Digisuraksha Cyber Security Internship

Name : Nikhil Saini

Intern id: 440

## **Tool Name:**

**NewSID**

## **History:**

**NewSID** was created by **Mark Russinovich** and **Bryce Cogswell**, founders of **Sysinternals**, to resolve the issue of duplicate **Security Identifiers (SIDs)** when deploying cloned Windows systems. Before Microsoft's introduction of **Sysprep**, NewSID was widely used for **post-clone SID regeneration**. It is now deprecated and unsupported for modern Windows versions, but it still serves an educational purpose in legacy system testing environments.

## **Description:**

**NewSID** is a graphical utility that changes a Windows computer’s SID. This is essential in environments where cloned systems could cause **SID conflicts**, especially in **domain-joined** Windows networks. It shows the current SID, generates a new one, and applies the change after a reboot.

## **What Is This Tool About?**

NewSID helps ensure each machine has a **unique SID**. Since SIDs are used in ACLs (Access Control Lists) and domain operations, duplication can break **network authentication**, **permissions**, and **security policies**. NewSID solves this by generating and assigning a **new random SID** to the local system.

**Key Characteristics / Features:**

1. GUI interface (easy to use)
2. Random or copied SID generation
3. Shows original vs. new SID preview
4. Requires reboot for changes to take effect
5. SID comparison tool included
6. Extremely lightweight (~400KB)
7. No installation — portable EXE
8. Generates new SIDs based on secure algorithm
9. Can rename computer during process
10. Works on legacy Windows OS (XP, 2000, NT, Server 2003)

## **Types / Modules Available:**

* **SID Changer**: Main module to generate and apply a new SID
* **SID Viewer**: Displays current system SID
* **Optional Rename Module**: Rename the machine during SID regeneration

## **How to Setup: Compatibility Notice:**

✅ Works only on: **Windows XP, Windows Server 2003, Windows 2000, NT4**  
 ❌ Not compatible with: Windows Vista and later (including Windows 10/11)

### **On a Test Windows VM (XP or Server 2003):**

1. Download NewSID.exe from an archive or trusted research source (it’s no longer officially available).
2. Extract NewSID.exe to the desktop.
3. Double-click to launch the GUI.
4. Click **"Generate New SID"**.
5. (Optional) Tick the box to **rename computer**.
6. System will reboot to complete SID change.

## **How Will This Tool Help?**

|  |  |
| --- | --- |
| **Purpose** | **Benefit** |
| Prevent SID collisions | Useful when deploying cloned systems |
| Preserve system integrity | Ensures domain trust relationships aren’t broken |
| Works in air-gapped legacy labs | No need for full Sysprep automation |
| Easy for beginner forensic learning | Teaches SID structures and identity concepts |

## **Proof of Concept (PoC) Images + Actions:**

## **Setup:**

* **VirtualBox/VMware** with Windows XP or Server 2003
* NewSID.exe placed on desktop

### **▶ Actions:**

1. Run NewSID.exe
2. Click **Generate New SID**
3. Observe **SID before and after**
4. Click **OK**, system reboots

## **🧾 15-Liner Summary:**

1. Changes Windows SID (Security Identifier)
2. Prevents SID duplication errors
3. Works only on legacy systems
4. No install required
5. GUI-based operation
6. Random or custom SID option
7. Can rename computer
8. Lightweight tool (<1MB)
9. Useful in cloning environments
10. Deprecated but useful in labs
11. One-click SID replacement
12. Requires reboot
13. Visual SID comparison
14. Not for modern Windows
15. Last officially supported in Server 2003

## **Time to Use / Best Case Scenarios:**

* When deploying **cloned legacy systems**
* During lab setup for **SID-based research**
* When **domain SID conflicts** arise
* For **offline system re-identification**
* In CTFs or cyber range practice on XP-era systems

## **When to Use During Investigation:**

* Investigating duplicate SID issues
* When dealing with a system restored from an image
* When preparing cloned systems for testing in isolated environments

## **Best Person to Use This Tool & Required Skills:**

### **👤 Best User:**

* System administrators working in legacy domains
* Cybersecurity researchers testing SID-based exploits or configurations
* Forensics students building knowledge of Windows identity mechanisms

**Required Skills:**

* Familiarity with Windows internals (XP-era)
* Understanding of SID structure
* VM setup experience
* Basic GUI operation

## **Flaws / Suggestions to Improve:**

|  |  |
| --- | --- |
| **Flaw** | **Suggestion** |
| Deprecated and unsupported | Tool should clearly alert about compatibility limits |
| Unsafe on modern Windows | Replace with Sysprep in modern systems |
| Requires reboot | Add snapshot/rollback integration |
| Not command-line automatable | Include CLI version for scripted environments |

## **Good About the Tool:**

* Simple and intuitive for beginners
* Directly solves SID duplication
* Small and portable (fits on floppy disk!)
* Works great in virtual labs
* No admin rights required to run GUI
* Easy to teach in cyber forensics classrooms
* Useful for showing SID-related concepts in real time