

# Introduction

**Module 8**



## Introduction

- System hacking is the way hackers get **access** to **individual** computers on a network. **Ethical** hackers learn system hacking to **detect, prevent, and counter** these types of attacks.
- It is the procedure of **obtaining unauthorized access** to a system and its resources, **exploiting the weaknesses** in a computer system.
- Generally use password **cracking**, **viruses**, **malware**, Trojans, worms, phishing techniques, email **spamming**, **social engineering**, exploit operating system **vulnerabilities**, to get access to any victim's system.



## Introduction



### Goals of System Hacking:

- ▷ Gaining Access
- ▷ Escalating privileges
- ▷ Executing applications
- ▷ Hiding files
- ▷ Clearing tracks



# Password Cracking

**Module 8**



## Password Cracking

- Password cracking techniques are **used to recover** passwords from computer systems.
- Attackers use password cracking **techniques to gain** unauthorized **access** to the **vulnerable** system.
- Most of the password cracking techniques are successful due to **weak or easily guessable** passwords.

# 1. Password Complexity

**Module 8**



## Password Cracking



### ■ Password Strength:

- 2015 annual public sector information security survey says “**Weak authentication** security is the leading cause of data breaches, accounting for **76% of compromised records**.”
- **Complexity** defines the character set used.
- **Length** is a crucial factor, **over complexity**, **c0mpl3x** can be cracked much **faster** than **thisismypasswrđ**.
- The **formula** is  **$\log(C) / \log(2) * L$**  where C is the size of the character set and L the length of the password



## 2. Types of Password Attacks

**Module 8**





## Password Cracking

- **Non-Electronic Attacks:** Attacker need **not posses technical knowledge** to crack password, hence known as non-technical attack.
  - ▷ **Shoulder Surfing**
  - ▷ **Social Engineering**
  - ▷ **Dumpster Diving**
- **Active Online Attacks:** Attacker performs password cracking **by directly communicating** with the victim machine.
  - ▷ **Dictionary** and Brute **Forcing** Attack
  - ▷ **Hash Injection** and Phishing
  - ▷ **Trojan/Spyware/Keyloggers**
  - ▷ Password **Guessing**



## Password Cracking

- **Passive Online Attacks:** Attacker performs password cracking **without communicating** with the authorizing party.
  - ▷ Wire Sniffing (Eavesdropping)
  - ▷ Replay
- **Offline Attack:** Attacker **copies the target's password** file and then tries to crack passwords in his own system at different location.
  - ▷ Pre-Computed Hashes (Rainbow Table)
  - ▷ Distributed Network



## Password Cracking



### Non-Electronic Attacks

- **Shoulder Surfing:** Looking at either the user's keyboard or screen while he/she is logging in.
- **Social Engineering:** Convincing people to reveal passwords
- **Dumpster Diving:** Searching for sensitive information at the user's trash-bins, printer trash bins, and user desk for sticky notes.



## Password Cracking



### Active Online Attack

- **Dictionary Attack:** A **dictionary file** is loaded into the cracking application that runs against user accounts.
- **Brute Forcing 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 Cracking



### Active Online Attack: Password Guessing

- The attacker creates a **list of all possible passwords** from the information collected through **social engineering** or any other way and **tries them manually** on the victim's machine to crack the passwords.
  - Find a **valid** user
  - Create a **list** of possible passwords
  - **Rank** passwords from **high probability to low**
  - **Key in each** password, until correct password is **discovered**.



## Password Cracking



### ■ 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 in the **list of words** or dictionary that they use to perform password guessing attack.



## Password Cracking



### Active Online Attack: Malware

- Attacker **installs Trojan/Spyware/Keylogger** on victim's machine to collect victim's user names and passwords.
- Trojan/Spyware/Keylogger **runs in the background** and **send back** all user credentials to the attacker.



## Password Cracking



### Example of Active Online Attack Using USB Drive

- ▷ Download PassView, a password hacking tool
- ▷ Copy the downloaded files to USB drive
- ▷ Create autorun.info in USB drive
  - ▷ [autorun]
  - ▷ en=launch.bat





## Password Cracking



- ▷ Contents of launch.bat
  - ▷ start pspv.exe /stext pspv.txt
- ▷ Insert the USB drive and the autorun window will pop-up (if enabled)
- ▷ PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive



## Password Cracking

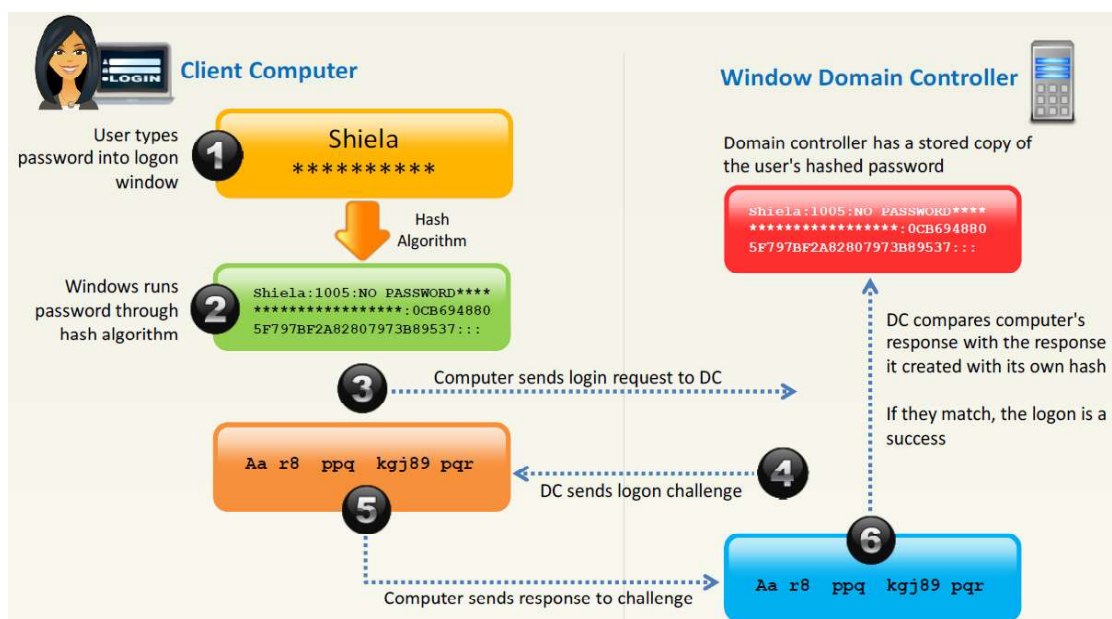


### Active Online Attack: Hash Injection Attack

- A hash injection/pass the hash attack allows an attacker to **inject a compromised hash into** a local **session** and use the hash to **validate to 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**.



## Password Cracking





## Password Cracking

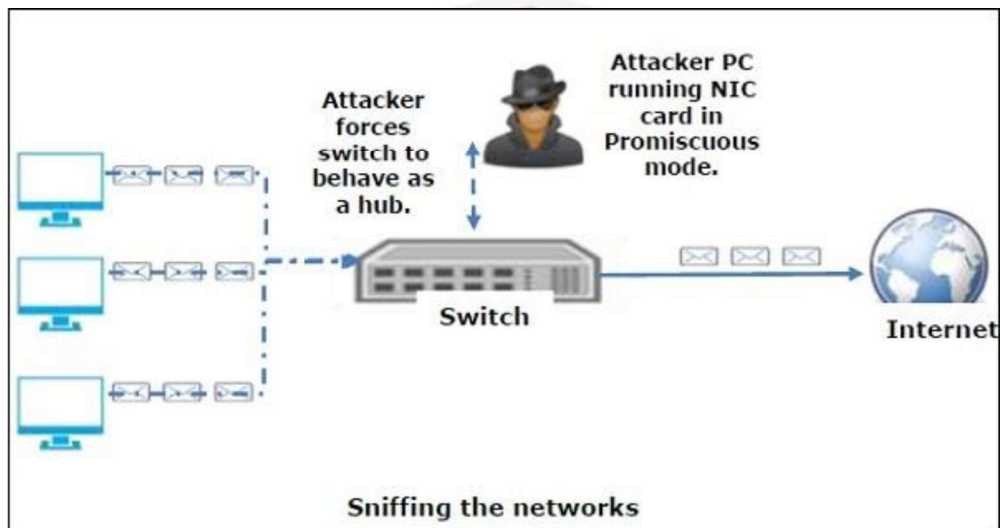


### Passive Online Attack: Wire Sniffing or Eavesdropping

- 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.



## Password Cracking



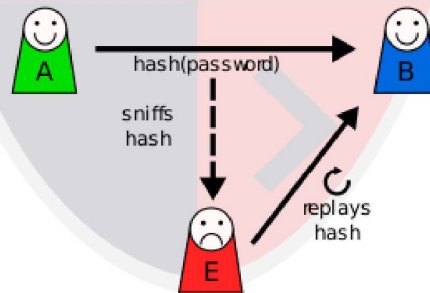


## Password Cracking



### Passive Online Attacks: Man-in-the-Middle and Replay Attack

- ▶ In a replay attack, packets and authentication tokens are **captured using a sniffer**. After the relevant info is extracted, the tokens are **placed back on the network** to gain access.





## Password Cracking



### Offline Attack: Rainbow Table Attack

- **Rainbow Table:** A rainbow table is a **precomputed table** which contains word lists like dictionary files and brute force lists and their **hash value**.
- **Compare the Hashes:** **Capture** the **hash** of a passwords and **compare** it with the precomputed **hash table**. If a match is found then the password is **cracked**.



## Password Cracking



■ **Easy to Recover:** It is **easy to recover** passwords by comparing captured password hashes to the precomputed tables.

■ **Precomputed Hashes:**

- ▷ 1qazwed -> 21c40e47dba72e77518ee3ef88ad0cc8
- ▷ hh021da -> 2ce80b192cfa47a0d6c8a2446314810b
- ▷ 9da8dasf -> eb0f5690164ffabbed1744087a4d6761
- ▷ sodifo8sf -> 2c749bf3fff89778efc50af7e4f8d6a8





## Password Cracking



### Tools to Create Rainbow Tables:

- **rtgen:** The rtgen program need **several parameters** to generate a rainbow table, the syntax of the command line is:
  - **Syntax:** rtgen hash\_algorithm charset plaintext\_len\_min plaintext\_len\_max table\_index chain\_len chain\_num part\_index
- **Winrtgen:** Winrtgen is a **graphical Rainbow Tables Generator** that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2(256), SHA-2(384), and SHA-2(512) hashes.



## Password Cracking



### Offline Attack: Distributed Network Attack

- A Distributed Network Attack (DNA) technique is used for recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords.
- The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network.

DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network.

DNA Client runs in the background, consuming only unused processor time.

# 3. Password Cracking with Keyloggers

Module 8



## Password Cracking

- A keylogger (also called as spy software) is a **small program** that **monitors** each and every **keystroke** a user types on a specific computer's **keyboard**.
- A keylogger program can be installed just in **a few seconds** and once installed you are only a step away from getting the victim's **password**.
- Once the keylogger is installed, it starts **operating in the background (stealth mode)** and captures every keystroke of the victim on that PC.
- The **victim** will **never come to know** about the presence of the keylogger on his/her computer as it runs in total stealth mode.