Digisuraksha Cybersecurity Internship 2025

Intern Name: Dhairya Kumar Patel
Intern ID: 445
Date: July 2025

Section 1: Tool Overview – ShellRunas

Description:

ShellRunas is a command-line utility developed by Microsoft Sysinternals. It extends the native Windows runas command by integrating its functionality directly into the Windows Explorer context menu. This allows users to execute programs with alternate user credentials (e.g., as an administrator or a different domain user) without needing to log off or switch user accounts.

Purpose:

ShellRunas simplifies the process of launching applications with elevated privileges or under different user contexts. It provides a convenient graphical interface for a task often relegated to the command line, making it highly accessible for system administrators, IT support, and power users.

Section 2: Key Characteristics / Features

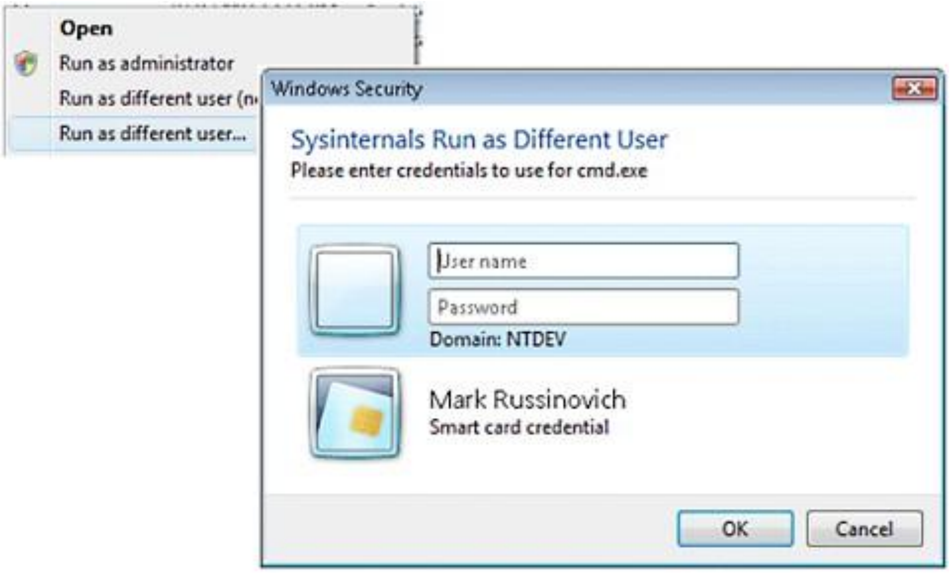
- - Context Menu Integration: Adds a “Run as different user” option to the right-click menu of executable files and shortcuts.
- - Alternate Credential Execution: Supports running applications with credentials of local, domain, or service accounts.
- - Command-Line Interface (CLI) Support: Parameters like /reg, /unreg, /netonly, and <program> [arguments] enable scripting and automation.
- - /netonly Parameter: Useful for remote access scenarios from non-domain machines.
- - Portable and Lightweight: Single executable, no installation required.
- - Microsoft Sysinternals Origin: Developed by trusted experts and maintained by Microsoft.

Section 3: How Will This Tool Help?

- - Streamlined Administrative Tasks: Enables privileged operations from standard user sessions.
- - Enhanced Security Posture: Supports least privilege principles.

- - Simplified Testing & Development: Useful for testing under different user contexts.
- - Efficient Remote Resource Access: Connect to network resources using domain credentials.
- - Improved User Experience: Avoids log-offs or Fast User Switching.

Section 4: Proof of Concept (PoC) Image



Sysinternals Run as Different User

Please enter credentials to use for cmd.exe

User name

Password

Domain: NTDEV

Mark Russinovich

Smart card credential

Section 5: Analysis Summary

ShellRunas is a highly effective utility for managing user contexts and privileges in Windows environments. Its GUI integration makes powerful credential-switching functionality accessible to a broader range of users.

🔍 Key Factors

Factor	Status	Risk/Benefit
Context Menu Integration	☑ Present	✅ High Benefit
Alternate Credential Support	☑ Present	✅ High Benefit
Portability	☑ Present	✅ High Benefit
CLI Automation	☑ Supported	✅ Medium Benefit
Modern UI Accessibility	☐ Limited (Win 11)	⚠ Medium Risk
Password Input	☐ Interactive Only	⚠ Low Risk

Section 6: Recommendations & Best Practices

- - Integrate into Standard Toolkits: Ideal for forensic analysts, sysadmins, and IT support.
- - User Training: Ensure users understand its secure and effective usage.
- - Combine with Least Privilege Policies: Use ShellRunas to reduce reliance on privileged accounts.
- - Modern UI Workarounds: Educate users on accessing context menu in Windows 11.
- - Security Awareness: Avoid /savecred in sensitive environments.

Section 7: Good About the Tool

- - Lightweight and Portable: No installation required.
- - High Compatibility: Works across Windows Vista and newer.
- - Easy Export and Reporting: Facilitates launching forensic tools.
- - Fast Parsing with Minimal Resource Usage: Efficient execution.
- - Indirect Forensic Insights: Useful for launching browser tools with specific profiles.

Section 8: Flaws / Suggestions to Improve

- - Cloud-Sync History Parsing: Not applicable to ShellRunas.
- - Real-time Monitoring: Not applicable.
- - Add Hash Validation for Integrity: Recommended for all executables.
- - Improve Visualization with AI Insight: Not applicable.
- - Plug-in for Encrypted Browser Profiles: Not applicable.
- - Modern UI Integration: Minor usability regression in Windows 11.
- - No Scriptable Password Input: Limits full automation; consider PowerShell alternatives.