**By Megha Banne (220)**

**🛠 Tool Name:**  
 Unshadow & sumdump2

**📜 History:**  
 Both tools are associated with the password cracking process and are often used with **John the Ripper**, a well-known password auditing tool.

* unshadow is used to merge /etc./passwd and /etc./shadow files into one format readable by cracking tools.
* sumdump2 converts Windows SAM and SYSTEM files into a format compatible with password crackers.

**📄 Description:**  
 These tools assist in preparing raw system credential data into usable formats for password recovery or audit. unshadow is used in **Linux environments**, and sumdump2 in **Windows environments**. Both play a key role in the **initial data transformation** during forensic analysis.

**📌 What Is This Tool About?**

* unshadow merges passwd and shadow files to generate hashes for cracking.
* sumdump2 extracts hashes from Windows SAM files for use in cracking tools.

They are essential preprocessing tools in digital forensics and penetration testing.

**⭐ Key Characteristics / Features:**

* Used with John the Ripper
* Converts system credential files into crackable formats
* Lightweight and command-line based
* Supports batch processing
* Useful for both live and offline systems
* Can be integrated into scripts
* Supports hash extraction from:
  + Linux (unshadow)
  + Windows (sumdump2)
* Minimal system requirements
* Fast execution
* Requires basic system access (read permission)

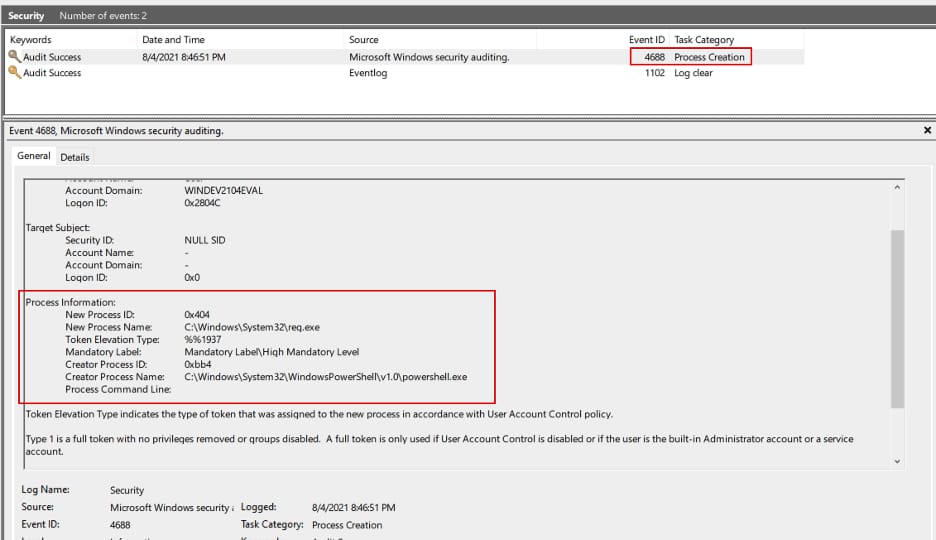
**🔧 Types / Modules Available:**

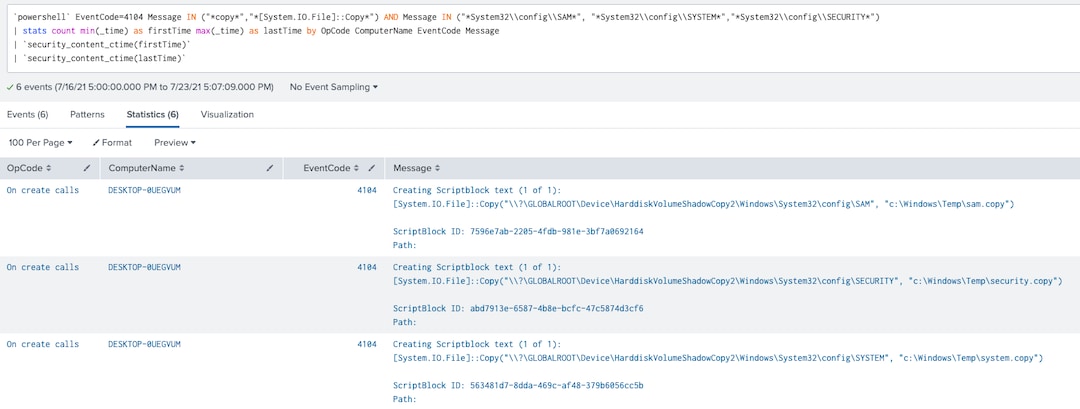
* unshadow (Linux)
* sumdump2 (Windows)
* Extensions via John the Ripper

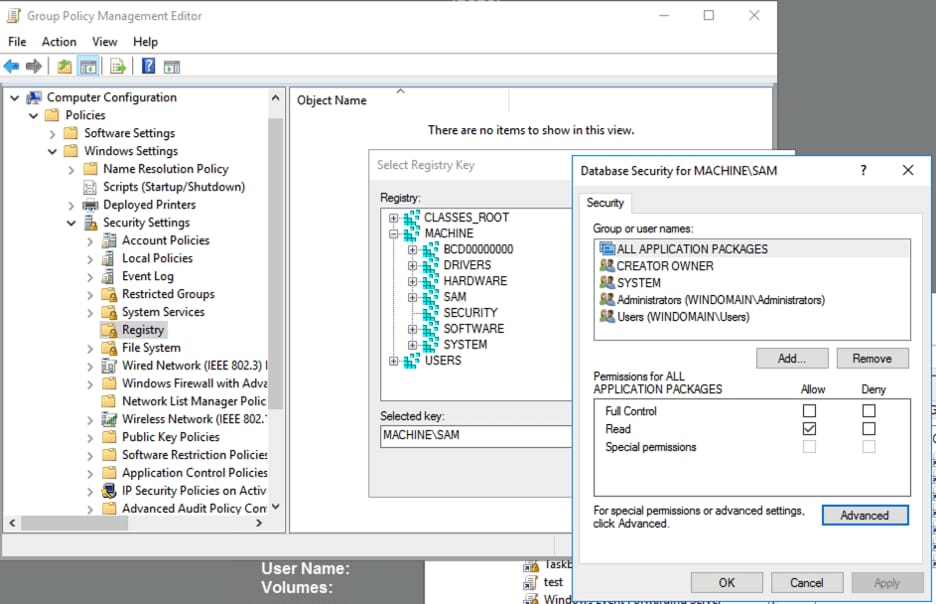
**🎯 How Will This Tool Help?**

* Converts raw authentication data into usable hashes
* Facilitates password recovery during investigation
* Speeds up the process of checking for weak/default passwords
* Supports internal audits and digital forensics
* Bridges gap between raw data and password cracking tools

**🖼 Proof of Concept (PoC)**







s  
**🧾 15-Liner Summary:**

1. Used in digital forensics
2. Supports Linux (unshadow) and Windows (sumdump2)
3. Converts system files into crackable hashes
4. Command-line interface
5. Lightweight and fast
6. Ideal for penetration testers
7. Essential in password recovery
8. Output readable by John the Ripper
9. Low system resource usage
10. No GUI required
11. Can be scripted
12. Assists in internal audits
13. Compatible with many systems
14. Helps identify weak passwords
15. No installation required (part of John suite)

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

* During credential analysis in a forensic case
* After image acquisition of a Linux/Windows system
* Before brute-force or dictionary attack
* While conducting red team or pentest exercises

**🕵 When to Use During Investigation:**

* Password audit
* Stolen credential analysis
* Insider threat analysis
* Privilege escalation tracing
* Malware persistence investigation

**👨‍💻 Best Person to Use This Tool & Required Skills:**  
 **Best User:**  
 cybersecurity Analyst, Forensic Examiner, Pentester

**Skills Required:**

* Knowledge of system authentication files
* Basic command-line experience (Linux/Windows)
* Familiarity with hash formats
* Experience with John the Ripper or other cracking tools

**🧩 Flaws / Suggestions to Improve:**

* No GUI available
* Limited to only hash extraction
* Better automation features can be added
* Add support for cloud-based authentication data
* Output validation could be improved

**✅ Good About the Tool:**

* Extremely lightweight
* Platform-specific specialization
* Fast and reliable
* High compatibility with forensic tools
* Trusted and widely used in the community