Advanced Security Evasion in Windows with Hidden Commands

Description:

Evaluate how well different security solutions can detect and respond to stealthy attack techniques, including hidden command execution, keyloggers, process injection, backdoors, and persistence mechanisms. The objective is to evaluate the detection capabilities of Windows Defender and third-party antivirus/EDR solutions by logging system behavior, network activity, and event logs. More Info on GitHub[Click Here]

Objectives:

1. Attacker Techniques (Evasion & Stealth Methods)

- Keylogger Deployment & Detection
- Backdoor Creation & Remote Access
- Non-Visual Command Execution & Process Hiding
- Process Injection & Memory Manipulation
- Persistence Techniques

2. Windows Security Tests (Detection & Logging)

- Configuring multiple security solutions (Windows Defender).
- PC activity, network traffic, and event logs to analyze security responses.
- Comparing security solutions based on detection effectiveness and response time.

Advanced Security Evasion in Windows with Hidden Commands

Team Responsibilities:

- Person 1: Attacker Implementation & Evasion Techniques
- Person 2: Windows Security & Defender Monitoring
- Person 3: Data Analysis & Reporting

References:

- https://lolbas-project.github.io/
- https://learn.microsoft.com/en-us/powershell/
- https://www.malwarebytes.com/keyloggers
- https://www.microsoft.com/security/blog
- https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors
- https://docs.rapid7.com/metasploit
- https://www.mandiant.com/resources/process-hollowing
- https://www.redteamjournal.com/dll-injection
- https://attack.mitre.org/techniques/T1053/
- https://docs.microsoft.com/en-us/sysinternals/
- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/
- https://www.elastic.co/security