Exercise – Windows Baseline Processes

Scenario

You are analyzing the output of process lists received from operators for four systems. Extrapolate the type of system, operating system version, and its purpose from these lists. Also assess if there is concern moving forward with an operation given the current state of the machine.

Exercise

Research and analyze the processes listed in the process enumeration outputs. Assess the following information for each system and document your results. Extrapolate as much information as possible for each criteria, create a hypothesis to answer each question, and back up your hypothesis with evidence from your research:

- The type of system (e.g. workstation, server, firewall, etc.)
- The operating system and service pack or revision in use (e.g. Windows 10, Windows 7, Windows XP SP2, Windows Server 2003 r2)
- The system's purpose (e.g. Mall Kiosk System, Web Mail Server, etc.)
- Virtualization implications (e.g. The system is virtualized, the system is a hypervisor, the system is bare metal, etc.)
- Security implications (e.g. the system is seriously vulnerable, the system is compromised, the system is very locked down, etc.)
- Operational implications (e.g. this system would be a good pivot for offensive missions, this system is a defensive nightmare, this system would be difficult to breach or to use for data exfiltration)

Submit

- A write-up in PDF or DOCX format annotating your process and the results of your analysis
- Submitted document names MUST include your last name, ie. Beckman_analysis.docs
- Do not ZIP files before submitting! Tip: You are not expected to do this in Powershell.

Grading

- 70% - Minimal effort at research and assessment
- +10% - Clear, concise, well presented report
- +10% - Critical analysis of processes, their security implications, and their operational implications
- +10% - Critical analysis of each system's operating system and purpose

Learning Objectives / Outcomes

- Familiarity with key Windows processes
- Researching Windows processes
- Analyzing windows processes and related information
- Assessing security and operational implications of Windows processes

- Assessing user application of Windows systems
- Presenting information in a clear and concise manner

Last updated 2017-06-30 11:49:20 EDT