



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

PASSWORD CRACKING



Module 04

Password Cracking Techniques and Countermeasures

Module Objectives



- 1 Understanding the Password Cracking and Password Complexity
- 2 Understanding Microsoft Authentication
- 3 Understanding Various Types of Password Attacks
- 4 Overview of Password Cracking Tools
- 5 Understanding Countermeasures against Password Attacks

Module Flow



1

Discuss Password Cracking Techniques

2

Discuss Password Cracking Tools

3

Discuss Password Cracking Countermeasures

Password Cracking



Password cracking techniques are used to **recover passwords** from computer systems



Attackers use password cracking techniques to **gain unauthorized access** to vulnerable systems



Most of the password cracking techniques are successful because of weak or easily **guessable passwords**

Password Complexity

1

Passwords that contain letters, special characters, and numbers **ap1@52**

2

Passwords that contain only numbers **23698217**

3

Passwords that contain only special characters **&*#@!(%)**

4

Passwords that contain letters and numbers **meet123**

5

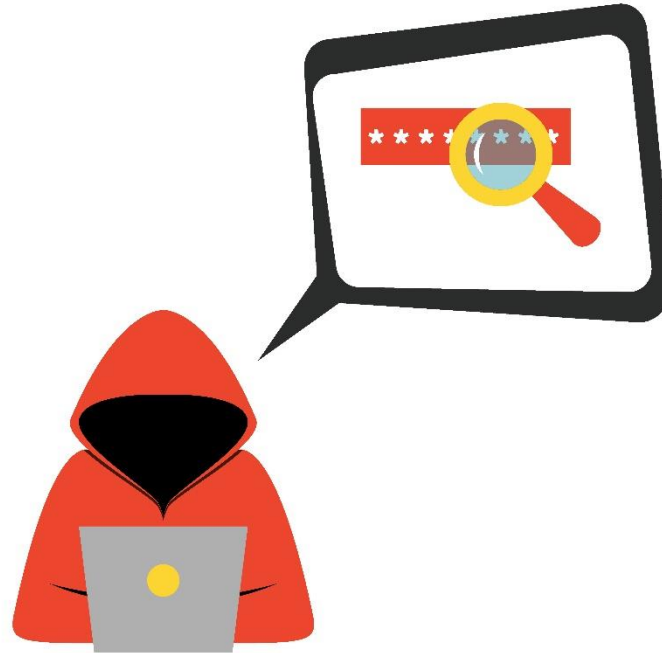
Passwords that contain only letters **POTHMYDE**

6

Passwords that contain only letters and special characters **bob@&ba**

7

Passwords that contain only special characters and numbers **123@\$45**



Microsoft Authentication

S

Security Accounts Manager (SAM) Database

- ❑ Windows stores user passwords in SAM, or in the **Active Directory database** in domains
- ❑ Passwords are never stored in clear text and are hashed, and the results are stored in the SAM

N

NTLM Authentication

- ❑ The NTLM authentication protocol types are as follows: **NTLM authentication protocol** and **LM authentication protocol**
- ❑ These protocols store the user's password in the **SAM database** using different hashing methods

K

Kerberos Authentication

- ❑ Microsoft has upgraded its **default authentication protocol** to Kerberos which provides a stronger authentication for client/server applications than NTLM

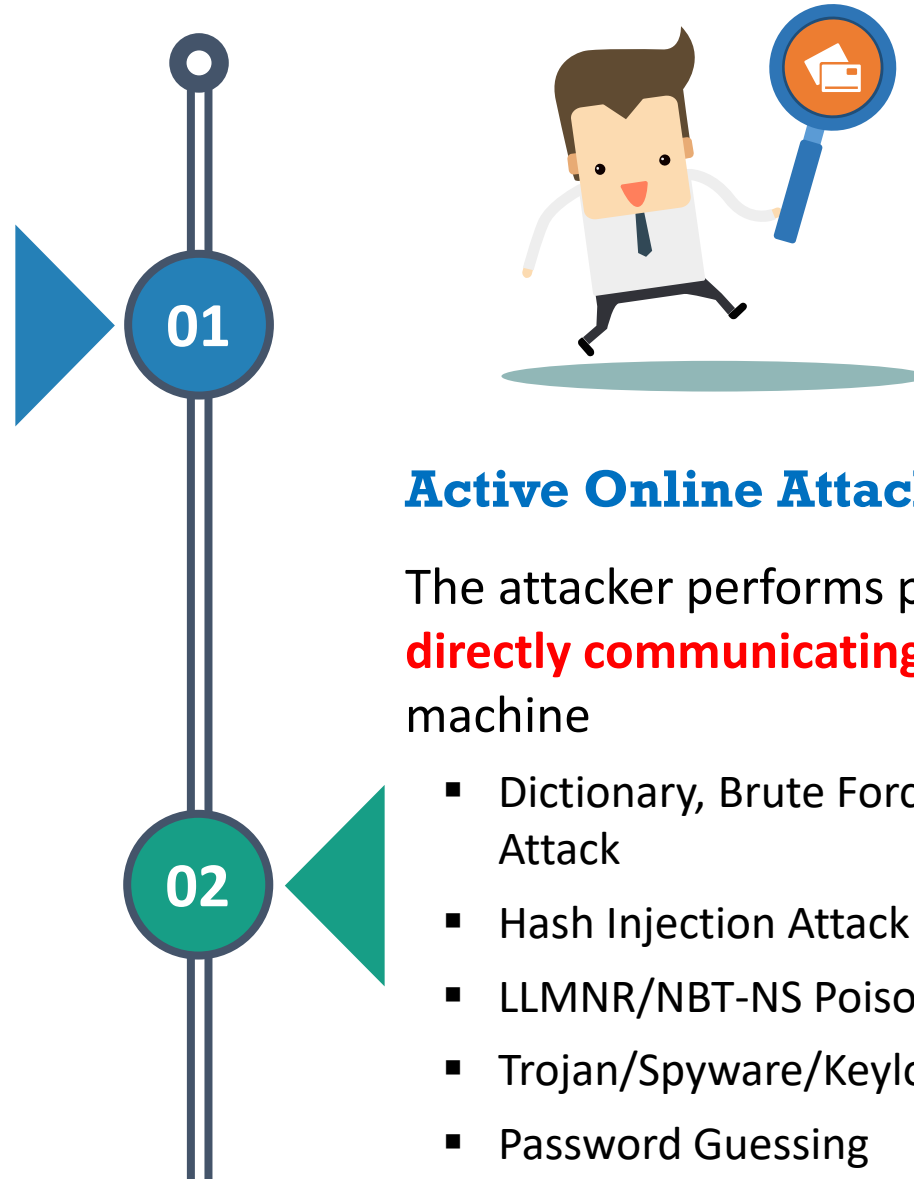


Types of Password Attacks

Non-Electronic Attacks

The attacker **does not need technical knowledge** to crack the password, hence it is known as a non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Diving



01



Active Online Attacks

The attacker performs password cracking by **directly communicating** with the victim's machine

- Dictionary, Brute Forcing, and Rule-based Attack
- Hash Injection Attack
- LLMNR/NBT-NS Poisoning
- Trojan/Spyware/Keyloggers
- Password Guessing

Types of Password Attacks (Cont'd)

Passive Online Attacks

The attacker performs password cracking **without communicating** with the authorizing party

- Wire Sniffing
- Man-in-the-Middle Attack
- Replay Attack



03



Offline Attacks

The attacker copies the target's **password file** and then tries to crack passwords on his own system at a different location

- Rainbow Table Attack (Pre-Computed Hashes)
- Distributed Network Attack

04

Dictionary, Brute-Force, and Rule-based Attack

Dictionary Attack



A **dictionary file** is loaded into the cracking application that runs against **user accounts**

Brute-Force Attack



The program tries **every combination of characters** until the password is broken

Rule-based Attack



This attack is used when the attacker gets some **information about the password**

Password Guessing

Frequency of attacks is less

The attacker creates a list of all possible passwords from the information collected through **social engineering** or any other way and manually inputs them on the victim's machine to **crack the passwords**

Failure rate is high

1

Find a **valid** user

2

Create a **list** of possible passwords

3

Rank passwords from **high to low** probability

4

Key in each password, until the **correct password** is discovered

Default Passwords

- ❑ A default password is a **password supplied by the manufacturer** with new equipment (e.g., switches, hubs, routers) that is password protected
- ❑ Attackers use **default passwords** present in the list of words or dictionary to **perform password guessing attack**

Online Tools to Search Default Passwords

- ✓ <https://www.fortypoundhead.com>
- ✓ <https://cirt.net>
- ✓ <http://www.defaultpassword.us>
- ✓ <https://www.routerpasswords.com>
- ✓ <https://default-password.info>

DEFAULT PASSWORDS

Open Sez Me! :: Passwords

5919 Default Passwords for thousands of systems from 777 vendors!

Last Updated: 7/6/2018 10:54:17 PM

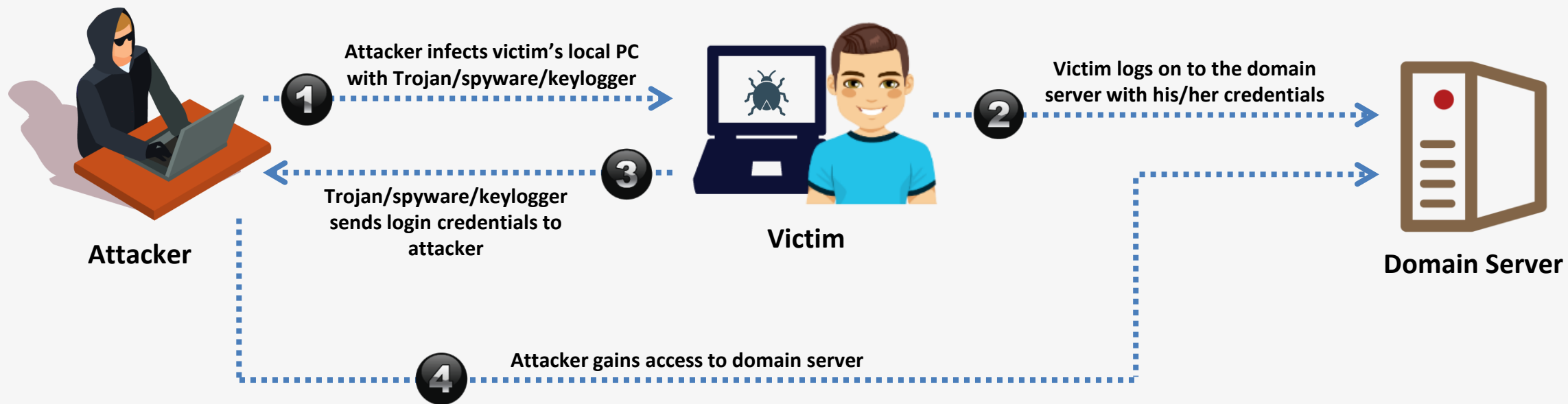
To begin, Select the vendor of the product you are looking for.

[Click here](#) to add new default passwords to this list.

\$ Top 26 Most Used Passwords	* Top 20 Most Used ATM PINs	1Net1	2Wire	360 Systems	3BB
3Com	3GO	3M	3ware	Abocom	ACC
Accelerated Networks	ACCONET	Accton	Aceex	Acer	Acorp
ACTi	Actiontec	Adaptec	ADB	ADC Kentrox	AdComplete.com
AddTron	ADIC	Adobe	ADP	ADT	Adtech
Adtran	Advanced Integration	Advantek Networks	Aerohive	Aethra	Agasio
Agere	AIRAYA	Airlink101	Airnet	Airtight Networks	AirVast
Airway	Aladdin	Alaxala	Alcatel Lucent	Alcatel	Alfa Network
Alice	Alien Technology	Allied Data	Allied Telesyn	Allied	Allnet
Allot	Alpha	Alteon	Alvarion	Ambicom	Ambit
AMI	Amigo	Amino	AMIT	Amitech	Amped Wireless
Ampttron	AMX	Andover Controls	Anker	AOC	AOpen
Apache	APC	Apple	ARC Wireless	Arcor	Areca
Arescom	Arlotto	ARRIS	Arrowpoint	Artem	Asante
Ascend	Ascom	Asmack	Asmax	Aspect	AST
Asus	AT&T	Atcom	Atheros	Atlantis	Atlassian
Attachmate	Audioactive	Autodesk	Avaya	Avenger News System	Award

<https://open-sez.me>

Trojans/Spyware/Keyloggers



- ☐ The attacker installs a Trojan/Spyware/Keylogger on the victim's machine to collect the victim's **usernames and passwords**
- ☐ The Trojan/Spyware/Keylogger **runs in the background** and sends back all user credentials to the attacker

Hash Injection/Pass-the-Hash (PtH) Attack

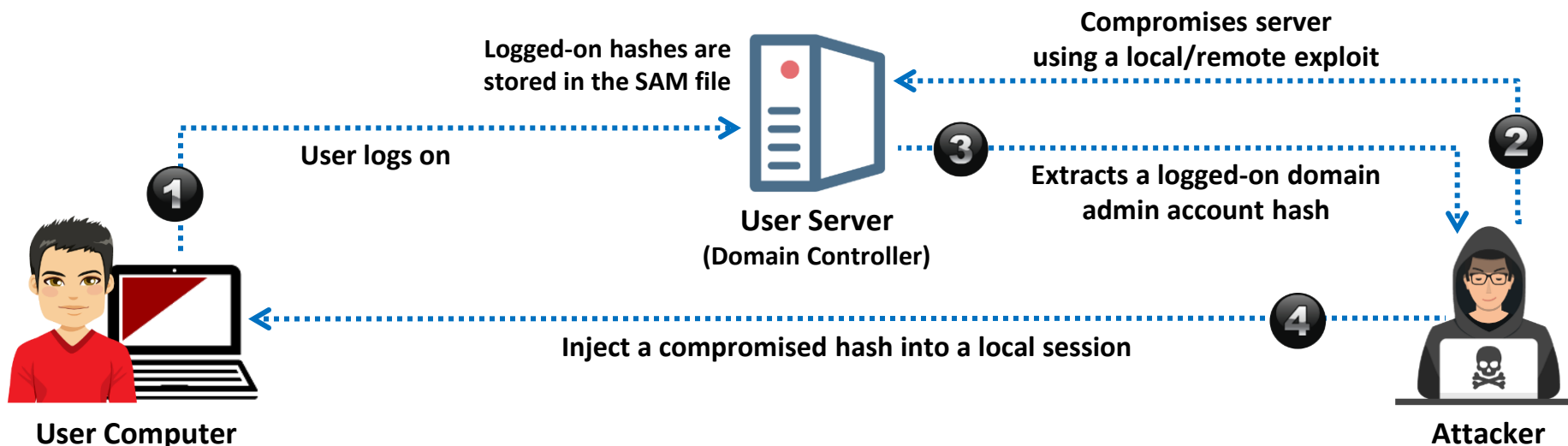
A hash injection/PtH attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate network resources



The attacker finds and extracts a logged-on **domain admin account hash**



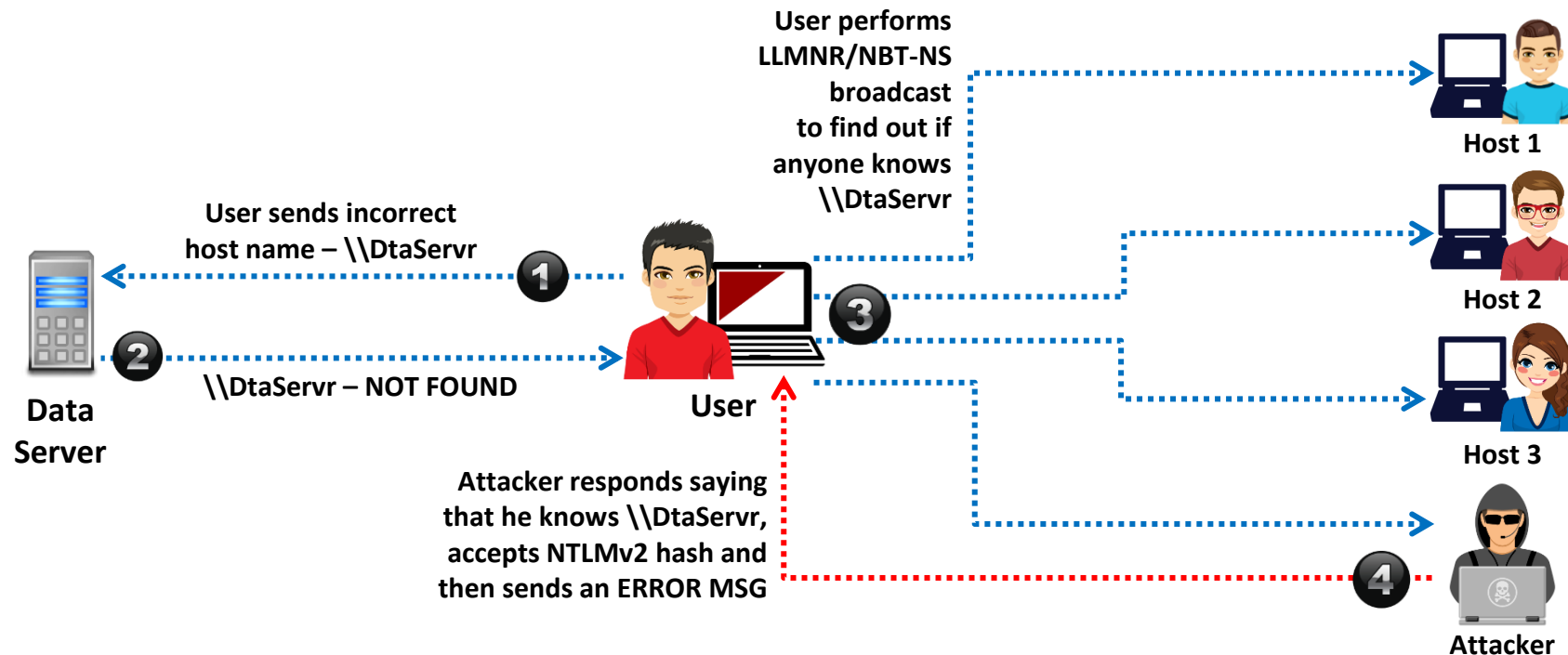
The attacker uses the extracted hash to log on to the **domain controller**



LLMNR/NBT-NS Poisoning



- ❑ LLMNR and NBT-NS are the two main elements of **Windows operating systems** that are used to perform **name resolution** for hosts present on the same link
- ❑ The attacker cracks the **NTLMv2 hash** obtained from the victim's authentication process
- ❑ The extracted credentials are used to log on to the **host system in the network**



Pass the Ticket Attack



Pass the Ticket is a technique used for **authenticating** a user to a system that is using **Kerberos** without providing the user's password



To perform this attack, the attacker dumps Kerberos tickets of legitimate accounts using **credential dumping tools**



The attacker then launches a pass the ticket attack either by **stealing the ST/TGT** from an end-user machine, or by stealing the ST/TGT from a compromised Authorization Server



The attacker uses the retrieved ticket to gain unauthorized access to the target network services

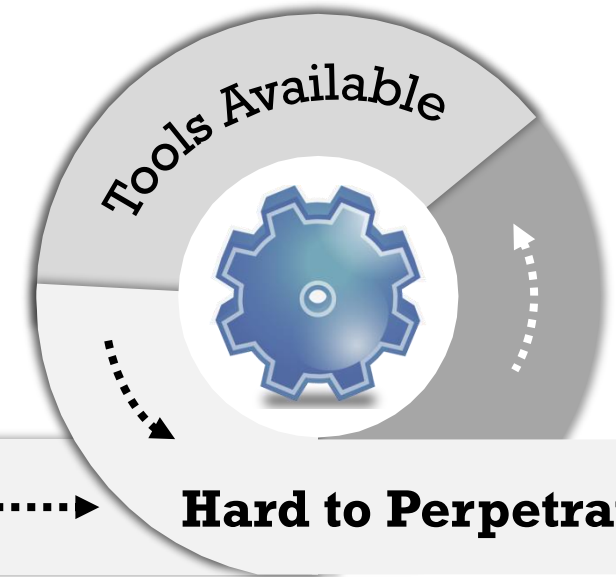


Tools such as **Mimikatz**, Rubeus, and Windows Credentials Editor are used by attackers to launch such attacks



Wire Sniffing

- Attackers run **packet sniffer tools** on the local area network (LAN) to access and record the raw network traffic
- The captured data may include **sensitive information** such as **passwords** (FTP, rlogin sessions, etc.) and emails
- Sniffed credentials are used to **gain unauthorized access** to the target system



Wire Sniffing► **Computationally Complex**► **Hard to Perpetrate**



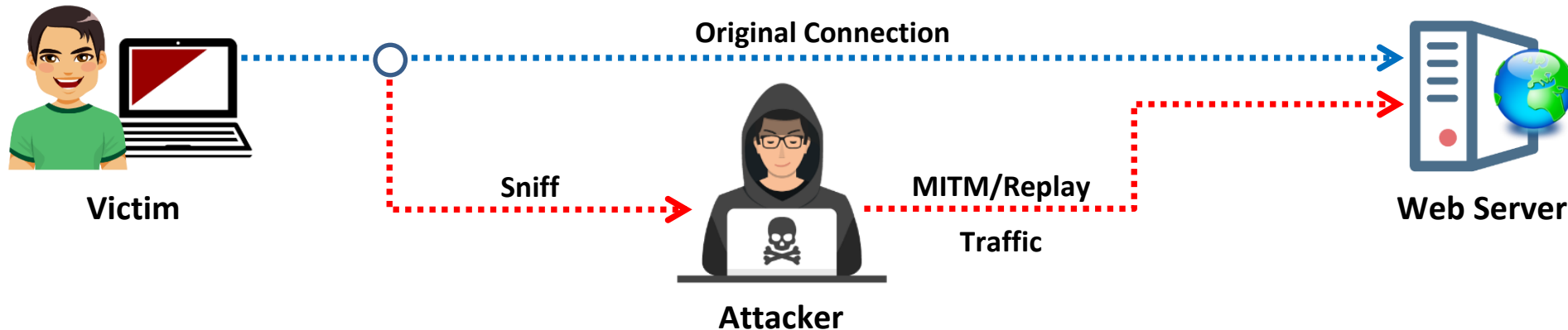
Man-in-the-Middle and Replay Attacks

- ❑ In an MITM attack, the attacker **acquires access to the communication channels** between the victim and the server to extract the information needed
- ❑ In a replay attack, packets and authentication tokens are captured using a **sniffer**. After the relevant information is extracted, the tokens are placed back on the network to gain access



Considerations

- Relatively **hard to perpetrate**
- Must be **trusted** by one or both sides
- Can sometimes be broken by **invalidating traffic**



Rainbow Table Attack

- 1 Rainbow Table**
A precomputed table that contains word lists like **dictionary files**, **brute force lists**, and their **hash values**
- 2 Compare the Hashes**
The hash **of passwords** is captured and compared with the precomputed hash table. If a match is found, then the password gets cracked
- 3 Easy to Recover**
It is easy to recover passwords by comparing the captured password hashes to the **precomputed tables**

Precomputed Hashes



1qazwed	→	4259cc34599c530b28a6a8f225d668590
hh021da	→	c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf	→	3cd696a8571a843cda453a229d741843
sodifo8sf	→	c744b1716cbf8d4dd0ff4ce31a177151



Module Flow



1

Discuss Password Cracking Techniques

2

Discuss Password Cracking Tools

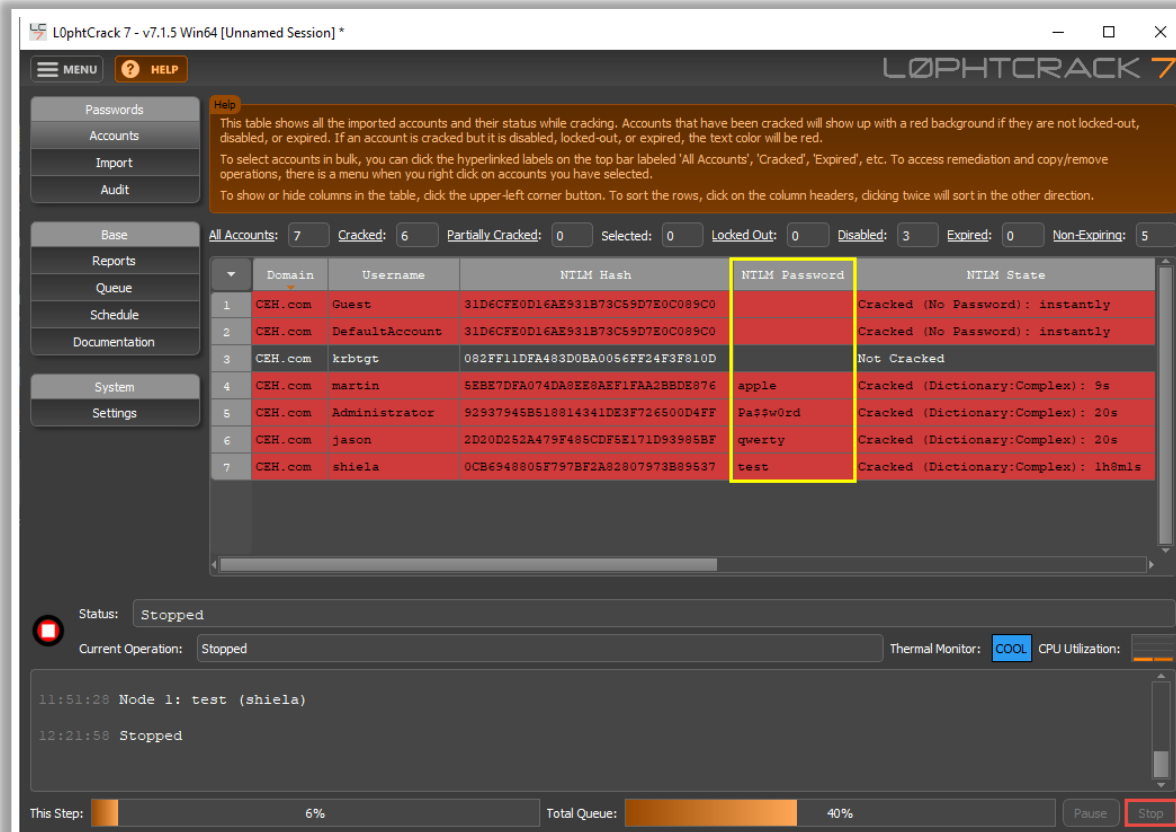
3

Discuss Password Cracking Countermeasures

Password-Cracking Tools: L0phtCrack and ophcrack

L0phtCrack

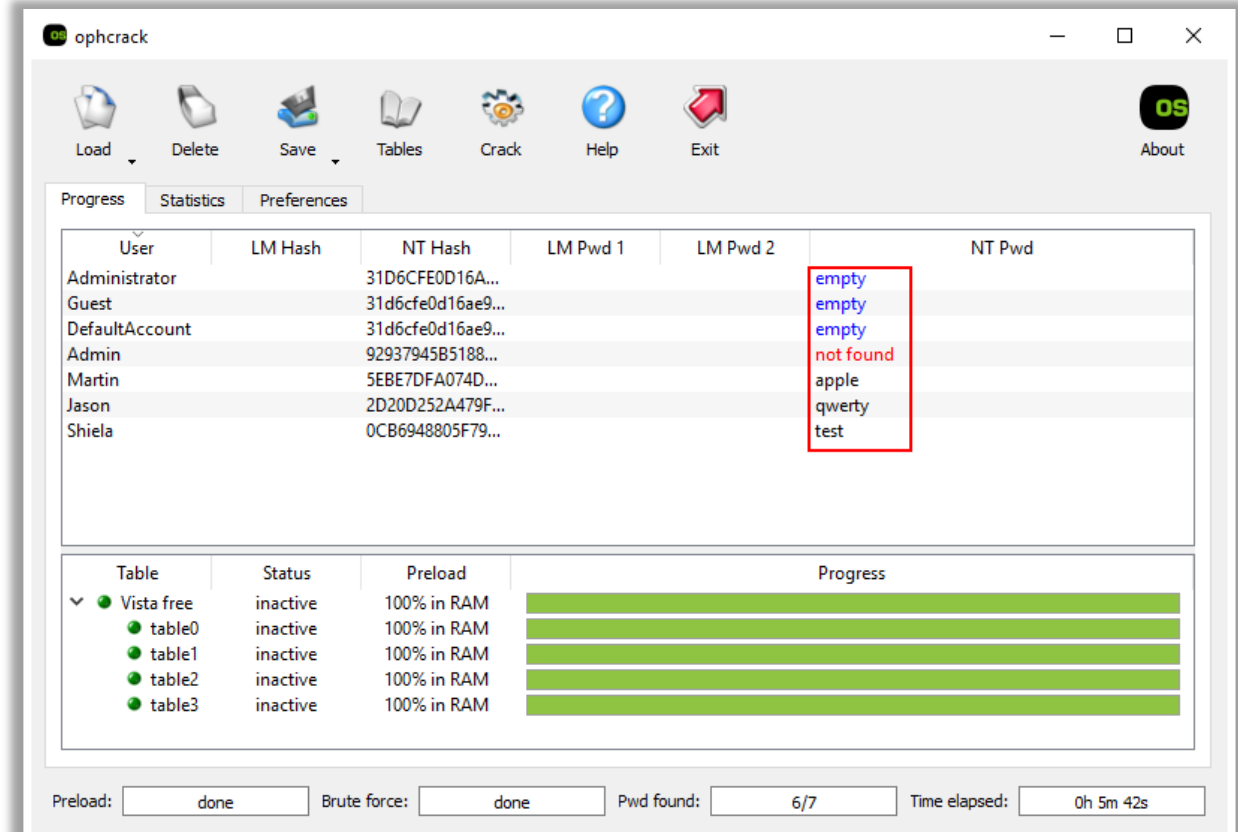
A tool designed to **audit passwords** and recover applications



<https://www.l0phtcrack.com>

ophcrack

A Windows password cracker based on **rainbow tables**. It comes with a Graphical User Interface and runs on multiple platforms



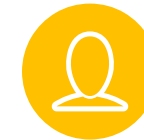
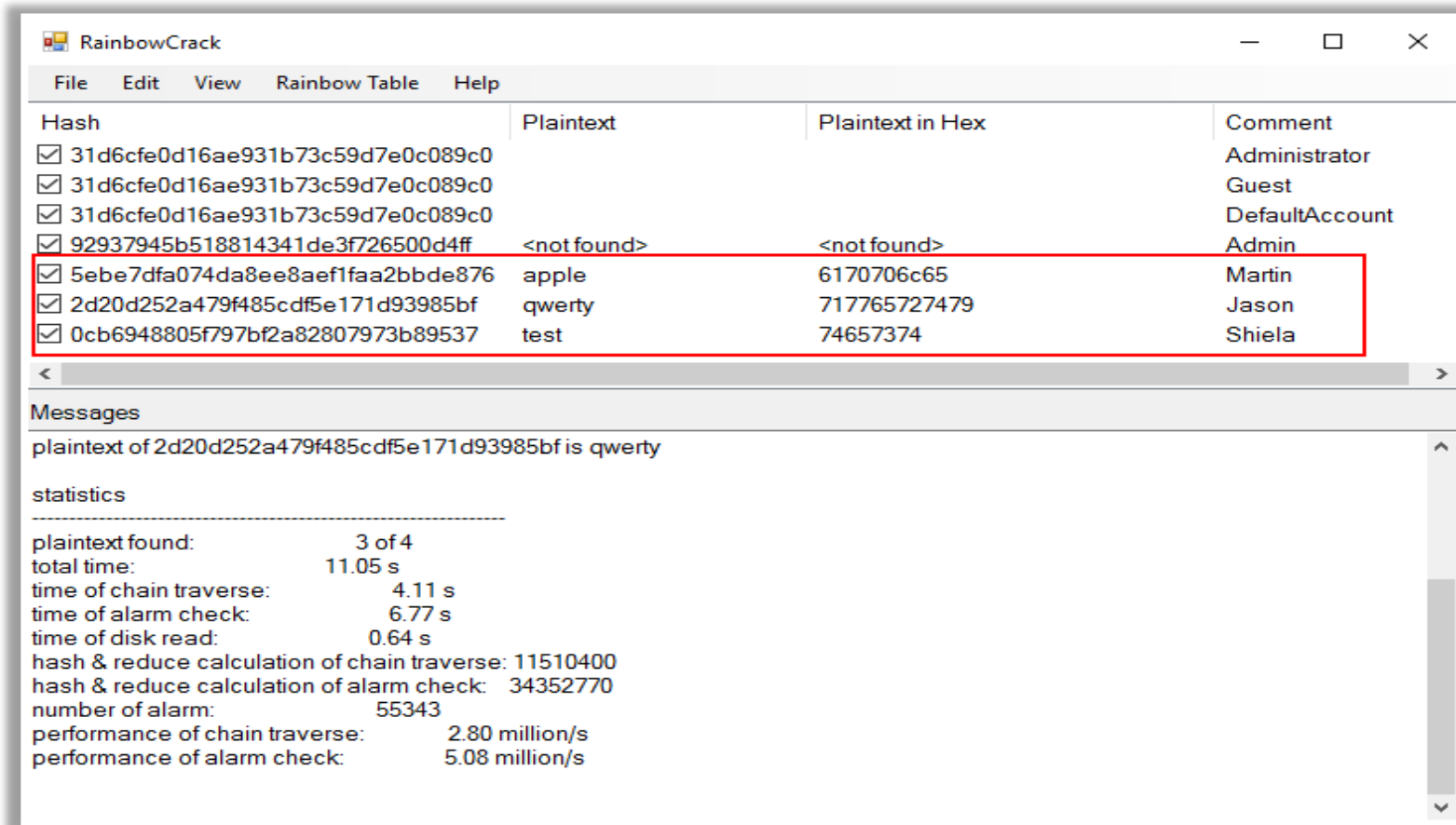
<https://ophcrack.sourceforge.io>

Password-Cracking Tools



RainbowCrack

RainbowCrack cracks hashes with **rainbow tables**. It uses a **time-memory tradeoff** algorithm to crack hashes



John the Ripper

<https://www.openwall.com>



hashcat

<https://hashcat.net>



THC-Hydra

<https://github.com>



Medusa

<http://foofus.net>

<http://project-rainbowcrack.com>

Module Flow



1

Discuss Password Cracking Techniques

2

Discuss Password Cracking Tools

3

Discuss Password Cracking Countermeasures

Password Cracking Countermeasures

1

Disallow use of the **same password** during a password change

3

Disallow the use of passwords that can be found in a **dictionary**

5

Set the **password change policy** to 30 days

2

Disallow password **sharing**

4

Do not use **cleartext** protocols and protocols with **weak encryption**

6

Do not use any system **default passwords**



Password Cracking Countermeasures (Cont'd)

7

Make passwords hard to guess by requiring **8-12 alphanumeric** characters consisting of a combination of uppercase and lowercase letters, numbers, and symbols

8

Ensure that applications **neither store** passwords in memory **nor write** them to disks in clear text

9

Use a **random string** (salt) as a prefix or suffix to the password before encryption

10

Disallow the use of passwords such as **date of birth**, spouse, child's, or pet's name

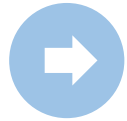
11

Lockout an account subjected to too many **incorrect password** guesses

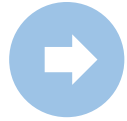
12

Use **two-factor or multi-factor authentication**, for example, using CAPTCHA to prevent automated attacks

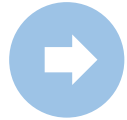
Module Summary



This module has discussed the password cracking and password complexity



It has covered the Microsoft authentication mechanisms



It also discussed in detail on various types of password attacks



It demonstrated on how to use password cracking tools



Finally, this module ended with a detailed discussion on various countermeasures against password attacks



In the next module, we will discuss in detail on various social engineering techniques and countermeasures