What is /etc/shadow?

`/etc/shadow` is the Linux file that stores user password hashes and aging information, readable only by root (unlike the world-readable `/etc/passwd`). Each line holds a hash in a format like `$6$` (SHA-512) or `$y$` (yescrypt) with a salt. An attacker who reads `/etc/shadow` (after gaining root) cracks the hashes offline with John or Hashcat to recover passwords, often reused elsewhere. It is the Linux equivalent of dumping the SAM.

HOW IT WORKS

01 The attack and payload

After gaining root (via a privilege escalation), the attacker takes the hashes and cracks them offline:

- Combine the files for cracking: `unshadow /etc/passwd /etc/shadow > hashes.txt`
- Crack with John: `john --wordlist=rockyou.txt hashes.txt`
- Or Hashcat (SHA-512crypt): `hashcat -m 1800 hashes.txt rockyou.txt`

Recovered passwords are frequently reused for SSH, sudo, databases, or other hosts, extending the compromise. Documented for defensive context.

> ROOT-ONLY, THEN OFFLINE
>
> `/etc/shadow` *needs root to read, but once read it is cracked offline at the attacker's leisure. The defense is strong password hashing plus not reusing the password anywhere else.*

HOW TO DEFEND

- Enforce strong, unique passwords so salted hashes resist offline cracking.
- Use a strong hashing scheme (yescrypt or SHA-512 with high rounds), which modern distros default to.
- Prevent the privilege escalation that gives root in the first place (the only way to read shadow).
- Do not reuse Linux passwords for SSH keys, databases, or other systems.
- Monitor for reads of `/etc/shadow` by non-root processes and unusual access.

SOURCES

[1] Linux man-pages: shadow(5)

[2] MITRE ATT&CK: OS Credential Dumping (T1003)

[3] MITRE ATT&CK: Credential Access (TA0006)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-etc-shadow

Open online