Sysinternals

## **Sysinternals Suite**

### **Task 1 – Introduction**

Sysinternals is a collection of advanced system utilities from Microsoft for troubleshooting, monitoring, and analyzing Windows systems.  
Created by Mark Russinovich, it includes tools for processes, files, disks, networking, and security.

### **Task 2 – Install the Sysinternals Suite**

**Normal Usage:**

* Download from Microsoft’s official site.
* Extract to a folder and add to PATH for command-line access.

**Unusual Usage / Security Concerns:**

* Download from unofficial sites (possible trojans).
* Hidden installation or execution by threat actors.

### **Task 3 – Using Sysinternals Live**

**Normal Usage:**

* Access tools directly from Microsoft servers via \\live.sysinternals.com\tools.
* No local installation required.

**Unusual Usage / Security Concerns:**

* Remote execution without admin approval.
* Used in persistence scripts by attackers to fetch tools.

### **Task 4 – File and Disk Utilities**

**Examples:**

* **AccessChk** – Checks file and folder permissions.
* **Disk2vhd** – Converts physical disks to virtual hard disks.
* **SDelete** – Securely deletes files.

**Unusual Usage / Security Concerns:**

* SDelete used to destroy forensic evidence.
* Disk2vhd used to exfiltrate entire system images.
* AccessChk used to find privilege escalation paths.

### **Task 5 – Networking Utilities**

**Examples:**

* **TCPView** – Lists active TCP/UDP connections.
* **PsPing** – Measures network latency and throughput.
* **Whois** – Queries domain registration.

**Unusual Usage / Security Concerns:**

* Attackers using TCPView to monitor investigator connections.
* Whois used for recon on potential targets.
* PsPing used for network mapping.

### **Task 6 – Process Utilities**

**Examples:**

* **Process Explorer** – Advanced Task Manager with DLL view.
* **Process Monitor (Procmon)** – Tracks file/registry/process activity.
* **PsExec** – Remote process execution tool.

**Unusual Usage / Security Concerns:**

* PsExec used for lateral movement in networks.
* Procmon used by attackers to understand security tools.
* Process Explorer manipulated to hide malicious processes.

### **Task 7 – Security Utilities**

**Examples:**

* **Autologon** – Configures Windows automatic logon.
* **Sigcheck** – Verifies digital signatures of files.
* **LogonSessions** – Displays logged-in sessions.

**Unusual Usage / Security Concerns:**

* Autologon misused to capture credentials.
* Sigcheck results ignored, allowing unsigned malware to run.
* LogonSessions used to identify active accounts for attacks.

### **Task 8 – System Information**

**Examples:**

* **Coreinfo** – Shows CPU topology.
* **RAMMap** – Displays memory usage by process.
* **VMMap** – Analyzes virtual memory.

**Unusual Usage / Security Concerns:**

* RAMMap used to find and dump sensitive memory contents.
* VMMap used to reverse engineer protected applications.

### **Task 9 – Miscellaneous**

**Examples:**

* **BgInfo** – Displays system info on desktop.
* **ZoomIt** – Screen zoom tool for presentations.

**Unusual Usage / Security Concerns:**

* BgInfo replaced with malicious background script.
* ZoomIt embedded with trojanized versions from fake sources.

### **Task 10 – Conclusion**

Sysinternals provides deep insight into Windows internals, making it a favorite for system administrators and incident responders.  
However, many tools (PsExec, SDelete, Procmon) are **dual-use** — they can be valuable for defenders but equally dangerous in attacker hands.  
Always verify **execution source, digital signatures, and intent** before running these tools in a secure environment.

