T1555.003 Extracția parolelor din Security Account Manager (SAM)

Identificare și Clasificare	Tactică MITRE ATT&CK	Credențial Access
	Tehnică	Credențial Dumping
	Subtehnică	T1555.003 – Security Account Manager (SAM)
	Sistem țintă	Windows (toate versiunile moderne)
	Nivel de acces necesar	SYSTEM sau echivalent (ex: prin escaladare de privilegii)
Descriere tehnică	Fișierul *SAM* conține hash-urile parolelor pentru conturile locale *Windows*. Acesta este stocat în: • ***C:\Windows\System32\config\SAM*** • Pentru decriptare este necesar și: *SYSTEM* (cheile de criptare) Atacatorii vizează acest fișier pentru a extrage credențiale și a efectua mișcări laterale sau escaladări.	
Metode de exploatare	1. Acces Local • *HiveNightmare* (CVE-2021-36934): *SAM* accesibil din *Shadow Copy* • ***reg save*** din ***cmd*** pentru a extrage *SAM* și *SYSTEM*: *„ reg save HKLM\SAM sam.save* *reg save HKLM\SYSTEM system.save ”* 2. Acces Distant cu privilegii • Folosirea ***secretsdump.py*** din Impacket pentru dump *SAM* remote: *„ secretsdump.py administrator@victima.local ”* 3. Analiză *offline*: • Extracție de *hashuri* din imagini *forensice* sau *VSS* (Volume Shadow Copy) • Tool-uri: ***FTK Imager, Volatility, Autopsy***	
Formate de Hash & Exploatare	• *LM / NTLM hashes* (pot fi crack-uite cu Hashcat/John). • *NTLM relay* sau *pass-the-hash* pentru mișcare laterală.	
Metode de detecție	1. Windows Event Logs • Event ID 4663: acces neautorizat la fișierul SAM. • Comportamente suspecte: ***reg.exe***, ***vssadmin***, ***powershell*** anomalii. 2. Sysmon- Reguli de detecție *„ <RuleGroup name="File Access - SAM" groupRelation="or"> <FileCreateTime onmatch="include">C:\Windows\System32\config\SAM</FileCreateTime> </RuleGroup> ”* 3. YARA/Sigma Rules • Detectarea uneltelor Mimikatz, secretsdump, etc. • Detecții bazate pe comenzi sau strings în RAM	
CWE relevante indirecte	CWE-ID	Descriere
	CWE-269	Improper Privilege Management
	CWE-284	Improper Access Control
	CWE-732	Incorrect Permission Assignment for Critical Resource

T1555.003 Extracția parolelor din Security Account Manager (SAM)

<table>
<tr><td rowspan="4">CVE asociate</td><td>CVE-2025-21313</td><td>• Denumirea: Vulnerabilitate DoS în Windows SAM.
• Scor: 6.5 (MEDIU)
• CWE asociat: CWE-833 – Deadlock
• Descriere: Această vulnerabilitate afectează componenta Security Account Manager (SAM) din Windows și poate fi exploatată pentru a provoca o stare de Denial of Service (DoS). Atacatorii pot trimite cereri special create către SAM, determinând scurgeri de memorie și prăbușirea serviciului, ceea ce duce la indisponibilitatea sistemului.
• Sistem afectat: Versiuni ale Windows 11 și Windows Server 2022 până la anumite actualizări specifice.</td></tr>
<tr><td>CVE-2024-12802</td><td>• Denumirea: Bypass MFA în SonicWALL SSL-VPN.
• Scor: 9.1 (CRITIC)
• CWE asociat: CWE-305 – Authentication Bypass by Primary Weakness.
• Descriere: Această vulnerabilitate permite ocolirea autentificării multifactor (MFA) în SonicWALL SSL-VPN atunci când sunt utilizate nume de cont UPN și SAM distincte în integrarea cu Active Directory. Atacatorii pot exploata această separare pentru a evita MFA și a obține acces neautorizat.
• Sistem afectat: SonicWall Gen6/Gen7 firewalls.</td></tr>
<tr><td>CVE-2024-12754</td><td>• Denumirea: Escaladare de privilegii în AnyDesk.
• Scor: 5.5 (MEDIU)
• Descriere: Vulnerabilitatea din AnyDesk permite atacatorilor să obțină privilegii administrative prin manipularea imaginilor de fundal ale desktopului în timpul sesiunilor. Aceasta poate duce la accesarea fișierelor sensibile, inclusiv a bazei de date SAM, facilitând extracția hash-urilor de parole.
• Sistem afectat: Stații cu AnyDesk (versiuni neactualizate).</td></tr>
<tr><td>CVE-2021-36934</td><td>• Denumirea: HiveNightmare
• Scor: 7.8 (RIDICAT)
• CWE asociat: CWE-732 – Assignarea incorectă a permisiunilor
• Descriere: Vulnerabilitate de tip „HiveNightmare”: fișierele SAM, SYSTEM și SECURITY au permisiuni excesive, permițând utilizatorilor non-admin să le citească. Permite extracția hash-urilor de parole și compromiterea conturilor locale.
• Sistem afectat: Windows 10 (vers. 1809–21H1), Windows Server 2019/2022.</td></tr>
<tr><td colspan="2" rowspan="5">Măsuri de protecție și remediere</td><td>Măsură</td><td>Descriere</td></tr>
<tr><td>ACL-uri stricte pe config\SAM</td><td>Refuzare acces utilizatorilor non-SYSTE</td></tr>
<tr><td>Credential Guard</td><td>Protecție împotriva extracției din LSASS</td></tr>
<tr><td>Deprivilegiare</td><td>Evitarea autentificării ca administrator pe endpoint-uri</td></tr>
<tr><td>Monitorizare SIEM/EDR</td><td>Detectarea accesului la SAM, SYSTEM, LSASS, Shadow Copy</td></tr>
<tr><td>Harden VSS</td><td>Dezactivarea Shadow Copy unde nu e necesar</td></tr>
<tr><td colspan="2">Referință</td><td colspan="2">https://cybersecuritynews.com/t1555-003-technique-steal-passwords/
https://nvd.nist.gov/vuln/detail/CVE-2025-21313
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21313
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0001
https://nvd.nist.gov/vuln/detail/CVE-2024-12802
https://nvd.nist.gov/vuln/detail/CVE-2021-36934</td></tr>
</table>