- Filename: eccouncil-ceh31250-v11-7-5-1-fileless-malware.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Fileless Malware
  ==

Fileless Malware

Objectives:

- Define Fileless Malware
- List and describe Fileless Malware types and infection vectors
- Apply obfuscation to malware to bypass detection

- What is Fileless Malware?
  - Takes advantage of system vulnerabilities to inject malicious code into running processes
    - Malicious code runs system commands through PowerShell, WMI, bash, etc
      - This can be accomplished through...
        - User visiting a malicious website
          - Browser weakness
        - User running a malicious macro
        - Downloading a malicious file
- Types of Fileless Malware
  - 2 classification systems
    - Evidence
    - Entry Point
  - **Evidence**
    - Type I: No file activity performed
    - Type II: Indirect file activity
    - Type III: Files required
  - **Entry Point**
    - Exploits
      - File-based
        - Initial entry vector is a file
        - Payload is fileless
    - Hardware
      - Malware infects Firmware of...
        - Network Interface Cards
        - Hard Drives
        - CPU
        - USB
        - Hypervisor
    - Execution and Injection

      - *File-based*
        - Simple executable as first stage
          - 2nd stage downloaded and launched into memory, or injected into other legit process
      - *Macro-based*
        - VBA used to create malicious macro
        - Macro is enabled by user
        - Macro runs malicious code
      - *Script-based*
        - WMI, PowerShell, Bash, Python, javascript, vbscript
      - *Disk-based*
        - Boot record infection
- What is the process behind a fileless malware infection?
  - Point of Entry
    - Memory exploits
      - ie: eternalblue
    - Malicious Website
      - ie: malicious script execution, client-side attacks
    - Phishing Mail
      - ie: malicious attachment
    - Malicious Document
  - Code Execution
    - Script-based
      - Powershell, WMIC, bash, VBScript, etc
    - Code Injection
      - DLL injection
      - Process hollowing
  - Persistence
    - Registry entries
    - WMI
    - Scheduled task
  - Achieving Objectives
    - Recon
    - Cred grab
    - Sensitive data exfil
    - Cyber Espionage
- With so many protections available, how does Fileless malware sneak passed AV?
  - Mixed case
  - Insertion of characters

    - Commas and Semicolons
      - Interpreted as whitespace in Windows
    - Carat
      - Used for escaping
      - Use double carats for more effectiveness
        - `cmd.exe /c p^^o^^w^^e^^r^^s^^h^^e^^l^^l.exe`
  - Custom Environmental Variables
    - `set a=Power && set b=Shell && %a:~0,5%%b:~0,5%`
  - Built-in Environmental Variables
    - `%CommonProgramFiles%` = **C:\Program Files\Common Files**
      - `cmd.exe /c "%CommonProgramFiles:~3,1%owershell"`
  - Double Quotes
    - Argument Delimiter
      - Used to concatenate
        - `cmd.exe /c P""owe""r""Sh""e""ll`
  - DEMO
    - Parrot: LPORT = 443, HTTP on 8000, serving /home/dlowrie/Tools/Shells/Powershell
    - Target: Run script *update_script.cmd*