

Forum:[Hack Forums](#)

Thread: [Hash Identification](#)

DramaKing - September 12, 2024, 10:50 am

Need some help identifying a hash algo for a security camera that no one at my company remembers the password to. I know that the password 'friday5767' returns hash 'ae47ddabbb6c1808a24e0129a8a4d1957d0ac8f725223e80c485199b8aa6a211'. It matches SHA256, but the correct SHA256 hash is 'f3cf61ae8ef0f3139d657e15788807aca142000033fff145653c69004896618a'. I know that it's a long shot, but does anyone have an idea of how to reproduce this?

BiNBo - September 12, 2024, 11:31 am

My first thought is that the camera's system might be applying a "salt" or a "pepper." This would explain why the standard SHA256 hash doesn't match. You could see if it's a simple salt, maybe try common ones like the camera's model number, MAC address, or even the default password. Also, though less likely, it's remotely possible there's a hash collision – two different inputs producing the same hash. Which you could get around by trying slight variations of the password to see if any produce the matching hash. Just a few ideas that came to mind right away, you might have already thought of these though. Another route is to start by reaching out to the camera manufacturer if that's an option. They might have the quickest solution, or could potentially offer some insight that could lead to one.

account_ - September 12, 2024, 11:41 am

running as SHA256 f3cf61ae8ef0f3139d657e15788807aca142000033fff145653c69004896618a probably as some sort of fixed salt, low chance of getting it if that's the case.

f3cf61ae8ef0f3139d657e15788807aca142000033fff145653c69004896618a:friday5767

MitVap - September 12, 2024, 11:50 am

Tried testing multiple hash algorithms: SHA256, SHA384, SHA512, SHA3-256, Keccak-256, and GOST R 34.11-94. Used both pre and post-salt methods with potential salts like "device_serial" (I used standard security cameras for home and business as a base with random alpha-numeric combinations based on the model serial string), "installation_date" (iterating through the last year), shared values like "default", and common words for salt like "12345" etc. Still no match on the hash.

If possible, check for device-specific salts (e.g., serial number, MAC address) or installation details. I'm assuming some cameras use proprietary hashing, if you know the brand and model we might be able to guess better.

account_ - September 12, 2024, 11:51 am

edit
ae47ddabbb6c1808a24e0129a8a4d1957d0ac8f725223e80c485199b8aa6a211 running now

DramaKing - September 12, 2024, 11:57 am

(Sep 12, 2024 11:31 AM)BiNBo Wrote: [\[CITE\]](#) My first thought is that the camera's system might be applying a "salt" or a "pepper." This would explain why the standard SHA256 hash doesn't match. You could see if it's a simple salt, maybe try common ones like the camera's model number, MAC address, or even the default password. Also, though less likely, it's remotely possible there's a hash collision – two different inputs producing the same hash. Which you could get around by trying slight

variations of the password to see if any produce the matching hash. Just a few ideas that came to mind right away, you might have already thought of these though. Another route is to start by reaching out to the camera manufacturer if that's an option. They might have the quickest solution, or could potentially offer some insight that could lead to one.

Nah, it's not a hash collision. There's only one input that I'm dealing with. An input must always produce the same output. I pulled the hash straight from the NVR's database, but I suppose that there could be a salt.

Okay, I've done some network sniffing now. The NVR uses Digest Authentication when it connects to the cameras. I have no idea how it's able to use a SHA256 hash to generate a nonce value.