Password Hygiene Assessment

Taufiq Ali
@NullDubai

21st December 2018

01

Why are we talking about password hygiene?

02

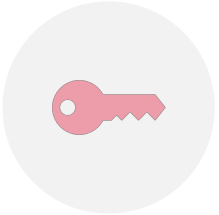
What are we going to talk about password hygiene??

03

How are we going assess password hygiene?

Why are we talking about password hygiene?

Password hygiene is very underrated



Having multiple password policies is not enough

Enforcing complex passwords is difficult

Absence of measure on effectiveness of your password policies

What are we going to talk about?

Getting started with Password Hygiene Assessment

Infrastructure requirements & benchmarking

Tools of the trade

Analyzing Password Trends

Getting started with Password Hygiene Assessment

- Familiarize yourself with Password cracking jargons
  - What is a wordlist / dictionary / rainbow table?
  - What are the tools available?
  - What are Rules & Masks
  - Online password databases
  - GPU based cracking vs CPU based cracking
  - Password filters
  - …..

Infrastructure requirements & benchmarking

Processor with more cores for CPU cracking

Fast storage device to read and write all the wordlist - SSD

GPU that supports password cracking – List here

Cracking in AWS and Azure – Tutorial

Tools of the trade

- Hashcat vs John the Ripper
- JTR is better at cracking passwords using CPU
- Hashcat is more efficient at multi-threading support for fast hashes
- Real ammunitions are Dictionaries/Wordlist

Choosing the right dictionaries/ wordlist

1. First crack passwords only using dictionaries hashes.org
   - Have I Been Pwned (501M Passwords)
   - Myspace Passwords (116M Passwords)
   - Badoo Passwords (85M Passwords)
   - LinkedIn Passwords (61M Passwords)
   - …
2. Crack the left-over passwords using word list + rules
   - Choose the rules that work the best for you.
   - Benchmarking of default rules in hash cat is done here
3. Crack the left-over passwords using masks

Note: Goal is ONLY to determine passwords that can easily be cracked with minimal effort

Analyzing Password Trends

- Most commonly used passwords
- Most commonly found password patterns
- Number of users having the same hash hashes
- Password length stats
- Password cracked via only wordlist
- Password cracked via only wordlist + rules
- Password cracked via only wordlist + rules + masks

Domain Password Audit Tool (DPAT)

Count	Description	More Info
59718	Password Hashes	Details
59198	Unique Password Hashes	
27353	User Passwords Discovered Through Cracking	
26833	Unique User Passwords Discovered Through Cracking	
45.8	Percent of User Passwords Cracked	Details
45.3	Percent of Unique User Passwords Cracked	Details
45	Members of "Enterpise Admins" group	Details
40	"Enterpise Admins" Passwords Cracked	Details
46	Members of "Domain Admins" group	Details
22	"Domain Admins" Passwords Cracked	Details
1520	LM Hashes (Non-blank)	
999	Unique LM Hashes (Non-blank)	
10	Users Passwords Only Cracked via LM Hash	Details
10	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details

Password Filters

- Purpose of password filter is to eliminate bad passwords in your organization
- Password filters allow password blacklisting
- Open Password Filter Project
- Password Filter Benchmarking
- Azure AD Password Blacklisting
- Password Policy Enforcer

Password Policy Enforcer Parameters

Golden Rules

1. Assess your password hygiene regularly
2. Create a healthy password culture
3. Allow better and yet controlled choice of passwords

References

- **Building your own rig:**
  - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/building-my-own-personal-password-cracking-box/
  - https://www.netmux.com/blog/how-to-build-a-password-cracking-rig
- **Benchmarks**
  - http://crackingservice.com/v2/?q=benchmarks
  - https://tutorials.technology/blog/08-Hashcat-GPU-benchmarking-table-Nvidia-and-amd.html
  - https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40
  - https://hashcat.net/wiki/doku.php?id=oclhashcat
  - https://www.openwall.com/lists/john-users/2015/12/06/1
  - http://www.adeptus-mechanicus.com/codex/jtrhcmkv/jtrhcmkv.php
  - http://www.adeptus-mechanicus.com/codex/markov2/markov2.php