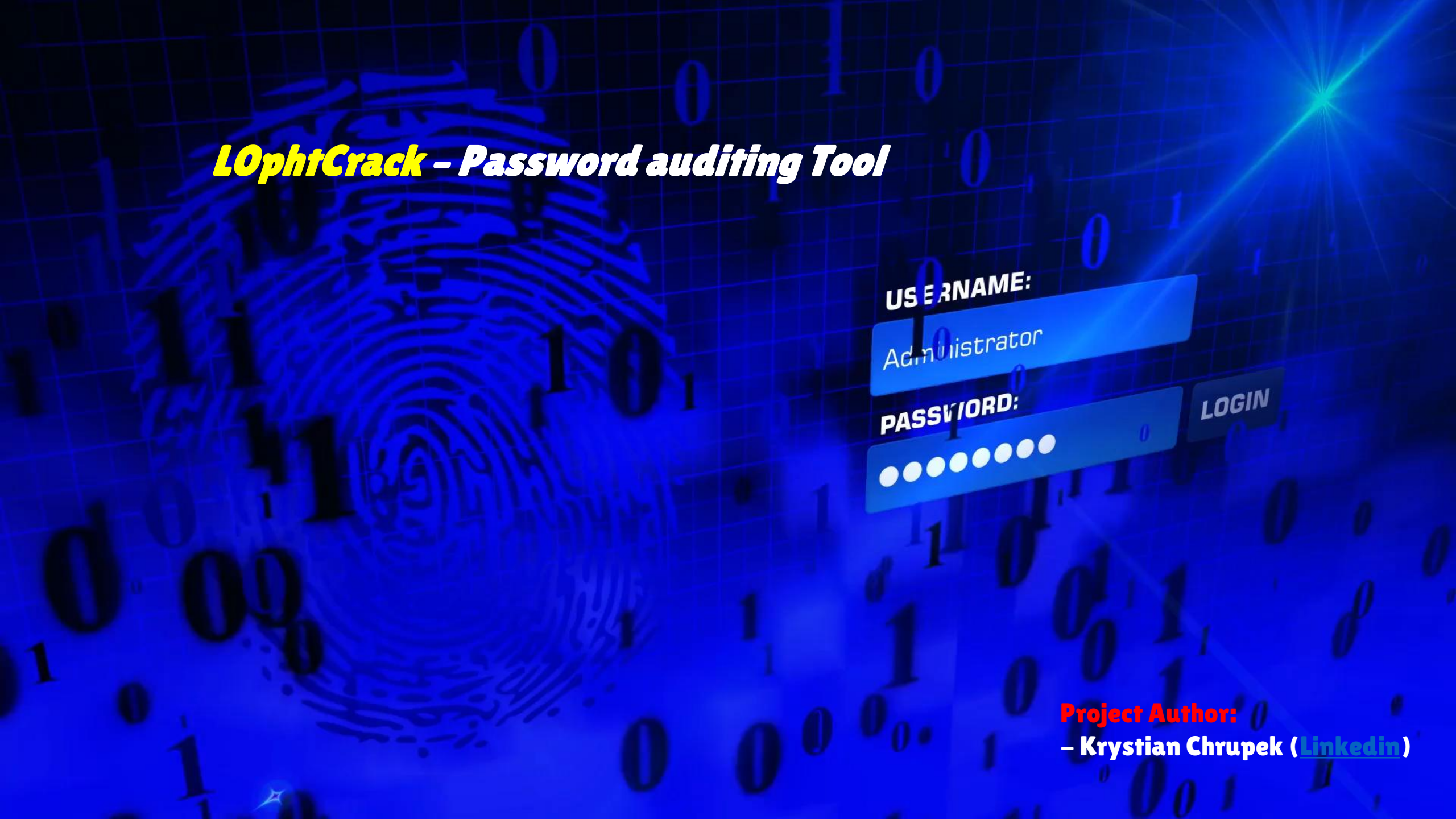
LOphtCrack – Password auditing Tool



Project Author:
– Krystian Chrupek (Linkedin)

🔥 Warning – Educational Use Only

The password auditing demonstration presented in this presentation is performed in a fully controlled and authorized environment. The target user is operating in **Windows Server 2022 virtual machine running in Oracle VirtualBox**, owned and managed by the author and used exclusively for **testing and learning purposes**.

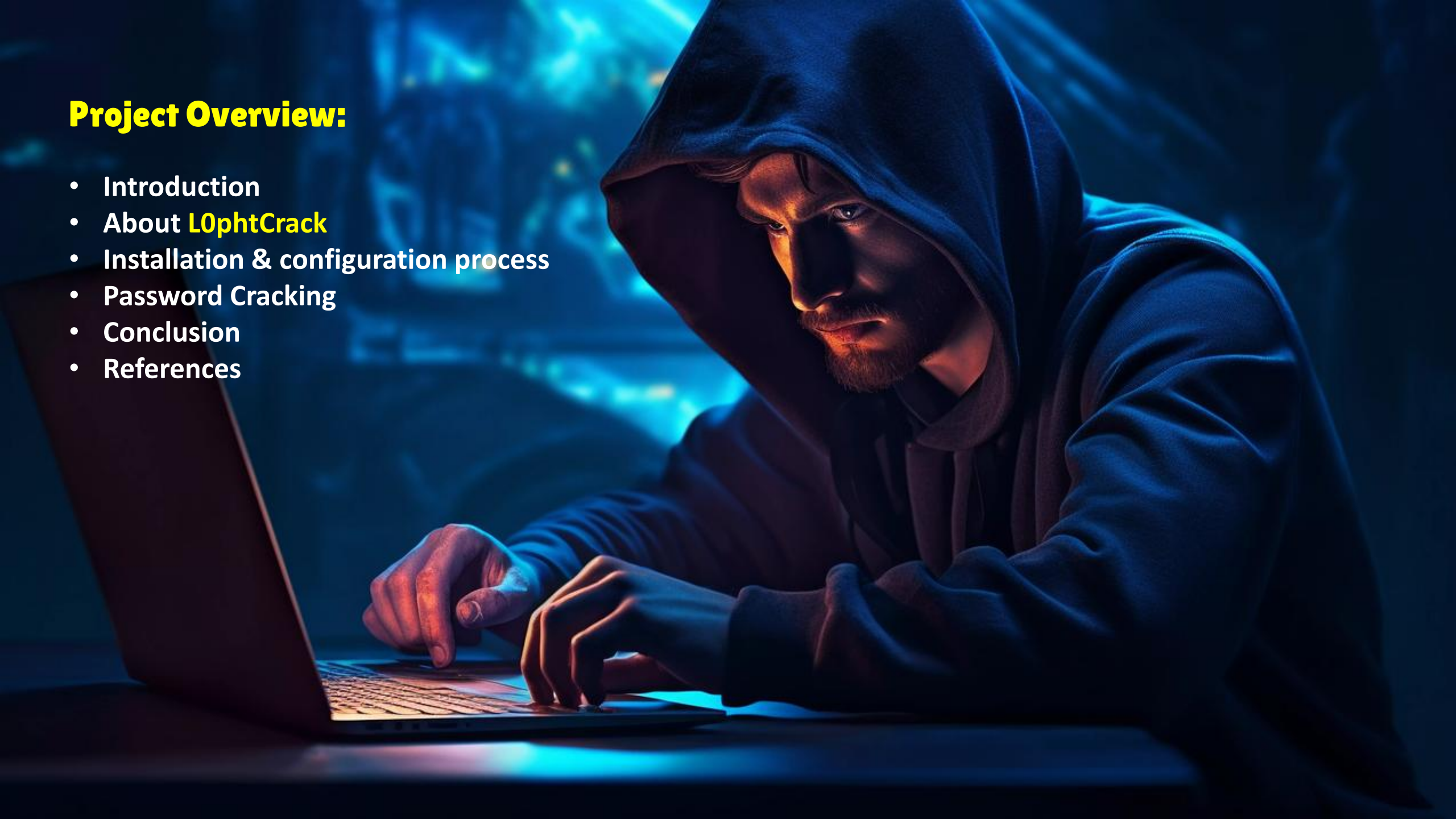
This project demonstrates the use of **L0phtCrack** to analyze password security by performing **controlled password auditing and hash analysis** on a system to which the author has full administrative rights.

This project does NOT intend to:

- perform unauthorized password cracking or auditing,
- access systems without explicit permission,
- compromise third-party or production environments,
- violate privacy, security, or data protection laws,
- misuse recovered credentials for malicious purposes.

Tools such as **L0phtCrack** must be used **only on systems you own or on environments where you have explicit permission to perform security testing**.

Unauthorized password auditing or credential attacks may be **illegal** and may **violate local laws and organizational security policies**. All actions presented here were carried out within a **legal, ethical, and controlled testing scope**, and solely for the purpose of understanding password security weaknesses and improving defensive security practices



Project Overview:

- Introduction
- About L0phtCrack
- Installation & configuration process
- Password Cracking
- Conclusion
- References

Introduction

This project is conducted in a fully controlled and authorized environment, where the target system is a **Windows Server 2022 virtual machine running in Oracle VirtualBox**, owned and managed by the author.

The purpose of this project is strictly **educational**, focusing on understanding how password auditing tools operate, how credential weaknesses can be identified, and how improper password practices can impact system security.

As part of the project, the **L0phtCrack** tool will be installed and configured step by step. The project will then demonstrate a **practical example of password auditing** performed against a **newly created local user account (PasswordTester)** on Windows Server 2022.

This test account is created **specifically for demonstration purposes**, using a known weak password (**abc123@**), allowing safe and controlled analysis.

L0phtCrack

L0phtCrack is a password auditing and recovery tool designed to assess the strength of user passwords in Windows environments. It is commonly used by security professionals to identify weak or easily guessable credentials and to demonstrate the risks associated with poor password policies.

The tool works by **extracting password hashes** from the operating system and attempting to recover plaintext passwords using multiple techniques, such as dictionary attacks, brute-force attacks, and rainbow tables.

Key features:

- Audits **local and domain user passwords** on Windows systems
- Supports **multiple attack methods** (dictionary, hybrid, brute-force)
- Allows analysis of **password complexity and policy weaknesses**
- Provides clear reporting to support **security awareness and hardening**

Typical use cases:

- Security assessments and penetration testing (with authorization)
- Password policy validation
- Training and educational demonstrations
- Identifying weak credentials before they are exploited

Installation & Configuration process

Installation:

1) Open the provided link and download the open-source Win64 installation file.
2) Double-click the downloaded file to start the installation wizard and keep clicking Next until the installation is completed.
3) After the installation is finished, right-click the application and run it with administrator privileges.
- Default installation path: C:\Program Files\L0phtCrack 7

Configuration:

1) Launch the application with administrator privileges. The startup screen will present three options:
- Password Auditing Wizard
- Start a New Session
- Open an Existing Session
2) Select „Password Auditing Wizard" and click Next.
3) Choose the target system type.
- In this project, „Windows" is selected, as the target system is Windows Server 2022.
4) Select the source from which Windows password hashes will be retrieved.
- In this case, „The local machine" is chosen because the software is installed directly on the Windows Server.
5) Choose the credentials used for hash extraction.
- „Use Logged-In User Credentials" is selected.
6) Select the audit type.
- For this demonstration, „Quick Password Audit" is used.
7) Proceed through the Reporting Options window using the default/preconfigured settings.
8) Leave „Run this job immediately" enabled in the next window and click Next.
9) Click Finish to start the password auditing process.

Password Cracking

	Username	NTLM Hash	NTLM Password	NTLM State	User Info
1	Administrator	4E109E327B658FC7F8B3092DBB31AD01	krystian	Cracked (User Info): instantly	(Built-in account for administering the computer/domain)
2	DefaultAccount			No Password Hash	(A user account managed by the system.)
3	Guest			No Password Hash	(Built-in account for guest access to the computer/domain)
4	krystian 2	6AF066A443EE3AA87FCF6B7D8BE42C1E		Not Cracked 2	krystian
5	PasswordTestter	997CF2B89EAED44B1F873F952DDAEBAE	abc123@	Cracked (Dictionary:Fast): 12s	
6	WDAGUtilityAccount	9AC9FCEEB7B6D9DC250D8CB9EC6DD5ED		Not Cracked	(A user account managed and used by the system for Windows I

1

Weak password has been cracked

1. The test account **PasswordTester** was successfully cracked using a dictionary-based attack.The password **abc123@** was identified within seconds, confirming that **simple and predictable passwords are highly vulnerable** to automated password auditing tools.

2. In contrast, the **primary user account of the system (krystian) was not cracked** during the audit.

Conclusion

Use of L0phtCrack in cybersecurity

L0phtCrack is a powerful **password auditing and security assessment tool** used to evaluate the strength of user passwords within Windows environments.

When used ethically and with proper authorization, it allows administrators and security professionals to:

- identify weak or reused passwords,
- assess the effectiveness of existing password policies,
- detect misconfigurations related to credential management,
- support system hardening and security awareness efforts.

This project demonstrated how L0phtCrack can be applied in a **controlled lab environment** to safely test and compare password security without causing harm to production systems.

Password security – key principles

The results show that **weak passwords can be cracked quickly**, while strong passwords effectively resist automated attacks.
Strong passwords should:

- be **at least 12–14 characters long**,
- include **uppercase, lowercase letters, numbers, and special characters**,
- **avoid dictionary words and predictable patterns**,
- be **unique for each account**.

Password strength directly impacts system security and even basic audits can quickly expose weak credentials.

References

1) L0phtCrack Official Project Page:

- https://l0phtcrack.gitlab.io/

(Source of the tool, documentation, and installation files)

2) MetBrains Learning Platform

- Malware Analysis – Day 1

(General overview and educational context of L0phtCrack usage in password auditing and security analysis)