University of Echahid Hamma Lakhdar
Faculty of Exact sciences
Level: 1st year IoT&Cyber Security Master degree

Module: Information Security.
Date: 07-01- 2024.
Duration: 1 hr, 30 mins.

Final Exam

Exercise 1: (05 pts)

A. In a Web Application, a user submits input in a login form. The input contains the following:

```
'<script>alert("Hacked!");</script>'
```

1) Explain what type of vulnerability this demonstrates.
2) How can developers secure their web applications to prevent such attacks?
3) What are the differences between persistent and non-persistent XSS attacks?

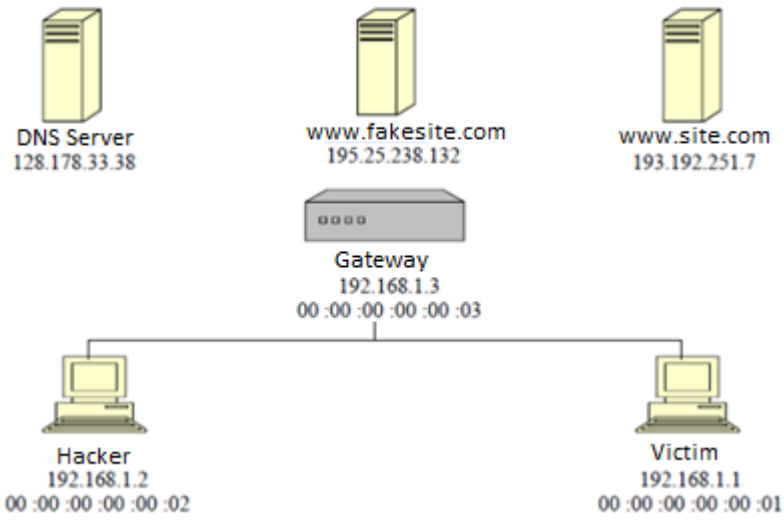
B. A function susceptible to stack buffer overflow is implemented as follows:

```
void processUserInput(char *input) {
    char localBuffer[12];
    strcpy(localBuffer, input); // No bounds checking
}
```

1) Identify the security flaw in the function and explain how an attacker can exploit it.
2) Describe how the stack layout changes during a stack buffer overflow attack.

Exercise 2: (04 pts)

Let's consider the following schema.



1) Explain in detail how can the hacker perform an *ARP-spoofing* attack and become a Man in the middle?
2) The victim wants to access to site.com. How can the hacker exploit the *Domain Name System* to redirect the victim to fakesite.com?
   Note: Use MAC and IP addresses from the schema in your answers.

Exercise 3: (-Lab session-07 pts)

1. Explain the differences between **encryption, encoding, and hashing**, and provide scenarios where each would be appropriately used.
2. Identify and describe three psychological techniques commonly used in **social engineering** attacks.
3. Which tools can be used to detect packet **sniffing** activities on your network?
4. Describe the steps that would be taken to verify the authenticity of an email and determine if it is a **phishing** attempt.
5. What are the measures that protects the user against **stolen credentials**?

Exercise 4: (04 pts)

Ali wants to send a secure message to Bachir ensuring its **integrity, confidentiality, and non-repudiation**.

1. What are the **security mechanisms** that Ali can use for each service?
2. Explain in schema how Ali proceeds before sending the message and how Bachir reacts upon receiving the message to ensure the three services.

تمرين 1:

1. شرح نوع الثغرة التي يمثلها هذا المثال.
2. كيف يمكن للمطورين تأمين تطبيقاتهم Web لمنع مثل هذه الهجمات؟
3. ما الفرق بين هجمات **persistent** XSS و **non-persistent**؟

1. حدد الثغرة الأمنية في الدالة واشرح كيف يمكن للمهاجم استغلالها.
2. صف كيف يتغير محتوى **stack** أثناء هجوم **stack buffer overflow**.

تمرين 2

1. اشرح بالتفصيل كيف يمكن للمخترق تنفيذ هجوم **ARP-spoofing** ليصبح **Man in the Middle**؟
2. يريد الضحية الوصول إلى **site.com**. كيف يمكن للمخترق استغلال **Domain Name System** لإعادة توجيه الضحية إلى **fakesite.com**؟

ملاحظة: استخدم عناوين **MAC** و **IP** من المخطط في إجاباتك.

تمرين 3:

- اشرح الفروقات بين **encryption** و **encoding** و **hashing**، واذكر سيناريوهات يكون فيها استخدام كل منها مناسبًا.
- حدد وصف ثلاث تقنيات نفسية تُستخدم عادةً في هجمات **social engineering**.
- ما الأدوات التي يمكن استخدامها لاكتشاف أنشطة **packet sniffing** على الشبكة؟
- صف الخطوات التي يمكن اتخاذها للتحقق من صحة مصدر بريد إلكتروني وتحديد ما إذا كان محاولة **phishing**.
- ما الإجراءات التي تحمي المستخدم من سرقة بيانات الاعتماد؟

تمرين 4

يريد علي إرسال رسالة آمنة إلى بشير مع ضمان سلامتها وسريتها وعدم الإنكار.

1. ما هي الآليات الأمنية التي يمكن لعلي استخدامها لتوفير كل خدمة؟
2. اشرح في مخطط كيف يتصرف علي قبل إرسال الرسالة وكيف يتفاعل بشير عند استلامها لكي يضمنا إكتمال الخدمات الثلاثة.

Correction

Exercise 1: (05 pts)

C. In a Web Application, a user submits input in a login form. The input contains the following:

```
'<script>alert("Hacked!");</script>'
```

1) Explain what type of vulnerability this demonstrates.
   This demonstrates a Reflected XSS attack.
2) How can developers secure their web applications to prevent such attacks?

   Developers can prevent it by Escaping special characters in user input (e.g., <, >, &) and Validating and sanitizing inputs.

3) What are the differences between persistent and non-persistent XSS attacks?

   Persistent XSS (Stored XSS): The malicious script is permanently stored on the target server (e.g., in a database) and is executed whenever a victim accesses the affected page.

   Non-persistent XSS (Reflected XSS): The malicious script is not stored on the server. It is included in the URL or a user input and executed immediately upon interaction by the victim.

D. A function susceptible to stack buffer overflow is implemented as follows:

```c
void processUserInput(char *input) {
    char localBuffer[12];
    strcpy(localBuffer, input); // No bounds checking
}
```

1) Identify the security flaw in the function and explain how an attacker can exploit it.
   The function does not perform bounds checking when copying user input into localBuffer. This allows an attacker to overwrite the stack's return address.
2) Describe how the stack layout changes during a stack buffer overflow attack.
   The attacker can provide an input longer than 12 characters, overwriting the return address with a pointer to malicious code.

Exercise 2: (04 pts)

Let's consider the following schema.

1) Explain in detail how can the hacker perform an *ARP-spoofing* attack and become a Man in the middle?
   The hacker sends gratuitous ARP replies to both the gateway and the victim. The hacker claims that its MAC address (00:00:00:00:00:02) corresponds to both the gateway's IP (192.168.1.3) and the victim's IP (192.168.1.1). This poisons the ARP cache of both devices, making the victim send its traffic to the hacker instead of the gateway. Similarly, the gateway sends its traffic destined

for the victim to the hacker. The hacker can now intercept, modify, or forward the traffic, becoming a Man in the Middle.

2) The victim wants to access to site.com. How can the hacker exploit the *Domain Name System* to redirect the victim to fakesite.com?
The hacker can intercept the victim's DNS request for site.com and respond with a forged DNS reply, providing the IP address of fakesite.com instead of site.com. For example:

- **The victim sends a DNS query to resolve site.com.**
- **The hacker responds with a DNS reply stating that site.com resolves to the IP address of fakesite.com (195.25.238.132).**
- **The victim's browser connects to 195.25. 238.132, displaying the malicious site fakesite.com instead of the legitimate site.com.**

Exercise 3: (-Lab session-07 pts)

1. Explain the differences between **encryption, encoding, and hashing**, and provide scenarios where each would be appropriately used.

Encryption: Converts plaintext to ciphertext to ensure data confidentiality. Used in secure communications, like HTTPS.

Encoding: Transforms data into a different format for specific purposes, such as UTF-8 encoding for text transmission.

Hashing: Creates a fixed-length hash from input data to ensure data integrity. Used in password storage and integrity checks.

2. Identify and describe three psychological techniques commonly used in **social engineering** attacks.

Authority: Attackers impersonate figures of authority to exploit victims' natural tendency to obey authority figures.

Urgency: Creates a sense of urgency or panic to pressure victims into making hasty decisions without proper verification.

Social Proof: Suggests that others are doing something, encouraging the victim to follow suit.

3. Which tools can be used to detect packet **sniffing** activities on your network?
WireShark, Nmap.
4. Describe the steps that would be taken to verify the authenticity of an email and determine if it is a **phishing** attempt.
To verify the authenticity of an email and determine if it is a phishing attempt, I would:
    - **Verify the sender's email address**
    - **Check for spelling errors in the email content**
    - **Analyse URLs for misspelled domains**
5. What are the measures that protects the user against **stolen credentials**?
    - **Using Two-Factor Authentication (2FA)**
    - **Avoiding password reuse across accounts**
    - **Using a password manager**

Exercise 4: (04 pts)

Ali wants to send a secure message to Bachir ensuring its **integrity, confidentiality, and non-repudiation**.

1. What are the **security mechanisms** that Ali can use for each service?

Security services	Mechanism
Non repudiation	Digital signature
Confidentiality	Encryption
Integrity	Hashing algorithm

2. Explain in schema how Ali proceeds before sending the message and how Bachir reacts upon receiving the message to ensure the three services.