Pwdump

By Contributors to Wikimedia projects

Published: 2007-08-09 · Archived: 2026-04-05 18:11:00 UTC

From Wikipedia, the free encyclopedia

pwdump is the name of various Windows programs that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database and from the Active Directory domain's users cache on the operating system.

It is widely used, to perform both the famous pass-the-hash attack, or also can be used to brute-force users' password directly. In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped. Pwdump could be said to compromise security because it could allow a malicious administrator to access user's passwords.[1]

The initial program called pwdump was written by Jeremy Allison. He published the source code in 1997 (see open-source).[2] Since then there have been further developments by other programmers:

1. **pwdump** (1997) — original program by Jeremy Allison.[3]
2. **pwdump2** (2000) — by Todd Sabin of Bindview (GPL), uses DLL injection.[4]
3. **pwdump3** — by Phil Staubs (GPL), works over the network.
    - **pwdump3e** — by Phil Staubs (GPL), sends encrypted over network.
4. **pwdump4** — by bingle (GPL), improvement on pwdump3 and pwdump2.
5. **pwdump5** — by AntonYo! (freeware).
6. **pwdump6** (c. 2006) — by fizzgig (GPL), improvement of pwdump3e. No source code.
    - **fgdump** (2007) — by fizzgig, improvement of pwdump6 w/ addons. No source code.
7. **pwdump7** — by Andres Tarasco (freeware), uses own filesystem drivers. No source code.
8. **pwdump8** — by Fulvio Zanetti and Andrea Petralia, supports AES128 encrypted hashes (Windows 10 and later). No source code.[5]

1. ^ *"LSASS Memory - Red Canary Threat Detection Report"*. *Red Canary. Retrieved 2023-12-11.*
2. ^ Allison 2012 see *pwdump.c*
3. ^ Allison 2012.
4. ^ SecuriTeam.com 2017.
5. ^ Blackmath 2019.

- *Allison, Jeremy (30 September 2012). "Index of /pub/samba/pwdump". Samba. Retrieved 15 June 2017.*
- *Sabin, Todd (1 February 2017). "New version of PWDump2 allows dumping of password hashes Active Directory". SecuriTeam.com. Retrieved 15 June 2017.*
- *"pwdump8". forums.hak5.org. 15 May 2019.*