What is a rogue account?

A rogue account is persistence by creating a new user the attacker controls, or hijacking an existing one, then giving it the privileges they need (often local admin or Domain Admin). Because it is a valid account, the attacker logs in normally and blends in, and it survives the cleanup of other footholds. Variants include adding a hidden local admin, a new domain account, or quietly adding an account to a privileged group. It maps to MITRE T1136 (create account) and T1098 (account manipulation).

HOW IT WORKS

01 The technique and payload

With sufficient privilege, the attacker provisions an account:

- Local admin (Windows): `net user svc_backup P@ss /add` then `net localgroup administrators svc_backup /add`.
- Domain account: create a user and add it to a privileged group, or re-enable a dormant admin.
- Linux: `useradd -ou 0 -g 0 backup` (a second UID-0 account) or add a user to `sudo`/`wheel`.
- Quieter still: just add an existing account to a privileged group rather than creating one.

The attacker then logs in as a normal user. Documented for defensive context.

> **A VALID LOGIN SURVIVES**
>
> *A rogue account beats a single fix: resetting one compromised user's password does nothing to an attacker-created account. Eradication must enumerate accounts and group membership, not just rotate the obvious password.*

HOW TO DEFEND

- Alert on account creation and privileged-group changes (Windows events 4720/4728/4732; Linux `useradd`-/sudoers changes).
- Review local and domain accounts and privileged-group membership regularly; remove unknown or dormant ones.
- Watch for UID-0 duplicates and unexpected sudo/wheel/administrators members.
- Use MFA and conditional access so a rogue password alone is not enough to log in.
- During incident response, audit all accounts, not just the one known to be compromised.

SOURCES

[1] MITRE ATT&CK: Account Manipulation (T1098)

[2] Microsoft: Windows account management

[3] MITRE ATT&CK: Persistence (TA0003)

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence/what-is-a-rogue-account

Open online