# H2 Hashes

## Chapter 2 – Protocol Building Blocks

Analysing One-Way Functions in Scheider’s 2015 book *Applied Cryptography*. According to the book, one-way function is quite easy compute, instead the reverse function is hard to implement. Basically, one way function means that it is possible to create it quite easily, but no one can reverse it back. There are still ways to use the one-way functions as authentication to differentiate the valid passwords from invalid passwords. Trapdoor one-way function is a way to implement secret bidirectionally adding another value in the scope. The so-called other function is known secret given along with the delivered function and the secret gives a way to open the function (Schneir 2015).

One-Way Hash Function on the other hand is known as a central of the modern cryptography. The hash function logic is quite simple. It takes input string(pre-image) and converts it as a hash value. The has function is public and the security of it is its one-wayness. It’s works as a fingerprint to one direction to ensure authenticity sending one way hash value owning the value and sending it to recipient knowing the sender. This is also possible to implement with secret key as message authentication code (MAC) method does (Schneir 2015).

## Cracking Passwords with Hashcat

Cracking hashes bidirectionally to turn values back to the original one is not possible, but the hashes are vulnerable turning the values back using word dictionary containing the correct password (Karvinen 2022).

## Command Line Basics Revisited

Linux command line tool which is existed long time in use and is still valid for the professional and other use. Using Linux OS and some basic tools in it. For example, test editors’ Nano and Pico (Karvinen 2020).

## Security Penetration Testing – The Art of Hacking Series

Learning objectives is relating to password weaknesses and password attacks. Starting hacking from the easiest point of view to use network to find default passwords from systems and using them to exploit target system vulnerability. People may also use same passwords in systems and softwares, so using these vulnerabilities is fairly simple. It’s possible to sniff passwords via public hotspot or using man-in-the-middle attack. Basically, cracking some devices network it is possible to sniff credentials inside of that network. There are also many tools to build sniffing credentials and the tools are fairly simple to pick up use from the net. Actually, there are many tools using different kinds of methods to sniff user information from systems.

Modern technology makes easier to crack passwords with powerful machines and new techniques and tools. Different service providers offers different services to make passwords more difficult to crack. For example, Linux offers salting service which add some difficulty into passwords. It makes cracking more difficult to use password dictionaries to resolve passwords. In general, using simple basic passwords is dangerous and increases risky to get hacked (OREILLY 2022).

## a) Install Hashcat and test that it works

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 1. Installing Hashcat and updating the apps

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 2. Adding directory hashed

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 3. Nessessary settings

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 4. Identifying hash types

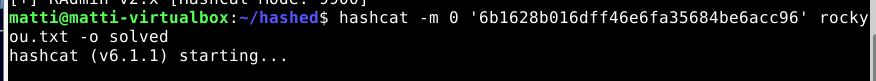


Figure 5. Cracking the hash

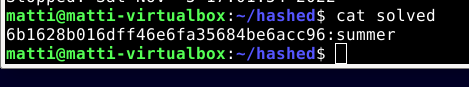


Figure 6. Cat solved

## b) Crack this hash

The hash: 21232f297a57a5a743894a0e4a801fc3

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 7. Cat solved

## c) Crack this Windows NTLM hash

The hash: f2477a144dff4f216ab81f2ac3e3207d

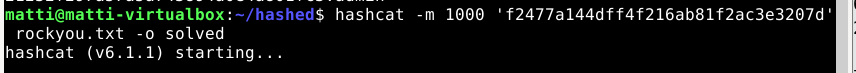


Figure 8. Windows hash

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 9. Cat solved

## d) Try cracking this hash and comment on your hash rate

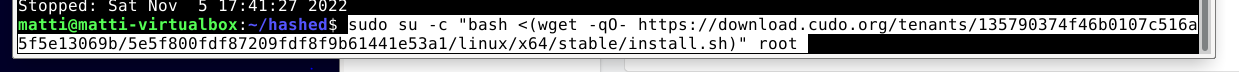


Figure 10. Installing Cudo miner

Kuva, joka sisältää kohteen teksti

Kuvaus luotu automaattisesti

Figure 11. The Cudo Miner tool

Kuva, joka sisältää kohteen pöytä

Kuvaus luotu automaattisesti

Figure 12. Hash rate

## Sources:

Schneir 2015, OREILLY , Part 1: Cryptographic Protocols, [CHAPTER 2: Protocol Building Blocks | Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition (oreilly.com)](https://learning.oreilly.com/library/view/applied-cryptography-protocols/9781119096726/10_chap02.html#chap02-sec003) Read: 5.11.2022

Karvinen, T. 2022, Cracking Passwords with Hashcat, [Cracking Passwords with Hashcat (terokarvinen.com)](https://terokarvinen.com/2022/cracking-passwords-with-hashcat/) Read: 5.11.2022

Karvinen, T. 2020, Command Line Basics Revisited, ,[Command Line Basics Revisited (terokarvinen.com)](https://terokarvinen.com/2020/command-line-basics-revisited/) Read: 5.11.2022

OREILLY, 2022 ,6.0 Learning Objectives, [6.1 Understanding Authentication and Authorization Mechanisms | Security Penetration Testing The Art of Hacking Series LiveLessons (oreilly.com)](https://learning.oreilly.com/videos/security-penetration-testing/9780134833989/9780134833989-sptt_00_06_01_00/) Read: 5.11.2022