SOC Use Case Report

UC-004: Local Admin Creation via net.exe

Author	Abishek V
Date	22 January 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Event Logs
Target OS	Windows 10
Attacker OS	Kali Linux

1. Use Case Summary

Use Case ID	UC-004
Use Case Name	Create Local Admin Accounts using net.exe
Category	Privilege Escalation / Persistence
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

Creation of local administrator accounts using built-in Windows utilities such as `net.exe` is a common attacker technique for persistence and privilege escalation.

2. Scenario

- Endpoint: Windows 10 (`192.168.56.110`)
- Existing user: `clair`
- Attacker user: `kali`
- New account created: `helpdesk-temp`

SOC risk point: `net user` and `net localgroup` are LOLBins. Their use for admin creation should always be validated.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs

Key Event IDs

4688	Process creation (`net.exe`)
4720	User account created
4722	User account enabled
4732	Member added to local Administrators group
4624	Logon session associated with actor

4. Detection Logic

Trigger when:

- `net.exe` is executed, AND
- a new local user is created or added to Administrators group

High-risk indicators:

- executed by non-IT user
- executed outside business hours
- admin group addition immediately after account creation

5. SOC L1 Playbook

Phase A: Triage

1. Identify process execution (`net.exe`)
2. Confirm user/group modification events
3. Identify actor account and target host

Phase B: Investigation

1. Validate command usage context (interactive vs scripted)
2. Confirm whether change approval exists
3. Review actor login source and timing
4. Check for repeated admin creation on other hosts

6. Evidence Timeline

Time	Event ID	Entity	Observation
14:12:08	4688	net.exe	Command execution detected
14:12:11	4720	helpdesk-temp	Local user created
14:12:15	4732	helpdesk-temp	Added to Administrators group
14:12:22	4624	clair	Interactive session active

Outcome: Local admin account created using built-in utility. No approval identified. Escalation required.

7. False Positive Checks

- IT support activity confirmed
- temporary admin created during system setup
- endpoint provisioning process

8. Verdict Criteria

True Positive if:

- admin account created without authorization
- created via LOLBin (`net.exe`)
- repeated across endpoints

Unauthorized admin creation via `net.exe` should be escalated immediately.

9. SOC Response Actions

- disable and remove unauthorized account
- remove admin group membership
- reset passwords if required
- review activity from the actor account

10. Ticket Notes

Ticket: UC-004 Admin Creation via net.exe
Severity: High
Verdict: Escalation required

Analyst Notes

- Detected execution of `net.exe` resulting in creation of local admin account `helpdesk-temp`.
- Account was immediately added to Administrators group.
- No authorization context identified. Activity classified as suspicious privilege escalation.