CybeCloud System Auditor Toolkit (SAT v1.0)

Windows Security and Configuration Assessment Framework

1. Introduction

The **System Auditor Toolkit (SAT)** is a lightweight, PowerShell-based framework for auditing Windows systems. Developed by **CybeCloud**, it is designed for use by administrators, blue teams, and authorized penetration testers who need reliable visibility into host configurations and potential security gaps.

SAT performs **non-destructive, read-only assessments**. It collects critical system data, inspects security-relevant configurations, and highlights potential misconfigurations that may warrant further review.

Important Note
This toolkit is intended strictly for **authorized use**. Running SAT without explicit permission may violate laws or organizational policies.

2. Key Features

- System profiling: OS, hardware, and patch details
- User context and administrator enumeration
- Service path and permission analysis
- Scheduled task discovery (non-Microsoft tasks)
- Network overview: adapters, ports, Wi-Fi profiles
- Security settings validation (UAC, LSA, Defender)
- Installed software inventory (third-party focus)
- Heuristic search for potentially sensitive files

3. Function Reference

Get-SystemOverview

Provides operating system, hardware, domain, and recent patch information.

Test-UserContext

Displays current user details and lists members of the local Administrators group.

Find-VulnerableServices

Identifies unquoted service paths and services with insecure file permissions.

Audit-ScheduledTasks

Lists scheduled tasks excluding Microsoft defaults, highlighting non-standard entries.

Get-NetworkConfig

Summarizes network interfaces, IP configurations, listening ports, and saved Wi-Fi profiles.

Check-SecuritySettings

Validates User Account Control (UAC), Local Security Authority (LSA) protection, and Defender status.

Get-InstalledSoftware

Generates a list of installed applications excluding Microsoft/Windows defaults.

Find-SensitiveFiles

Searches common locations for files with names or extensions likely to indicate sensitive data.

Start-SystemAudit

Main function that runs the audit. Supports **Quick** and **Stealth** modes for flexibility.

4. Execution Modes

Full Audit

```
Start-SystemAudit
```

Quick Audit

Runs only essential checks (System and User).

```
Start-SystemAudit -Quick
```

Stealth Mode

Suppresses banner and introduces random delay.

```
Start-SystemAudit -Stealth
```

5. Output Format

Results are grouped into structured sections:

```
=== SYSTEM INFORMATION ===
=== USER CONTEXT ===
=== SERVICE ANALYSIS ===
=== SCHEDULED TASKS ===
=== NETWORK CONFIGURATION ===
=== SECURITY SETTINGS ===
=== INSTALLED SOFTWARE ===
=== SENSITIVE FILE SEARCH ===
```

Each section is presented in a clear, tabular format.
Output can be redirected to a file:

```
Start-SystemAudit | Out-File audit-results.txt
```

6. Installation & Usage

1. Save the script as `AuditKit.ps1`.
2. Open PowerShell with elevated privileges (recommended).

Allow script execution for the session:

```
 Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
.\AuditKit.ps1
```

3.

7. Security Considerations

- **Non-destructive**: Only queries system state, no modifications.
- **Privileges**: Some functions require administrative rights.
- **Confidentiality**: Outputs may include sensitive data (e.g., Wi-Fi keys, file paths). Handle securely.
- **False Positives**: Sensitive file search is heuristic-based and may return benign results.

8. Intended Use Cases

- Routine **system administration**
- **Blue team triage** and incident response
- **Penetration testing** with explicit authorization
- Establishing a **baseline security posture** for Windows systems

9. Roadmap & Contributions

Planned enhancements include:

- Export options (JSON, CSV)
- Modular reporting tailored to different environments
- Expanded heuristics for sensitive file searches
- More granular service and permission analysis

Community contributions are welcome. Submit issues or pull requests through the official repository.

10. Legal Disclaimer

CybeCloud SAT is intended for use only on systems you **own** or are **explicitly authorized** to audit. Unauthorized use may result in disciplinary or legal action.

CybeCloud assumes no liability for misuse of this tool.

11. Summary

The **CybeCloud System Auditor Toolkit (SAT v1.0)** consolidates critical Windows auditing functions into a single, script-only utility. It is portable, non-intrusive, and effective for identifying misconfigurations, security gaps, and areas that require further investigation.

SAT empowers professionals to:

- Gain rapid insight into system state
- Validate security baselines
- Detect misconfigurations early
- Strengthen system defenses with actionable visibility

Developed by CybeCloud

Download & Documentation: https://github.com/CybeCloud/CybeCloud-System-Auditor-CSA-