What is an SSH key backdoor?

An SSH authorized_keys backdoor is adding the attacker's public key to a user's `~/.ssh/authorized_keys` file, granting passwordless SSH login as that user from then on. It survives password resets (it is key-based, not password-based) and reboots, needs only write access to that file, and blends in with legitimate keys. Adding it to root's authorized_keys is full persistent root. It is one of the simplest and most durable Linux backdoors and maps to MITRE T1098.004.

HOW IT WORKS

01 The technique and payload

With write access to the target user's home, the attacker appends their key:

- `mkdir -p ~/.ssh && echo "ssh-ed25519 AAAA...attacker" >> ~/.ssh/authorized_keys`
- For root persistence: append to `/root/.ssh/authorized_keys` (needs root).
- They then log in anytime: `ssh -i attacker_key user@host`, no password prompt.

Because it is key-based, resetting the user's password does nothing, the backdoor still works. Documented for defensive context.

> SURVIVES PASSWORD RESETS
>
> *The reason this backdoor is so durable: it is key-based, so changing the account password does not remove it. Only deleting the rogue key (or the file) closes the door.*

HOW TO DEFEND

- Monitor `authorized_keys` files (all users, especially root) for additions; alert on changes via file integrity monitoring.
- Baseline legitimate keys and review them periodically; remove unknown ones.
- Centralize SSH key management (or use certificates) so rogue keys stand out.
- Restrict SSH (disable root login, restrict source IPs, use a bastion) to limit where a stolen key works.
- Detect logins from new keys and unusual source addresses.

SOURCES

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

[2] Linux man-pages: sshd authorized_keys

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

Find the backdoors an attacker would leave behind.
securelayer7.net/learn/persistence/what-is-an-ssh-authorized-keys-backdoor

Open online