**Module 7: Malware**

* **Malware (mal means malicious/ harmful, ware means software)**
* software that is specifically designed to disrupt,damage, or gain unauthorized access to a computer system.
* Malware are categories on the basis of characteristics:
* Malware Types: Virus, Trojan, Worms, RootKit, Spyware, Backdoor, Adware

* **Remote Access Trojan (RAT):**
* Using Windows 11 and Window Server 2022
* njRAT tool in Windows 11
* **For Installing njRAT tool in window 11:**
* Goto backup drive > CEH-tools> Module 7 Malware threats > Trojan types> remote access trojan(RAT)> njRAT > run “njRAT” exe
* **Steps for Creating njRAT trojan:**
* Open “njRAT” application & Assign Port Number and Start
* Goto “Builder” tab on bottom & Assign host ip(listener machine ip)
* Leave all other options by default and Build the trojan
* Save the builded file in exe format in windows 10 and copy it to shared drive then paste it
* Create snapshot in vmware and assign description if in case of problem in windows 2022 to revert it back to original state.
* Goto window server 2022 > backup drive> run the builded “exe” file/malware
* Goto windows10 > see the status of windows server 2022 > right click> goto “ Remote desktop “ for Remote Desktop Connection.

- Right Click and Explore the options for different Features.

* **( Virustotal - online tool to detect Virus )**

- upload malware “exe” and analyze the malware status

- In Windows 11, goto CEH tools> malware Threats >

Crypters > Swayzcryptor > open “swayzcryptor” tool

- insert file inside swayzcryptor > check all checkboxes > encrypt >

save in location

* Goto “Virustotal” online tool and upload file and analyse the malware detected status.
* **JPS Virus maker Tool: (in window 11)**

**Steps:**

* In windows 11> goto CEH tools> malware Threats > Virus Maker > JPS Virus maker
* Open JPS virus maker tool
* Hide run, disable cmd, hide clock,hide taskmanager
* Goto right arrow option> change window password> change computer name
* Leave all other options by default
* Change bits(64 bits), Create virus and exit.
* Access virus via server 2022 through shared drive.
* Run the virus.
* Check the changes in server 2022
* **Malware Analysis:**
* the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, malvertising, and ransomware.
* Types of Malware Analysis: Static Malware Analysis, Dynamic Malware Analysis
* Static Malware Analysis: Analyzing malware in depth without its execution
* Dynamic Malware Analysis: in-depth insights by observing the malware running in a controlled / isolated environment to observe its behavior
* Zero Day malware: malware without digital Signature
* **Static Malware Analysis Tool: (in window 11)**
* Goto backup drive > CEH-tools> Malware Threats > Malware analysis tool > Static Malware analysis tool > String Searching tool> BinText > bintext.exe
* Packaging and Obfuscation Tools - pEid tool
* PE Extraction Tools - PE Explore

* **Dynamic Malware Analysis:**
* **Reg organizer tool** (in windows 11)

**Steps:**

1. Goto backup drive > CEH-Tools > Malware threats > malware analysis tool > Dynamic malware analysis tools > Registry Monitoring tools > Reg Organizer
2. Goto tools tab > Registry Snapshot > Create a Snapshot > enter Snapshot name > ok > close
3. Install / Uninstall application for testing the registry
4. Reopen Reg organizer tool> tools tab > registry snapshot > select snapshot > compare with the current registry value > check the installed/uninstalled app status > ok

**Checking Services:**

* Service manager tool
* Services.msc ( inbuilt tool in window os)

**Windows Startup Programs monitoring tools:**

* Tool: Autoruns for windows //to check startup services
* Tool: Win patrol

**Installation Monitoring Tools:**

* Tool: Mirekusoft Install Monitor

**Data Loss Prevention Tools:**

* Tool: PA File Sight

**Device Driver Monitoring tool:**

* Driver View Tool // checks and shows driver status
* Driver reviver Tool // checks for outdated drivers.