Sandfly Security™

Linux Password Hash Risks

Linux password hashes protect against brute force attack if credentials are stolen, but old algorithms are weak. This table shows past and current password hashing algorithms on Linux or other Unix systems. Choose a long password with modern hash for best attack resistance.

/etc/shadow Hash Prefix	Algorithm	Strength
(none)	descrypt	Obsolete
$sha1$	SHA1	Obsolete
$md5	MD5-SUN	Obsolete
_	BSDICrypt	Obsolete
1	md5crypt	Obsolete
$2a$	bcrypt	Obsolete - Use $2b$
$2x$	bcrypt	Obsolete - Use $2y$
3	smb-cifs	Obsolete
5	sha256crypt	Borderline
6	sha512crypt	Borderline
$2b$	bcrypt	Borderline
$2y$	bcrypt	Borderline
7	scrypt	Good
y	yescrypt	Good. Most distros now.
gy	yescrypt-gost	Good

Password Hash Strength Presentation

Solar Designer, who has contributed to many password hashes and cracking systems, has a presentation below on password algorithms, including resistance to ASIC and GPU attacks:

https://www.openwall.com/presentations/PHDays2014-Yescrypt/mgp00001.html

Hashes May Not Save You

Passwords are easily stolen in plaintext if the remote or local system is already compromised. Hashing won't save you and we recommend **not using passwords for authentication**. But since we live in reality and recognize that passwords are going to be with us for a while, we encourage you to make sure your passwords are strong and use a good hash to defend against brute force if stolen.

Passwords: Make it Long to Make it Strong

To make a password **stronger,** make it **longer**. Use 15+ characters as minimum, and more is always better. A passphrase is also a very good idea. A complex short password is weaker than a passphrase you can remember. Consider a system like Diceware to make human-friendly passwords. A minimum of seven words is the current recommendation.

Obsolete Hash and Password Auditing

Obsolete hashes and weak passwords are still a significant threat on Linux and enable easy compromise. Obsolete password hashes make it easy for attackers to brute force credentials once they obtain access. Weak passwords are common on many servers and embedded applications. Both threats help attackers enter and pivot into internal networks.

Sandfly's agentless Linux security platform includes a built-in password auditor that can find weak passwords. We also detect obsolete password hashes.

Sandfly works on embedded devices that are an especially high risk. Let us find bad passwords before attackers do, it will save you a lot of aggravation and grief. Please see our website for more information or reach out to us with any questions.

www.sandflysecurity.com