SURNAME	FIRST NAME	MATRICOLA	# of HWs

complete the Cybersecurity assignment by using this sheet – don't write in small letters and in case of bad handwriting use block letters

1. [0 – 4] What are the main differences between keyed hashing and unkeyed hashing? What are the consequences in terms of digital information security?

2. [0 – 5] Explain why it may be not secure to simply send an encrypted password for authentication. In particular, some precautions are needed. Discuss.

3. [0 – 4] Precisely analyze the following OpenSSL command lines: explain the purpose of each option included

```
openssl enc -d -aes-256-cbc -in text.txt.enc -out text.txt
openssl dgst -sha256 -verify public_key.pem -signature sign.bin message.txt
openssl x509 -in cert.pem -text -noout
```

Be accurate.

turn the sheet

complete the assignment by using this sheet – don't write in small letters and in case of bad handwriting use block letters

4. [0 – 3] Provide the mathematical expression of RSA encryption and decryption

5. [0 – 5] Suppose a LAN uses whitelist as the default policy; changing this default is not allowed. Write iptables rules that allow bidirectional communication between LAN host 1.2.3.4 and external host 255.254.253.252. The rule should minimize side effects and be as restrictive as possible

6. [0 – 3] Same setting of whitelisting. In detail, explain the meaning of the following

```
iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --sport 1024:5999 --dport 22 -m
conntrack --ctstate NEW -j ACCEPT
iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --sport 7001:65535 --dport 22 -m
conntrack --ctstate NEW -j ACCEPT
```

7. [0 – 4] Describe the Man-In-The-Middle attack and some ways for mitigating it.

8. [0 – 5] Algorithmically describe the high-level steps for running an offline dictionary attack to the passwords.

1. [0 – 4] What are the main differences between keyed hashing and unkeyed hashing? What are the consequences in terms of digital information security?

KEYED AND UNKEYED HASHING DIFFER MAINLY IN THE SECURITY GUARANTEES THEY PROVIDE:

AN UNKEYED HASH FUNCTION (LIKE SHA-256) TAKES ONLY THE MESSAGE AS INPUT AND PRODUCES A DIGEST THAT CAN BE RECOMPUTED BY ANYONE. THIS ENSURES INTEGRITY AGAINST ACCIDENTAL MODIFICATIONS, BUT IT DOESN'T PROVIDE AUTH, SO AN ATTACKER WHO ALTERS THE MESSAGE CAN ALSO RECOMPUTE THE DIGEST.

A KEYED HASH (HMAC) COMBINES THE MESSAGE WITH A SECRET KEY BEFORE APPLYING THE HASH FUNCTION, SO ONLY PARTIES KNOWING THE KEY CAN GENERATE OR VERIFY THE CORRECT TAG.

THE CONSEQUENCE IS THAT UNKEYED HASHING IS SUITABLE FOR DETECTING RANDOM ERRORS OR COMPARING FILE INTEGRITY, WHILE KEYED HASHING ADDITIONALLY ENSURES MESSAGE AUTH AND PROTECTS AGAINST ACTIVE TAMPERING.

2. [0 – 5] Explain why it may be not secure to simply send an encrypted password for authentication. In particular, some precautions are needed. Discuss.

ENCRYPTION ALONE DOESN'T PREVENT REPLAY ATTACK. IF AN ATTACKER CAPTURES THE ENCRYPTED PASSWORD WHILE IT'S TRANSMITTED, THEY CAN RESEND IT LATER WITHOUT NEEDING TO KNOW THE ORIGINAL PASSWORD. MOREOVER, IF THE ENCRYPTION KEY OR ALGORITHM IS WEAK, THE ATTACKER MIGHT DECRYPT THE CAPTURED VALUE.

TO PREVENT THESE THREATS, AUTH PROTOCOLS USE ADDITIONAL PRECAUTIONS SUCH AS NONCES OR CHALLENGE.

SECURE SYSTEMS ALSO AVOID TRANSMITTING RAW OR STATIC PASSWORDS AT ALL, PREFERRING PASSWORD-DERIVED KEYS, SALTED HASHES, OR STRONGER PROTOCOLS (TLS).

3. [0 – 4] Precisely analyze the following OpenSSL command lines: explain the purpose of each option included

```
openssl enc -d -aes-256-cbc -in text.txt.enc -out text.txt
openssl dgst -sha256 -verify public_key.pem -signature sign.bin message.txt
openssl x509 -in cert.pem -text -noout
```

1) THIS COMMAND DECRYPTS A FILE ENCRYPTED WITH AES-256 IN CBC MODE.
- -d SPECIFIES DECRYPTION
- -AES-256-CBC SELECT THE CIPHER
- -IN GIVES THE ENCRYPTED INPUT FILE
- -OUT SPECIFIES THE PLAINTEXT OUTPUT

2) THIS COMMAND VERIFIES A DIGITAL SIGNATURE.
- -SHA256 DEFINES THE HASH FUNCTION
- -VERIFY TOGETHER WITH A PUBLIC KEY CHECKS THE SIGNATURE IN SIGN.BIN AGAINST THE MESSAGE MESSAGE.TXT, ENSURING BOTH AUTHENTICITY AND INTEGRITY.

3) THIS COMMAND DISPLAYS THE CONTENT OF AN X 509 CERTIFICATE.
- -TEXT PRINTS THE HUMAN-READBLE FIELDS
- -NOOUT AVOIDS PRINTING THE BASE 64 PEM ENCODING

4. [0 – 3] Provide the mathematical expression of RSA encryption and decryption

IN RSA, THE PUBLIC KEY IS (n, e) AND THE PRIVATE KEY IS (n, d), WITH $n = p \cdot q$, $\varphi(n) = (p-1)(q-1)$ AND $ed = 1 \bmod \varphi(n)$
THE ENCRYPTION OF A MESSAGE m IS GIVEN BY $c = m^e \bmod n$, WHILE THE DECRYPTION IS $m = c^d \bmod n$.
CORRECTNESS FOLLOWS FROM EULER'S THEOREM, SINCE RAISING TO THE POWER $ed \bmod n$ RETURNS THE ORIGINAL MESSAGE.

5. [0 – 5] Suppose a LAN uses whitelist as the default policy; changing this default is not allowed. Write iptables rules that allow bidirectional communication between LAN host 1.2.3.4 and external host 255.254.253.252. The rule should minimize side effects and be as restrictive as possible

SINCE THE DEFAULT POLICY IS WHITELIST (DROP), WE MUST EXPLICITLY ALLOW TRAFFIC ONLY BETWEEN THE TWO SPECIFIED HOSTS. ONE ALLOWS FORWARDING FROM LAN HOST 1.2.3.4 TO EXTERNAL HOST 255.254.253.252, AND THE OTHER ALLOWS THE REVERSE DIRECTION.

```
IPTABLES -A FORWARD -S 1.2.3.4 -d 255.254 253.252 -j ACCEPT

IPTABLES -A FORWARD -S 255.254 253.252 -d 1.2.3.4 -j ACCEPT
```

THUS ONLY BIDIRECTIONAL COMMUNICATION BETWEEN THESE TWO IP ADDRESSES IS ENABLED, WHILE ALL OTHER TRAFFIC REMAINS BLOCKED.

6. [0 – 3] Same setting of whitelisting. In detail, explain the meaning of the following

```
iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --sport 1024:5999 --dport 22 -m
conntrack --ctstate NEW -j ACCEPT
iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --sport 7001:65535 --dport 22 -m
conntrack --ctstate NEW -j ACCEPT
```

THE TWO RULES ALLOW SSH ACCESS (PORT 22) FROM HOSTS IN THE LAN 192.168.1.0/24 THROUGH INTERFACE ETH1.
THE FIRST RULE ACCEPTS NEW TCP CONNECTIONS WHEN THE CLIENT USES A SOURCE PORT IN THE RANGE 1024 - 5999, WHILE THE SECOND RULE ACCEPTS NEW CONNECTIONS WHEN THE CLIENT USES A SOURCE PORT IN THE RANGE 7001 - 65535.
`-m conntrack --ctstate NEW` ENSURES THAT ONLY NEW CONNECTION ATTEMPTS ARE ALLOWED.

[0 – 4] Describe the Man-In-The-Middle attack and some ways for mitigating it.

MITM ATTACK OCCURS WHEN AN ADVERSARY SILENTLY INTERPOSES BETWEEN TWO PARTIES AND RELAYS / ALTER MESSAGES SO EACH SIDE BELIEVES IT'S TALKING DIRECTLY TO THE OTHER. WITHOUT AUTHENTICATION, THE ATTACKER CAN EAVESDROP, MODIFY DATA, INJECT COMMANDS, OR HARVEST CREDENTIALS.
TO MITIGATE IT, SYSTEMS MUST ENSURE AUTHENTICATION AND INTEGRITY OF COMMUNICATIONS: USE STRONG ENCRYPTION WITH AUTHENTICATED KEY EXCHANGE OR ENABLE HTTPS WITH HSTS TO PREVENT DOWNGRADE.

[0 – 5] Algorithmically describe the high-level steps for running an offline dictionary attack to the passwords.

THIS ATTACK CONSISTS OF TESTING CANDIDATE PASSWORDS AGAINST STORED PASSWORD HASHES WITHOUT INTERACTING WITH THE SYSTEM.

1. OBTAIN THE PASSWORD DB
2. FOR EACH CANDIDATE PASSWORD p IN A DICTIONARY OF COMMON PASSWORDS:
   a. IF A SALT IS USED, COMBINE p WITH THE CORRESPONDING SALT
   b. COMPUTE THE HASH OF THE CANDIDATE
   c. COMPARE THE RESULT WITH THE STORED HASH
3. IF A MATCH IS FOUND, p IS THE RECOVERED PASSWORD

SINCE THIS IS DONE OFFLINE, THE ATTACKER CAN TRY MANY TIMES WITHOUT BEING DETECTED.