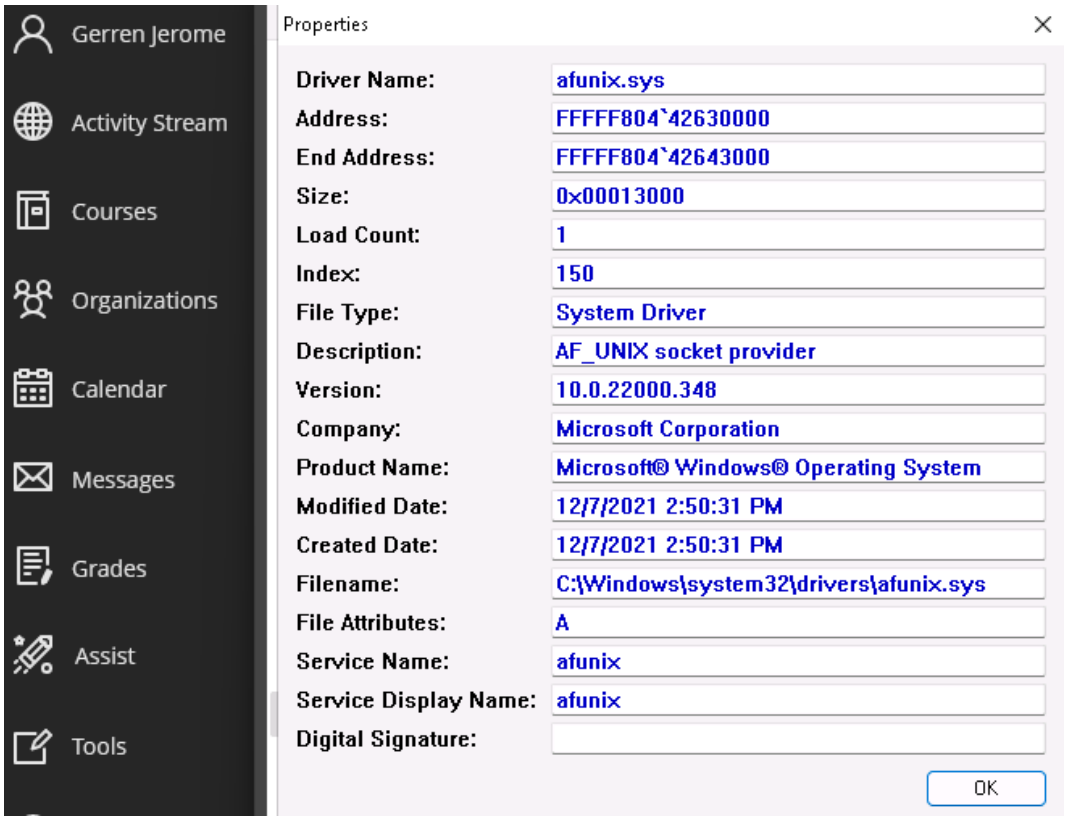
Gerren Jerome - [Malware Threats]

Confirm monitor is capturing correctly (activity in Secret.txt)



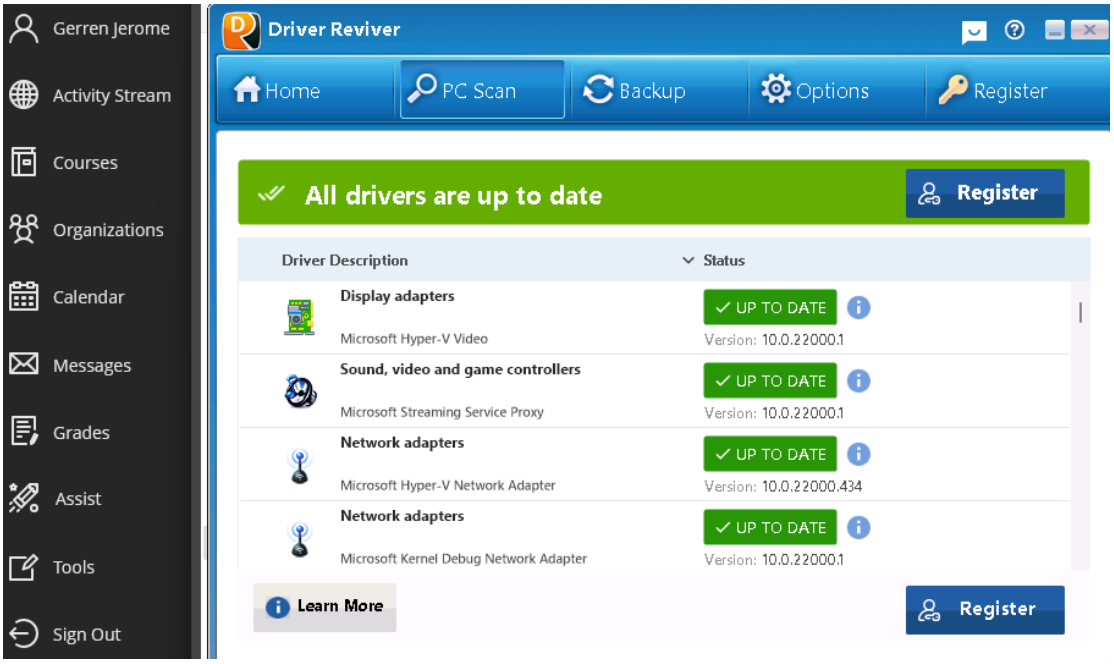
Perform device driver monitoring using DriverView and Driver Reviver

Display driver properties (not afunix.sys)



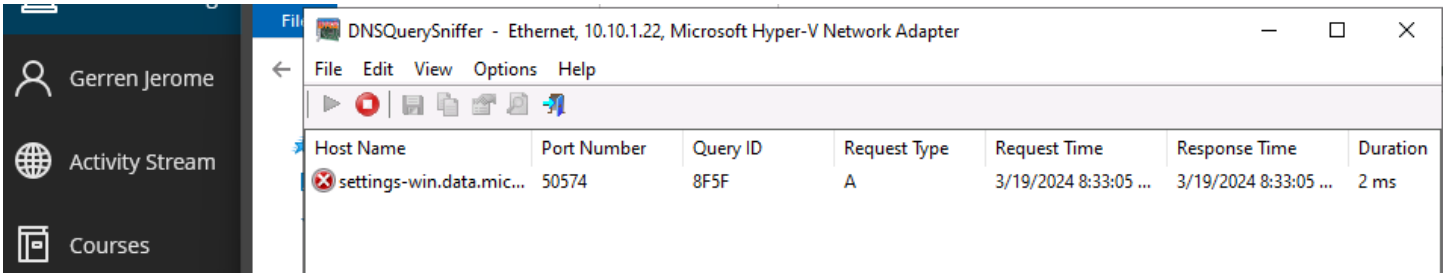
Gerren Jerome - [Malware Threats]

Status Driver Reviver scan



Perform DNS monitoring using DNSQuerySniffer.

Start sniffer.



Observe logged changes to DNS.

Gerren Jerome - Malware Threats

Reflection

This project provided hands-on experience with various malware analysis and enumeration techniques, enhancing my understanding of how to effectively identify, create, and analyze malware, as well as gather critical information from a target network. These skills are essential for effective ethical hacking and penetration testing.

This project demonstrates my ability to conduct comprehensive malware analysis and enumeration, showcasing my proficiency in using a wide range of tools and techniques to ensure network security.