Cyber Situational Awareness Tools
A New Perspective of Password Auditing

Dr Eliana Stavrou

Course Leader MSc Cybersecurity, UCLan Cyprus

11/06/2018
Introduction

Severe security breaches continue and get more focused
> Theft of personal information and identities took centre stage

Human aspect plays a key role
> Attackers rely on human error to gain access to systems

One of the main vulnerabilities that attackers still exploit to obtain unauthorised access
> Weak passwords & password management

Password audits are essential
> A future without passwords? Long term
> Identify authentication weaknesses
> Enhance SA as to organization’s security level

Informed decisions driven by password auditing results
> Design custom training activities & tools
Limited evaluation timeframe
When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected or compromised.
Password auditing tools

Areas of focus

Password strength meters

Analyze strength

Promising but not always accurate

Focus: the actual attack

Expert knowledge to configure tools

Password cracking

Design new password auditing tools, assisting users optimizing the password cracking process
Proposed functionality

1. PASSWORD CRACKING ATTACKS
   - Dictionary attack
   - Brute force attack

2. SITUATIONAL AWARENESS
   - Leaked passwords
   - Wordlists statistical analysis
   - User profiling

3. WORDLIST-RELATED FUNCTIONALITY
   - Preloaded / imported lists
   - Mangling rules
   - Wordlist generation (profiling, web crawling, security policy)

4. EVALUATION TIMEFRAME
   - Speed test (Merge/split)

5. RESULTS VISUALIZATION
   - Results analysis

Focus areas

Optimization through wordlists

- Customized wordlists
- Masks generation

Optimization

Merge/split
Password auditing policy

Proposed elements

1. Frequency
2. Accounts to be audited
3. Auditing profiles
4. Tools & configurations
5. Employees’ notifications
6. Customized training sessions
7. Schedule next password audit
8. Revise password policy
Password auditing toolkits

Ultimate Password Awareness Toolkit

Any actions or activities related to the material contained within this application is solely your responsibility. The misuse of the tools launched from this application can result in criminal charges brought against the persons in question. The author of UPAT will not be held responsible in the event any criminal charges be brought against any individuals misusing the tools to break the law.
Password auditing toolkits
Password Generation Toolkit
Conclusions

- Businesses need to be able to **catch up** with the ever evolving cyber threat landscape.
- Companies need to **invest** in cyber security capabilities / tools development.
- Password auditing should be **part** of an organization’s **cyber defence strategy**, it can protect from cyber attacks.
- Improve situational awareness, take **informed decisions** and decrease the risk of compromisation.
Q&A