|  |  |  |  |
| --- | --- | --- | --- |
| beaconing |  | 1 | 43 |
| Suspicious Network activity | * Abnormal for the associated process.   EX: notepad making connections to port 80  Service making multiple outbound connections (could be an updater)   * Abnormal for the environment:   Lots of activity during off hours.  Long running HTTP/HTTPS sessions  Beaconing   * Technique-specific:   Lateral movement implies connections to the other internal hosts.   * Known malicious host/ address   Based on threat intelligence  From incident, or other processes/ connections (pivoting) | 1 | 43 |
| Examining Services | Windows services are background tasks that are controlled through the windows services.exe process and can be configured to run automatically, and it will be used as a persistence method. The Get-Service PS cmandlets retrieves information about all running services. | 1 | 44 |
| Get-Service | Does not provide all the details we might want, including the path | 1 | 44 |
| Registry interrogation |  | 1 | 45 |
| FilterHashTable | PowerShell. When you don’t need all the data, it helps you filter data. It is better than using Where-Object |. It gets event for a specific data range | 1 | 48 |
| Differential analysis | Where we can take a list of known good services, take a list of current services, and then that will display all the things that changed and things that we need to investigate | 1 | 50 |
| PowerShell Legacy commands | It is Ok to continue using legacy commands to get the information you need to completed your analysis. When invoking legacy commands, specify .exe at the end of the command to avoid using PowerShell aliases with the same name. | 1 | 52 |
| PowerShell cheat sheet |  | 1 | 51 |
| Additional Supporting Tool | * The Sysinternals tools are excellent and free. * The center for internet security has templates that can be used and scoring tools that can be used with Windows. | 1 | 53 |
| Sysinternals tools | Suite of tools to add to your incident response and detection arsenal.   * **Process explorer**: detail information for running processes. * **Autoruns**: displays a comprehensive list of AutoStart extensibility points (ASEP) * **Process Monitor:** Shows file system, registry, network and process information in real time. * **Sysmom**: Collects detailed event information for system monitoring and analysis. * **TCPView:** Maps listening and active TCP and UDP activity to the associated applications. * **Procdump:** CLI tool to capture memory for a running process for analysis | 1 | 53 |
| Network investigations | Network information can provide valuable insight into an investigation, it is not without challenges though and should be used to augment other analysis activities. | 1 | 59 |
| Network investigations:  Sources | * Network Traffic: live capture * Network Devices: Firewalls, proxies. * Host Devices: Windows event logs can create logs about the network’s interaction. | 1 | 59 |
| Network investigations:  Challenges | * Accessibility: Data Export. * Fidelity: Missing data. * Visibility: Encryption | 1 | 59 |
| Analyzing packet captures | Full packet capture is often considered a gold standard.   * Provides the lowest (practical) View of data, * Analysis and investigation can be done offline.   Still have limitations in practice   * Very large files. * Encryption can hinder analysis. * Application layer protocols not easily evaluated.   Two commonly used format.   * Pcap: Older format, widely supported. * Pcapng: extensible, advance features such as encryption, stored comments, improves timestamps resolution and more | 1 | 60 |
| Tcpdump | Its power comes from the ability to extract useful information quickly at the command line leading to opportunities for parsing the output with text processing tools and automating these tasks | 1 | 61 |
| Tcpdump | Command-line tool to capture and display network traffic.   * In widespread use for several decades and display network traffic.   Available on most environments and platforms.   * Unix-like (Linux, macOS, BSD) Windows (windump) * Even many embedded analyses.   Performs Basic protocols analysis.   * Interprets IP, TCP, UDP, ICMP, etc.   Includes powerful options for filtering. | 1 | 61 |
| Tcpdump options | * Tcpdump -i interface: Capture traffic for an interface. Can also use *any.* * Tcpdump -i interface -w file: Captures for an interface and write to a file. * Tcpdump -r file -n: Read packets from a file and don’t resolve hosts and ports. * Tcpdump -r file -n -A: read packets from a file, don’t resolve, show as ASCII | 1 | 62 |
| Berkeley Packet filter (BPF) | Specialized language for filter packets.   * BPF expressions are composed of primitives and operators. * Primitives are composed of one or more qualifiers and an ID   Three kinds of qualifiers   * Type: what kind of ID is (host, net, port, or port range) * Dir: the direction (src, dst) * Proto: match a protocol IP, TCP. UDP, ICMP)   Can combine multiple primitives   * Using and (and, &&) or (or, ||) and not (not, !)   Parentheses to add precedence can also clarify intent. | 1 | 63 |