**Falcon High School  
Cybersecurity  
Thomas Russell – Instructor**

**Password Cracking**

**Video Link: https://youtu.be/Ptf8oXkoQ6w**

*“When he reached the entrance of the cavern, he pronounced the words, '****Open Sesame!'****, and the door opened.”*

*- The Arabian Nights, Alibaba and Forty Thieves.*

Passwords are the most common mechanism used to implement authentication. They have been used with computers from the earliest days. Password authentication is easy to implement, does not require complicated hardware or much processing power. Passwords are also non intrusive (as compared to biometrics) and easily changed. While password authentication is simple, is also suffers from several vulnerabilities which can be broadly classified under human and technical factors.

Human Factors

* Password may be easy to guess.
* Writing the password down.
* Discovering passwords by eavesdropping or even social engineering.
* Reuse of same password across multiple accounts. One breach compromises all accounts with shared password.

Technical Factors

* Storage strategy
* Protection in memory, transmission etc.

In this module, we will focus on the technical factors. For a digital forensics investigator, it is important to be aware of these vulnerabilities as well as the tools and techniques used to exploit these vulnerabilities to compromise/recover passwords. We will cover the use of hashing in protecting passwords, various approaches to cracking passwords, some tools and techniques used in password cracking and finally the use of salts and expensive hashing algorithms to defend against some of the technical attacks.

Download the following real collections of leaked password hashes from popular web sites and compromise as many passwords as possible. While neither collection can be cracked in a straight forward manner, you should be able to find necessary hints by searching the Internet.

**Collection 1:**

LinkedIn: [**http://www.adeptus-mechanicus.com/codex/linkhap/combo\_not.zip**](http://www.adeptus-mechanicus.com/codex/linkhap/combo_not.zip)

Background: [**http://en.wikipedia.org/wiki/2012\_LinkedIn\_hack**](http://en.wikipedia.org/wiki/2012_LinkedIn_hack)

Hints: [**https://news.ycombinator.com/item?id=4073309**](https://news.ycombinator.com/item?id=4073309)

**Collection 2:**

Formspring: [**http://www.novainfosec.com/wp-content/uploads/2012/07/part1.txt**](http://www.novainfosec.com/wp-content/uploads/2012/07/part1.txt)

Background: [**http://www.cnet.com/news/formspring-disables-user-passwords-in-security-breach/**](http://www.cnet.com/news/formspring-disables-user-passwords-in-security-breach/)

Hints: [**https://www.novainfosec.com/2012/07/11/formspring-breach-let-the-password-cracking-commence/**](https://www.novainfosec.com/2012/07/11/formspring-breach-let-the-password-cracking-commence/)

1. The following Ars Technica article, “Why passwords have never been weaker—and crackers have never been stronger” provides a comprehensive overview of the issues involved in password security.  
   [**http://arstechnica.com/security/2012/08/passwords-under-assault/**](http://arstechnica.com/security/2012/08/passwords-under-assault/)
2. There have been a number of excellent posts on the Coding Horror blog. Following are links to a couple of those.  
   [**http://blog.codinghorror.com/youre-probably-storing-passwords-incorrectly/**](http://blog.codinghorror.com/youre-probably-storing-passwords-incorrectly/)  
   [**http://blog.codinghorror.com/speed-hashing/**](http://blog.codinghorror.com/speed-hashing/)
3. An extensive collection of various password hash leaks from the past view years and associated analysis can be found at the following link.  
   [**http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php**](http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php)
4. A good list of password cracking tools can be found on SECTOOLS.  
   [**http://sectools.org/tag/crackers/**](http://sectools.org/tag/crackers/)
5. A great collection of wordlists for can be found on Skull Security.  
   [**www.skullsecurity.org/wiki/index.php/Passwords**](http://www.skullsecurity.org/wiki/index.php/Passwords)

Video

<https://youtu.be/Ptf8oXkoQ6w>