

MODULE 07 MALWARE THREATS LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/c5699a05-cc67-4ba0-8441-edf432095d14>
2. <https://labclient.labondemand.com/LabClient/e28ea8b4-c5d5-4d9f-a90b-c4041eec3fce>

Username on EC-Council System

1. 1. 2110886@uj.edu.sa

↓


☒ 6  Malware Threats (Expected Duration 2 hours, 55 minutes) Details ▾ ⓘ
CEHV12, Module 07

Required: Yes
Status: Complete
Started: 01/م 03:03 1445/رمضان (Arab Standard Time)
Ended: 01/م 04:08 1445/رمضان (Arab Standard Time)

Launch

↓

↓

☒ 6  Malware Threats (Expected Duration 2 hours, 55 minutes) Details ▾ ⓘ
CEHV12, Module 07

Required: Yes
Status: Running
Started: 01/م 03:03 1445/رمضان (Arab Standard Time)
Ended: 01/م 04:08 1445/رمضان (Arab Standard Time)

Launch Cancel

↓

Lab 01:

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

1. Launch njRAT GUI:
2. Navigate to the location of njRAT v0.7d.exe.
3. Double-click to launch the njRAT GUI.
4. Configure Server Settings:
5. Specify the port number for communication with the victim machine.
6. Click "Start" to initiate the server.
7. Build the Server:
8. Click on the "Builder" link.
9. Enter the IP address of the attacker machine in the Host field.
10. Check the "Registry Startup" option.
11. Click "Build" and save the server executable.
12. Transfer Server to Victim:
13. Share the server executable with the victim machine through email or network shares.
14. Execute Server on Victim Machine:
15. On the victim machine, run the server executable.
16. The server establishes a connection with the attacker machine.
17. Establish Remote Control:
18. In the njRAT GUI, observe the connection with the victim machine.
19. Perform remote actions like file management and process manipulation.

What I Learned:

- Explored how Remote Access Trojans (RATs) enable attackers to gain unauthorized access to victim machines.
- Understood the importance of securing systems against phishing attacks and drive-by downloads.
- Recognized the risks associated with granting administrative access to malicious actors.
- Learned to identify suspicious behavior indicative of a compromised system.

Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

1. Upload Trojan to VirusTotal:
2. Navigate to VirusTotal website.
3. Upload the Trojan executable for analysis.
4. Run SwayzCryptor:
5. Launch SwayzCryptor application.
6. Select Trojan File:
7. Choose the Trojan executable file for encryption.
8. Configure Crypter Settings:
9. Enable options like "Start up," "Mutex," and "Disable UAC."
10. Click "Encrypt" to cryptographically encrypt the file.
11. Save Encrypted File:
12. Specify the destination to save the encrypted file.
13. Upload Encrypted File to VirusTotal:
14. Upload the encrypted file to VirusTotal for analysis.

15. Test Undetectable Trojan:
16. Transfer the encrypted file to the victim machine.
17. Execute the file on the victim machine and observe detection results.

What I Learned:

- Discovered techniques used by attackers to evade detection by antivirus software.
- Explored the concept of crypting malware to obfuscate its malicious intent.
- Understood the limitations of antivirus software and the need for continuous updates to detection mechanisms.
- Gained insight into the effectiveness of crypters in bypassing antivirus detection.

Task 3: Create a Trojan Server using Theef RAT Trojan

1. Run Theef Server:
2. Execute the Theef server executable on the victim machine.
3. Establish Connection from Attacker Machine:
4. Launch Theef client on the attacker machine.
5. Enter the IP address of the victim machine and default port number.
6. Remote Operations:
7. Access victim machine details using Computer Information.
8. Perform actions like screen capture, keylogging, and process management.
9. Explore Additional Features:
10. Utilize features like Remote Desktop and Remote Cam/Microphone.
11. Terminate Connection:
12. Close all open connections and windows.

What I Learned:

- Explored the capabilities of Remote Access Trojans (RATs) in compromising victim systems.
- Understood the risks associated with executing unknown executable files on a system.
- Recognized the importance of securing networked environments against unauthorized access.
- Learned techniques used by attackers to maintain persistence and control over compromised systems.

Lab 02:

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

1. Open the JPS Virus Maker tool by navigating to E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker and double-clicking jps.exe.
2. Tick the "Auto Startup" checkbox and select desired virus options such as disabling TaskManager, Windows Update, Control Panel, Drives, hiding Windows Clock and Desktop Icons, enabling Remote Desktop, removing Bluetooth, turning off Windows Firewall and Defender, and setting auto startup.
3. Specify additional settings like changing Windows password, computer name, and icon.
4. Choose the architecture (x86 or x64) and click "Create Virus!".
5. Confirm the successful creation of the virus named "Server.exe" in the specified location.
6. Transfer the virus file to the victim machine through email, chat, mapped network drive, or other means.
7. On the victim machine (Windows Server 2019), navigate to Z:\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker and execute the Server.exe file.
8. Observe the system's response indicating successful infection, such as a blank desktop screen.
9. Restart the machine and attempt to log in with the provided password set during virus creation.
10. Experience limitations imposed by the virus, such as errors when trying to open applications like Task Manager.
11. Conclude the task by ending the lab and relaunching it to reset the infected machines.

What I Learned:

- Explored the functionality of the JPS Virus Maker tool in creating custom viruses.
- Learned about various options available for virus creation, including system modifications and auto-startup features.
- Understood the implications of virus infections on system functionality and security.
- Experienced firsthand the impact of malicious software on system integrity and user accessibility.

Lab 03:

Task 1: Perform Malware Scanning using Hybrid Analysis

1. Open the Windows 11 virtual machine and log in.
2. Allow the PC to be discoverable by other devices on the network.
3. Open Google Chrome and navigate to <https://www.hybrid-analysis.com>.
4. Accept any cookie notifications.
5. Drag and drop the suspicious file (tini.exe) for analysis.
6. Enter your email and a comment, then consent to the terms and conditions.
7. Select the analysis environment (Windows 7 64 bit) and generate a public report.
8. Review the analysis results, including anti-virus scans from various sources.
9. Explore detailed reports from VirusTotal.
10. Close all open windows.

What I Learn:

- How to use Hybrid Analysis for malware scanning.
- Understanding the importance of analyzing suspicious files.
- Interpreting analysis reports and anti-virus results.

Task 2: Perform a Strings Search using BinText

1. Open BinText and browse for the malicious file (face.exe).
2. Initiate the scan to extract text from the file.
3. Review the extracted strings and their types (ANSI, Unicode, Resource).
4. Analyze the extracted strings for potential insights.
5. Close all open windows.

What I Learn:

- How to use BinText for extracting text from files.
- Identifying different string types and their significance.
- Analyzing extracted strings for potential insights.

Task 3: Identify Packaging and Obfuscation Methods using PEId

1. Open PEId and browse for the malicious file (face.exe).
2. Analyze the identified signatures associated with packers and compilers.
3. Review the information provided by PEId.
4. Close all open windows.

What I Learn:

- Using PEId to detect packing and obfuscation methods.
- Understanding different signatures associated with packers and compilers.

Task 4: Analyze ELF Executable File using Detect It Easy (DIE)

1. Open Detect It Easy (DIE) and browse for the ELF file (ELF Test File).
2. Review the analysis results, including operating system and compiler details.
3. Explore additional information such as file hashes and entropy.
4. Close all open windows.

What I Learn:

- Using Detect It Easy (DIE) to analyze ELF executable files.
- Understanding file details and attributes provided by the tool.

Task 5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

1. Install PE Explorer and open the application.

2. Open the malicious file (face.exe) using PE Explorer.
3. Explore PE headers, data directories, and section headers.
4. Analyze file structures, hashes, and entropy.
5. Close all open windows.

What I Learn:

- How to use PE Explorer to view PE information of executable files.
- Understanding PE headers, sections, and data directories.

Task 6: Identify File Dependencies using Dependency Walker

1. Open Dependency Walker and import the malicious file (snoopy.exe).
2. Analyze the dependencies and linked libraries.
3. Explore detailed information about DLL dependencies.
4. Close all open windows.

What I Learn:

- Using Dependency Walker to identify file dependencies.
- Understanding the importance of library functions and dependencies.

Task 7: Perform Malware Disassembly using IDA and OllyDbg

Steps for IDA:

1. Open IDA and create a new project.
2. Import the malicious file (face.exe) for disassembly.
3. Analyze the disassembled code and explore various functionalities.
4. Close all open windows.

Steps for OllyDbg:

1. Open OllyDbg and load the malicious file (tini.exe).
2. Analyze threads, memory mappings, and executable modules.
3. Review log data and thread information.
4. Close all open windows.

What I Learn:

- Disassembling and analyzing malware using IDA and OllyDbg.
- Exploring disassembled code and identifying potential threats.

Task 8: Perform Malware Disassembly using Ghidra

1. Open Ghidra and create a new project.
2. Import the malicious file (face.exe) for analysis.
3. Analyze the disassembled code and explore symbols and components.
4. Close all open windows.

What I Learn:

- Using Ghidra for malware disassembly and analysis.
- Exploring symbols, headers, and components of disassembled code.

Lab4 :

Task 1: Perform Port Monitoring using TCPView and CurrPorts

1. Install and open TCPView and CurrPorts on your Windows machine.
2. Launch nJ RAT server and execute it from another machine.
3. Use TCPView and CurrPorts to monitor open ports and processes.
4. Identify suspicious processes associated with the server.
5. Analyze the details provided by TCPView and CurrPorts.
6. Close unwanted TCP connections or kill suspicious processes if necessary.

What I Learned:

- Understanding the importance of monitoring open ports for detecting malware.
- Installing and using port monitoring tools such as TCPView and CurrPorts.
- Identifying suspicious processes and connections on a Windows machine.
- Analyzing TCP and UDP endpoints to identify malicious activity.
- Taking action to close unwanted connections and terminate malicious processes.

Task 2: Perform Process Monitoring using Process Monitor

1. Install and open Process Monitor on your Windows machine.
2. Launch Process Monitor and agree to the License Agreement.
3. Explore the main window of Process Monitor to view real-time file system, Registry, process, and thread activity.
4. Look for the Trojan.exe process or any other suspicious processes.
5. Select the process and view its properties and event details.
6. Analyze the event properties, process details, and thread stacks to understand the nature of the process.
7. Close Process Monitor after completing the analysis.
8. Take necessary actions based on the findings, such as terminating suspicious processes or investigating further.

What I Learned:

- Understanding the importance of process monitoring for malware detection and analysis.
- Installing and using Process Monitor to monitor file system, Registry, process, and thread activity.
- Exploring process details, event properties, and thread stacks to analyze the behavior of suspicious processes.
- Learning to interpret information provided by Process Monitor to identify malicious activities.
- Taking appropriate actions based on the findings to mitigate security risks.

Task 3: Perform Registry Monitoring using Reg Organizer

1. Install and open Reg Organizer on your Windows machine.
2. Follow the installation wizard and agree to the License Agreement.
3. Create a registry snapshot using Reg Organizer.
4. Install any application to induce changes in the registry.
5. Compare the current registry snapshot with the previous one to identify changes.
6. Examine the registry entries and associated files to detect any unwanted modifications.
7. Take necessary actions to stop or delete suspicious registry entries manually.
8. Close Reg Organizer after completing the registry monitoring and analysis.

What I Learned:

- Understanding the significance of monitoring registry entries to detect malware and system changes.

- Installing and using Reg Organizer to track registry modifications.
- Creating and comparing registry snapshots to identify changes induced by installed applications or malware.
- Examining registry entries and associated files to understand their impact on system integrity.
- Taking proactive measures to stop or delete suspicious registry entries to maintain system security.

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

1. Install and open Windows Service Manager (SrvMan) on your Windows machine.
2. Explore the main window of Windows Service Manager to view all services available or running on the machine.
3. Identify any suspicious or unwanted services listed in the window.
4. Select a service and view its properties.
5. Take necessary actions such as stopping, deleting, or disabling suspicious services.
6. Monitor changes in services and scan for suspicious Windows services using SrvMan.
7. Close Windows Service Manager after completing the monitoring and management of services.

What I Learned:

- Understanding the importance of monitoring Windows services to detect malware and unauthorized activities.
- Installing and using Windows Service Manager (SrvMan) to track changes in services and scan for suspicious services.
- Exploring service properties and details to understand their functionality and impact on system security.
- Taking proactive measures to stop, delete, or disable suspicious services to mitigate security risks.
- Learning to monitor changes in services and maintain the integrity of the system configuration.

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

1. Install and open Autoruns for Windows and WinPatrol on your Windows machine.
2. Use Autoruns to view applications configured to run during system bootup.
3. Navigate through tabs like Logon, Explorer, Services, Drivers, and Known DLLs to inspect startup programs and associated details.
4. Identify any unwanted or suspicious programs set to start during bootup.
5. Disable or remove unwanted startup programs using Autoruns.
6. Switch to WinPatrol and explore tabs like Startup Programs, IE Helpers, Services, File Types, and Active Tasks.
7. Disable or remove unwanted startup programs, services, or tasks using WinPatrol.
8. Analyze the information provided by WinPatrol to understand the nature of startup programs and associated tasks.
9. Take necessary actions to manage and optimize startup programs for better system performance and security.
10. Close all open windows and applications after completing the monitoring and management of startup programs.

What I Learned:

- Understanding the significance of monitoring startup programs to detect malware.
- Utilizing tools like Autoruns for Windows and WinPatrol to inspect and manage startup programs.

- Exploring different tabs within Autoruns and WinPatrol to identify and disable unwanted startup items.
- Learning to interpret information provided by startup program monitoring tools to make informed decisions.
- Taking proactive measures to optimize system startup for improved performance and security.

Task 6: Perform Installation Monitoring using Mirekrosoft Install Monitor

1. Navigate to the directory: **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekrosoft Install Monitor.**
2. Double-click **SetupInstallMonitor.exe**.
3. If prompted, click the **Update** button and then click **Yes** if a User Account Control window appears.
4. Follow the installation steps.
5. Once installation is successful, click **Launch**.
6. In the Mirekrosoft Install Monitor main window, click **OK** on the Welcome pop-up and then click **Skip scan** in the Home tab.
7. Click the **Programs** tab to view installed programs.
8. Choose the program you want to uninstall (e.g., WinPatrol) and click **Uninstall**.
9. Respond to any pop-ups during the uninstallation process.
10. Once uninstalled, click the **Performance** tab to view and terminate running programs.
11. Terminate any desired programs.
12. Click the **Startup** tab to view and potentially disable startup programs.
13. Close all applications.

What I learned:

- Mirekrosoft Install Monitor helps detect hidden and background installations.
- It provides detailed information about installed software.
- It can uninstall programs completely.
- It monitors running programs and startup items.

Task 7: Perform Files and Folder Monitoring using PA File Sight

1. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight.**
2. Double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.
3. Follow installation steps.
4. Start the trial and ensure Ultra is selected.
5. Once installation is complete, navigate through the PA File Sight Console to configure monitoring.
6. Create folders, modify files, and observe monitoring activity.
7. Monitor file integrity and observe alerts.
8. Close all windows.

What I learned:

- PA File Sight monitors file and folder activities.
- It detects unauthorized file access and changes.
- It provides real-time alerts.
- It can monitor system-wide and network activity.

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

1. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView**.
2. Double-click **DriverView.exe** to launch.
3. View installed drivers and their properties.
4. Close DriverView.
5. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Reviver**.
6. Double-click **DriverReviverSetup.exe** to launch the setup.
7. Follow installation steps and initiate a driver scan.
8. Review scan results and update drivers if necessary.
9. Explore additional features such as system backup and restore.
10. Uninstall Driver Reviver and remove associated files.
11. Close all windows.

What I learned:

- DriverView displays installed device drivers and their details.
- Driver Reviver scans for outdated drivers and updates them.
- Outdated drivers can lead to system vulnerabilities.
- Regular driver updates optimize system performance.

Task 9: Perform DNS Monitoring using DNSQuerySniffer

1. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**.
2. Double-click **DNSQuerySniffer.exe**.
3. Configure capture options and start sniffing.
4. Monitor DNS queries and observe network activity.
5. Change DNS settings on the Windows Server 2022 machine.
6. Observe DNS changes in DNSQuerySniffer logs.
7. Analyze captured DNS query information.
8. Restore DNS settings.
9. Close all windows.

What I learned:

- DNSQuerySniffer captures DNS queries on the network.
- It displays detailed information about DNS queries.
- DNS monitoring helps detect suspicious network activity.
- Malicious applications can manipulate DNS settings.