République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
ECOLE SUPÉRIEURE EN INFORMATIQUE
8 Mai 1945 - Sidi-Bel-Abbès

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
المدرسة العليا للإعلام الآلي
8 ماي 1945 - سيدي بلعباس

Cyber Security - Computer Science and Network Security

LAB SHEET 2 – Authentication in Practice

Exercise 1

This document provides a step-by-step solution for encrypting and decrypting a text file between a Kali VM (Student A) and a Metasploitable2 VM (Student B). The Metasploitable2 account used is 'msfadmin' password is: 'msfadmin' . All commands assume the VMs are on an isolated host-only network. Replace KALI_IP, META_IP with your actual values. kali_user: ‘root’, kali_password:’toor’.
Make sure SSH works between the VMs (start ssh service on Metasploitable2 if needed):

```
sudo service ssh start
```

A — Using GPG (asymmetric, recommended)

Goal: Kali = Student A (receiver). Metasploitable2 = Student B (sender who encrypts for A).

1) On Kali (Student A) — generate a GPG keypair

1. Run on Kali:

```
gpg --full-generate-key
```

Choose RSA, 1024 bits, expiry (0 = no expiry), name/email and a strong passphrase.

2) On Kali — export the public key (ASCII)

Run on Kali:

```
gpg --armor --export "Student A Name" > A_pub.asc #Name entered previously in question 1
ls -l A_pub.asc
```

3) Transfer A_pub.asc to Metasploitable2 (msfadmin)

From Kali, run (replace META_IP and kali_user as needed):

```
scp A_pub.asc msfadmin@META_IP:/home/msfadmin/
```

4) On Metasploitable2 (msfadmin) — import A's public key and verify

Run on Metasploitable2:

```
gpg --import /home/msfadmin/A_pub.asc
gpg --list-keys
gpg --fingerprint "Student A Name"
```

Verify the fingerprint out-of-band with Student A (phone or in person).

5) On Metasploitable2 — prepare the plaintext and encrypt for A

Run on Metasploitable2:

```
echo "This is a secret message from Metasploitable2 to Kali." > message.txt
gpg --encrypt --recipient "Student A Name" --armor -o message_for_A.asc
message.txt
ls -l message_for_A.asc
```

6) Transfer encrypted file back to Kali

From Metasploitable2 (msfadmin) run:

```
scp message_for_A.asc kali_user@KALI_IP:/home/kali_user/
```

7) On Kali — decrypt

Run on Kali:

```
gpg --decrypt /home/kali_user/message_for_A.asc > message_decrypted.txt
cat message_decrypted.txt
```

GPG will prompt for Student A's passphrase if the private key is protected.

Exercise 2 — Reconnaissance & discovery

Goal: Find authentication-related services on Metasploitable2.

Tasks :

1. From Kali, run a full port/service scan on Metasploitable2:
2. Identify authentication services and note ports (**add screenshot to report**).

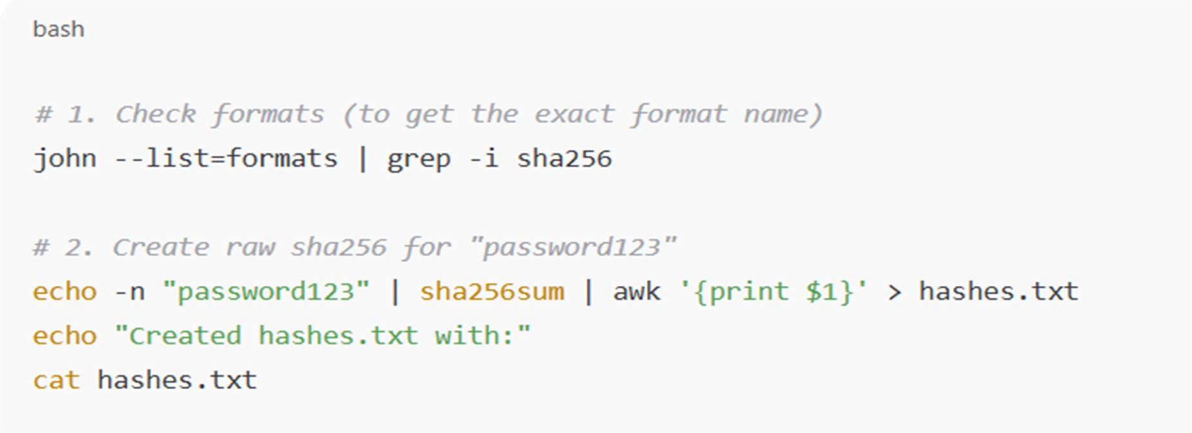
Exercise 3 — Simple hashing & cracking

Goal: Demonstrate that fast hashes (SHA-256) can be cracked using a wordlist.

Using John the Ripper (a favourite password cracking tool)

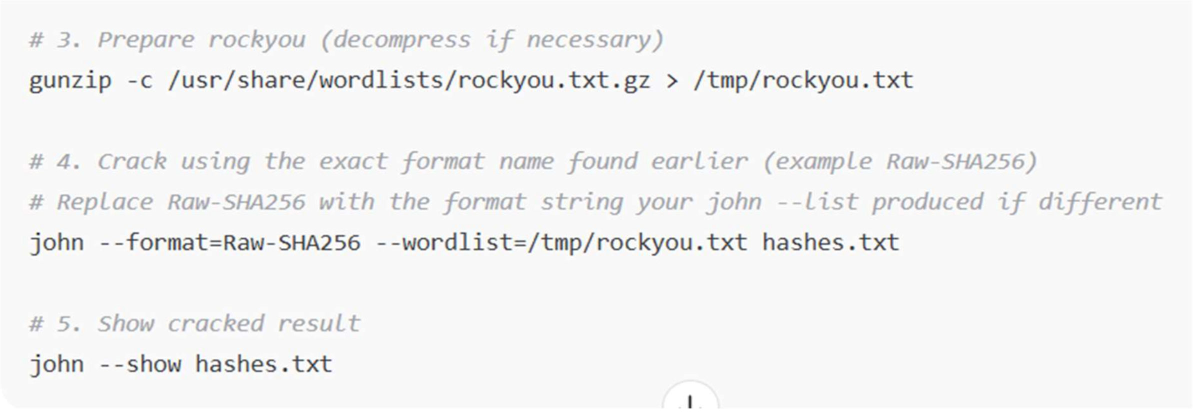
Student tasks (on Kali)

1. Compute SHA-256 of chosen password (example `password123`) and create a `hashes.txt` file in John format with a bash script



```bash
# 1. Check formats (to get the exact format name)
john --list=formats | grep -i sha256

# 2. Create raw sha256 for "password123"
echo -n "password123" | sha256sum | awk '{print $1}' > hashes.txt
echo "Created hashes.txt with:"
cat hashes.txt
```



```
# 3. Prepare rockyou (decompress if necessary)
gunzip -c /usr/share/wordlists/rockyou.txt.gz > /tmp/rockyou.txt

# 4. Crack using the exact format name found earlier (example Raw-SHA256)
# Replace Raw-SHA256 with the format string your john --list produced if different
john --format=Raw-SHA256 --wordlist=/tmp/rockyou.txt hashes.txt

# 5. Show cracked result
john --show hashes.txt
```

2. There are several solutions to fix the flaw. Name two solutions?
3. Try to fix the flaw with one of the solutions.

Exercise 4 — **Simulated online attack & defensive iptables rule.**

Goal: simulate a small brute-force using **`hydra`** tools and block the attacker's IP with `iptables`.

Steps / commands : knowing that in metasploitable2 the default user for ftp is msfadmin and the password is msfadmin**.**

1- Create a worldlist containing passwords known to the ftp service or easy passwords name the file**: passlist.txt.**

2- Launch a brute force attack to crack the FTP password of the Metasploitble machine using the Hydra tool following this command**: hydra -l msfadmin –P WORLDLIST_NAME ftp://IP_METASPLOITBLE -t 4**

You should have this output : **target successfully completed, 1 valid password found**

3- On Metasploitable2, block Kali IP using iptable.

4- Re-run Hydra from Kali and observe that attempts are blocked / time out.

Deliverables & Submission checklist for report

Students should submit the following: A short report contains:

1. Screenshots of key commands and outputs for each exercise.
2. The encrypted file produced (.asc,).
3. The decrypted plaintext file as proof of successful decryption.
4. Public key fingerprint of the sender and description of how they verified it.
5. The answers to exercise 3.