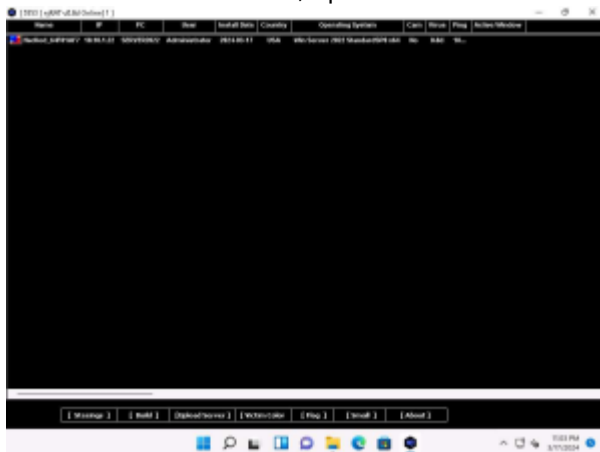


Lab Module 07

Lab 1: Gain Access to the Target System using Trojans

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

- njRAT v0.8d
 - puerto 5553
 - Build
 - Host (IP máquina local)
 - Randomize Stub
 - USB Spread Nj8d
 - Protect Process (BSOD)
 - Copiar .exe en maquina víctima y ejecutar
 - en ese mismo momento, aparece información en el RAT



- archivos
- tareas
- registro
- remote desktop
- control de camara
- keylogger

Lab 2: Infect the Target System using a Virus

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

- JPS Virus Maker
 - marcar Auto Startup
 - Disable TaskManager
 - Disable Windows Update
 - Disable Control Panel
 - Disable Drives
 - Hide Desktop Icons
 - Enable Remote Desktop
 - Remove Bluetooth
 - Turn Off Windows Firewall
 - Turn Off Windows Defender
 - en opciones:

- Change Windows Password
- Change Computer Name
- Enable Convert to Worm
- JPG Icon

Lab 3: Perform Static Malware Analysis

Task 1: Perform Malware Scanning using Hybrid Analysis

- <https://hybrid-analysis.com>

Task 2: Analyze ELF Executable File using Detect It Easy (DIE)

- Detect It Easy v3.09

Task 3: Perform Malware Disassembly using IDA and OllyDbg

- IDA Freeware 8.4

Lab 4 Module 07: Perform Dynamic Malware Analysis

Task 1: Perform Port Monitoring using TCPView and CurrPorts

Task 2: Perform Process Monitoring using Process Monitor

From:
<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:
<https://miguelangel.torresegea.es/wiki/info:cursos:pue:ethical-hacker:sesion2:lab7>

Last update: 21/02/2025 03:53

