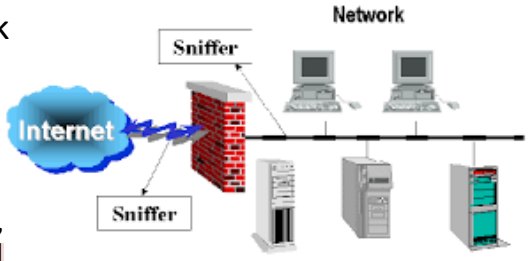
Chapter 3: Sniffers

- Understanding Network Sniffing
- Types of Network Sniffers
- Sniffing Techniques and Protocols
- Implications and Risks of Network Sniffing
- Mitigation and Prevention

Understanding Network Sniffing Definition

- Network sniffing is a technique that allows an attacker to **capture** and **analyze** network traffic.
- This can be done by placing a network **sniffer** on a network segment, or by using a remote **sniffing** tool.
- Once a network sniffer is in place, it can capture all of the traffic that passes through the network segment, including **usernames**, **passwords**, and other **sensitive** information.



فهمشبكة التنصتتعريف

- استنشاقالشبكة هي تقنية تسمح للمهاجمين**يأسرو تحليل**ازدحام انترنت.
- يمكنالقيام بذلك عن طريق وضع شبكة **الشم**على جزء من الشبكة ، أو باستخدام جهازتحكم عن بعد**شم**أداة.
- بمجردوضع أداة التنصت على الشبكة ، يمكنهاالتقاط كل حركة المرور التي تمر عبرقطاع الشبكة ، بما في ذلك**أسماء المستخدمين**و**كلمات السر**، وغيرها **حساس**معلومة.

Understanding Network Sniffing Purpose

- Network sniffers can be used for a variety of purposes, including:
  - Penetration testing
  - Network monitoring
  - Law enforcement investigations

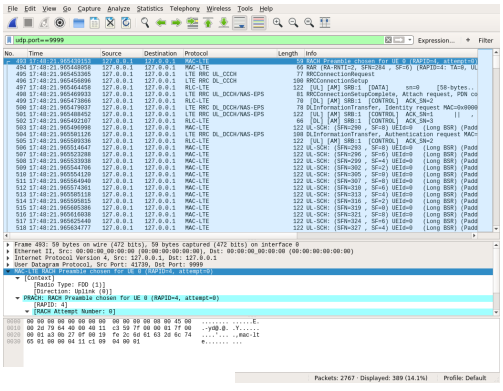
فهمشبكة التنصتغاية

- يمكناستخدام متشمم الشبكة لأغراض متنوعة ، بمافي ذلك:
  - اختبارالاختراق
  - شبكةالرصد
  - تحقيقاتإنفاذ القانون

32

Understanding Network Sniffing How it works

- Network sniffers work by capturing all of the packets that are sent and received on a network segment.
- Each packet contains a variety of information, including the **source** and **destination** addresses, the **type** of protocol, and the **data** payload.
- The network sniffer can then analyze this information to look for specific patterns, such as **usernames**, **passwords**, and other **sensitive** information.



فهمشبكة التنصتكيف تعمل

- يعملمتشممو الشبكة عن طريق التقاط جميعالحزم التي يتم إرسالها واستلامها على جزءالشبكة.
- تحتويكل حزمة على مجموعة متنوعة من المعلومات ،بما في ذلك ملف**مصدر**و **وجهة**عناوين**يكتب**البروتوكول ، و**بيانات** الحمولة.
- يمكنلمتصمم الشبكة بعد ذلك تحليل هذه المعلوماتللبحث عن أنماط معينة ، مثل **أسماءالمستخدمين**و**كلمات السر**، وغيرها **حساس**معلومة.

33

33

Types of Network Sniffers

- There are two main types of network sniffers:
  - Hardware sniffers
  - Software sniffers

أنواعمتشمم الشبكة

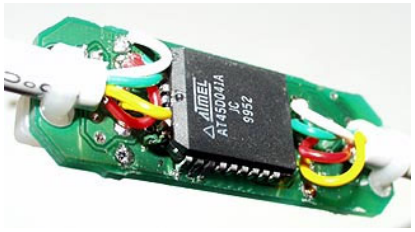
- هناكنوعان رئيسيان من متشمم الشبكة:
  - متشممالأجهزة
  - المتشممونالبرمجيات

34

34

Types of Network Sniffers Hardware sniffers

- Hardware sniffers are physical devices that are placed on a network **segment**.
- They are typically more **expensive** than software sniffers, but they can capture more traffic and provide more detailed information.



أنواعمتشمم الشبكةمتشمم الأجهزة

- متشمموالأجهزة عبارة عن أجهزة ماديةيتم وضعها على الشبكة **شريحة**.
- همعادة أكثر **غالي**من متلصصي البرامج ،لكن يمكنهم التقاط المزيد منحركة المرور وتقديم معلومات أكثرتفصيلاً.

35

Types of Network Sniffers Software sniffers

- Software sniffers are software **applications** that run on a computer.
- They are typically **less** expensive than hardware sniffers, but they can only capture traffic that **passes** through the computer that they are running on.

أنواعمتشمم الشبكةالمتشممون البرمجيات

- المتشممونالبرمجيات هم برمجيات **التطبيقات**التي تعمل على جهاز الكمبيوتر.
- هم عادة**أقل**باهظ الثمن من أجهزة التعرفعلى الأجهزة ، لكن يمكنهم فقطالتقاط حركة المرور التي **يمر، يمرر،اجتاز بنجاح**من خلال الكمبيوتر الذييتم تشغيلهم عليه.

36

Passive Network Sniffing Definition

- Passive network sniffing is a type of network sniffing in which the attacker **does not** alter the network traffic.
- This means that the attacker can only see the traffic that is sent and received, and they **cannot inject** their **own packets** into the traffic stream.

استنشاقالشبكة السلبيةتعريف

- استنشاقالشبكة الخاملة هو نوع من استنشاق الشبكة يكون فيه المهاجم **لا**تغيير حركة مرور الشبكة.
- هذايعني أن المهاجم يمكنه فقط رؤية حركة المرور المرسلة والمستلمة ،وهم**لا يمكن الحقن**هم**الحزم الخاصة**في تيار حركة المرور.

37

Passive Network Sniffing Characteristics

- Passive network sniffing is a relatively **easy** technique to perform.
- All that is required is a **network sniffer** that is placed on a network segment that contains the **traffic** that the attacker is interested in.

- يعتبراستنشاق الشبكة السلبية أمراً نسبياً**سهل**تقنية لأداء.
- كل ما هو مطلوب هو أ**شبكة الشم**التي يتم وضعها على جزء الشبكة الذي يحتوي على**مرور**التي يهتم بها المهاجم.

38

38

Active Network Sniffing Definition

- Active network sniffing is a type of network sniffing in which the attacker **alters** the network traffic.
- This means that the attacker can see the traffic that is sent and received, and they can also **inject** their own packets into the traffic stream.

استنشاق الشبكة النشطةتعريف

- استنشاق الشبكة النشط هو نوع من استنشاق الشبكة يكون فيه المهاجم**يغير**حركة مرور الشبكة.
- هذا يعني أن المهاجم يمكنه رؤية حركة المرور التي يتم إرسالها واستلامها ، ويمكنه أيضاً**حقن**الحزم الخاصة بهم في تدفق حركة المرور.

39

39

Active Network Sniffing Characteristics

- Active network sniffing is a more **complex** technique to perform than passive network sniffing.
- This is because the attacker **must** first find a way to alter the network traffic.
- Once the attacker has found a way to alter the network traffic, they can then **inject** their own packets into the traffic stream.

- يعداستنشاق الشبكة النشط أكثر من ذلك**معقد**تقنية لأداء من استنشاق الشبكةالسلبي.
- هذاالأن المهاجم**يجب**أولاً إيجاد طريقة لتغيير حركة مرور الشبكة.
- بمجردأن يجد المهاجم طريقة لتغيير حركة مرور الشبكة ، يمكنه ذلك**حقن** الحزمالخاصة بهم في تدفق حركة المرور.

40

40

Sniffing Techniques and Protocols

- There are a variety of common sniffing techniques that attackers use, including:
  - ARP spoofing
  - DNS poisoning
  - MAC flooding

تقنياتوبروتوكولات الشم

- هناكمجموعة متنوعة من تقنيات الاستنشاق الشائعةالتي يستخدمها المهاجمون ، بما في ذلك:
  - انتحالARP
  - تسممDNS
  - الفيضاناتMAC

41

Protocols often targeted by sniffing attacks

- There are a variety of protocols that are often targeted by sniffing attacks, including:
  - HTTP
  - FTP
  - SMTP

غالبأما تستهدف البروتوكولات بهجمات الاستنشاق

- هناكمجموعة متنوعة من البروتوكولات التي غالباً ما يتم استهدافهابواسطة هجمات الاستنشاق ، بما في ذلك:
  - HTTP
  - بروتوكولنقل الملفات
  - SMTP

42

الأثار والمخاطر

Implications and Risks of Network Sniffing

- **Data theft**: Attackers can use network sniffing to steal sensitive data, such as passwords, credit card numbers, and social security numbers.
- **Identity theft**: Attackers can use network sniffing to steal a user's identity and impersonate them.
- **Denial of service**: Attackers can use network sniffing to disrupt a user's service by flooding the network with traffic.
- **Malware infection**: Attackers can use network sniffing to infect a user's computer with malware.

تداعياتومخاطر استنشاق الشبكة

- **سرقةالبيانات**: يمكن للمهاجمين استخدام الاستنشاق عبر الشبكة لسرقة البيانات الحساسة ،مثل كلمات المرور وأرقام بطاقات الائتمان وأرقام التأمين الاجتماعي.
- **سرقةالهوية**: يمكن للمهاجمين استخدام استنشاق الشبكة لسرقة هوية المستخدموانتحال شخصيته.
- **الحرمانمن الخدمة**: يمكن للمهاجمين استخدام تقنية استنشاق الشبكة لتعطيلخدمة المستخدم عن طريق إغراق الشبكة بحركة المرور.
- **الإصابةبالبرامج الضارة**: يمكن للمهاجمين استخدام استنشاق الشبكة لإصابة كمبيوترالمستخدم ببرامج ضارة.

43

Mitigation strategies

- **Use strong passwords**: Strong passwords make it more difficult for attackers to guess passwords and gain access to accounts.
- **Enable two-factor authentication**: Two-factor authentication adds an extra layer of security by requiring users to enter a code from their phone in addition to their password.
- **Use secure protocols**: Secure protocols, such as HTTPS, encrypt data in transit, making it more difficult for attackers to steal data.
- **Keep software up to date**: Software updates often include security patches that can help to protect against known vulnerabilities.
- **Be aware of the risks of public Wi-Fi**: Public Wi-Fi networks are often not secure, so it is important to be careful about what information you share when using them.

44

استراتيجياتالتخفيف

- **استخدمكلمات مرور قوية**: تجعل كلمات المرور القوية من الصعب على المهاجمينتخمين كلمات المرور والوصول إلى الحسابات.
- **قمبتمكين المصادقة الثنائية**: تضيف المصادقة ذات العاملين طبقة إضافية منالأمان من خلال مطالبة المستخدمين بإدخال رمز من هواتفهم بالإضافة إلى كلمةالمرور الخاصة بهم.
- **إستخدمبروتوكولات آمنة**: تقوم البروتوكولات الآمنة ، مثل HTTPS ، بتشفير البيانات أثناءالنقل ، مما يزيد من صعوبة سرقة البيانات على المهاجمين.
- **حافظعلى تحديث البرنامج**: غالباً ما تتضمن تحديثات البرامج تصحيحات أمان يمكن أنتساعد في الحماية من الثغرات الأمنية المعروفة.
- **كنعلي دراية بمخاطر شبكات Wi-Fi العامة**: غالباً ما تكون شبكات Wi-Fi العامةغير آمنة ، لذا من المهم توخي الحذر بشأن المعلومات التي تشاركها عند استخدامها.

Conclusion

- It is important to be aware of the risks of network sniffing and to take steps to protect yourself.
- By following the mitigation strategies listed above, you can help to reduce your risk of being a victim of a network sniffing attack.

45

خاتمة

- منالمهم أن تكون على دراية بمخاطر استنشاقالشبكات وأن تتخذ خطوات لحمايةنفسك.
- باتباعاستراتيجيات التخفيف المذكورة أعلاه ،يمكنك المساعدة في تقليل مخاطرالوقوع ضحية لـ هجوماستنشاق الشبكة.

45

Chapter 4:

- What is cryptography?
- What is cryptanalysis?
- What is cryptology?
- Encryption Algorithms

What is cryptography?

- Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

ماهو التشفير؟

- علمالتشفير هو دراسة وتطبيق التقنيات التي تخفيالمعنى الحقيقي للمعلومات عن طريق تحويلهاإلى
التنسيقاتغير البشرية القابلة للقراءة والعكس صحيح.

What is cryptography? cont.

- Cryptography is used in a wide variety of applications, including:
  - Secure communication
  - Data protection
  - Authentication
  - Integrity verification
  - Non-repudiation

ماهو التشفير؟تابع

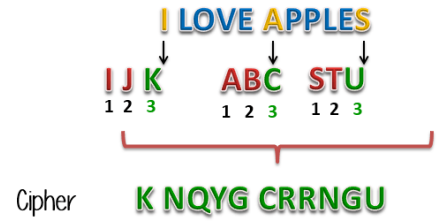
- يستخدمالتشفير في مجموعة متنوعة من التطبيقات ،بما في ذلك:
  - اتصالآمن
  - حمايةالبيانات
  - المصادقة
  - التحققمن النزاهة
  - عدمالتنصل

48

What is cryptography? cont.

- Suppose you want to send the message "**I LOVE APPLES**", you can replace every letter in the phrase with the third successive letter in the alphabet.
- The encrypted message will be "**K NQXG CRRNGV**".
- To decrypt our message, we will have to go back three letters in the alphabet using the letter that we want to decrypt.

Key: Replace every letter with 3rd successive letter



ماهو التشفير؟تابع

- لنفترضأنك تريد إرسال الرسالة " **احبالتفاح**". يمكنك استبدال كل حرففي العبارة بالحرف الثالث علىالتوالي في الأبجدية.
- ستكونالرسالة المشفرة " **K NQXG CRRNGV**".
- لفكتشفير رسالتنا ، سيتعين علينا العودةبثلاثة أحرف في الأبجدية باستخدامالحرف الذي نريد فك تشفيره.

49

49

Fundamentals of Encryption

- **Encryption** is the process of converting plaintext into ciphertext.
- **Ciphertext** is unreadable without the key.
- The **key** is a secret value that is used to **encrypt** and **decrypt** data.
- There are two main types of encryption: **symmetric** encryption and **asymmetric** encryption.

أساسياتالتشفير

- **التشفير**هي عملية تحويل النص العادي إلىنص مشفر.
- **نصمجفر**غير قابل للقراءة بدون المفتاح.
- ال**مفتاح**هي قيمة سرية يتم استخدامها **تشفير**و**فك تشفير**بيانات.
- هناكنوعان رئيسيان من التشفير: **متماثل** التشفيرو**غير متماثل** التشفير.

50

Symmetric Encryption

- Symmetric encryption uses the **same key** to encrypt and decrypt data.
- Symmetric encryption is **fast** and **efficient**, but it requires that the key be **shared** between the **sender** and **receiver**.
- Examples of symmetric encryption algorithms include:
  - Advanced Encryption Standard (AES)
  - Data Encryption Standard (DES)

التشفيرالمتماثل

- يستخدمالتشفير المتماثل الامتداد**نفس المفتاح**لتشفير وفك تشفير البيانات.
- التشفيرالمتماثل هو**سريع**و**فعال**، لكنه يتطلب أن يكون المفتاح**مشترك**بين ال**مرسل**و**المتلقي**.
- تتضمنأمثلة خوارزميات التشفير المتماثل ما يلي:
  - معيارالتشفير المتقدم (AES)
  - معيارتشفير البيانات (DES)

51

Asymmetric Encryption

- Asymmetric encryption uses two different keys: a **public** key and a **private** key.
- The **public** key can be used to **encrypt** data, but only the **private** key can be used to **decrypt** it.
- Asymmetric encryption is **slower** than symmetric encryption, but it does not require that the key be shared between the sender and receiver.
- Examples of asymmetric encryption algorithms include:
  - Rivest-Shamir-Adleman (RSA)
  - Diffie-Hellman

52

التشفيرغير المتماثل

- يستخدمالتشفير غير المتماثل مفتاحين مختلفين: **أعام**مفتاح و **خاص** مفتاح.
- ال**عام**يمكن استخدام المفتاح ل**تشفير**البيانات ، ولكن فقط**خاص**يمكن استخدام المفتاحل**فك تشفير**هو - هي.
- التشفيرغير المتماثل**أبطأ**من التشفير المتماثل ، لكنه لا يتطلب مشاركة المفتاحبين المرسل والمستقبل.

- تتضمنأمثلة خوارزميات التشفير غير المتماثل ما يلي:
  - ريفستشامير أدلمان (RSA)
  - ديفيهيلمان

Hashing

- **Hashing** is a **one-way** function that converts data into a **fixed-length** value.
- Hashes are used for a variety of purposes, including:
  - Data integrity verification
  - Digital signatures
  - Password hashing
- Hash functions are often used in **conjunction** with encryption to provide **additional** security.
- Examples of hash functions include:
  - Message Digest 5 (MD5)
  - Secure Hash Algorithm (SHA-256)

53

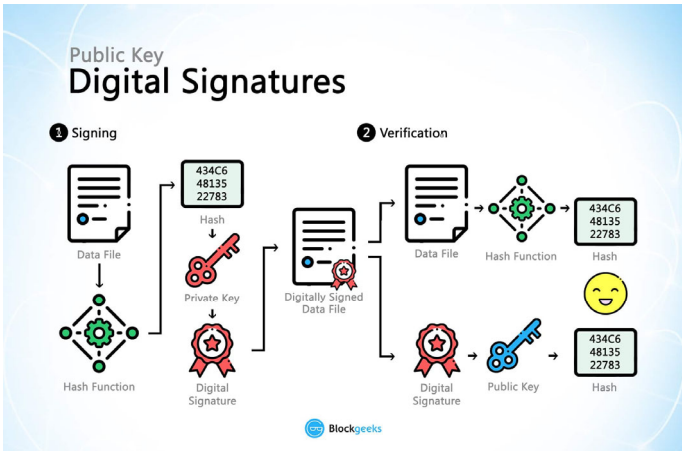
تجزئة

- **تجزئة**هو**طريقة واحدة**وظيفة تحول البيانات إلى ملف**طول ثابت** قيمة.

- تستخدمالتجزئة لأغراض متنوعة ، بما في ذلك:
  - التحققمن سلامة البيانات
  - التوقيعاتالرقمية
  - تجزئةكلمة المرور
- غالبًاما تستُخدم وظائِف التجزئة في ملفات**اقِتران**مع التشفير لتقديمه**إضافي**حماية.
- تتضمنأمثلة وظائف التجزئة ما يلي:
  - ملخصالرسالة 5 (MD5)
  - خوارزميةالتجزئة الآمنة (SHA-256)

Digital Signatures

- A digital signature is a **mathematical** scheme for verifying the **authenticity** of digital messages or documents.
- A digital signature is created by using a **private key** to encrypt a hash of the message or document.



54

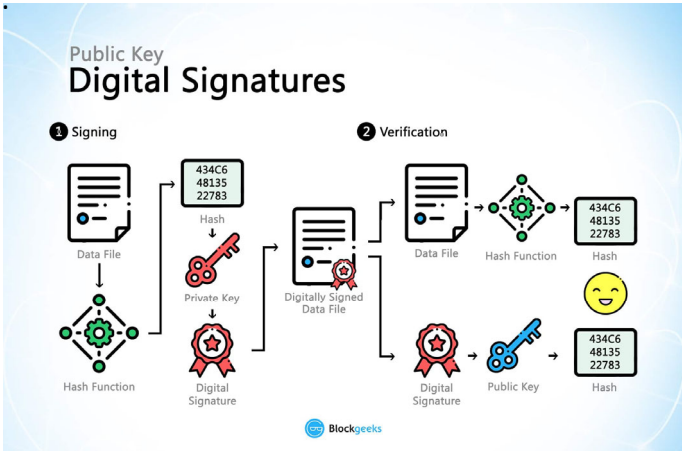
التوقيعاتالرقمية

- التوقيعالرقمي هو ملف **رياضي** مخططللتحقق من**أصالة**من الرسائلالرقمية أو وثائق.
- يتمإنشاء التوقيع الرقمي باستخدامملف**مفتاح سري** لتشفيرتجزئة للرسالة أو المستند.

54

Digital Signatures cont.

- The recipient can use the **public key** to **decrypt** the hash and verify that it matches the hash of the message or document.
- If the hashes do not match, then the message or document has been tampered with.



55

- يمكنللمستلم استخدام ملف **المفتاح العمومي**ل **فكتشفير**التجزئة وتحقق منتطابقها مع تجزئة الرسالةأو المستند.
- إذالم تتطابق التجزئات ، فستظهرالرسالة أو تمالعبث بالمستند.

55

Cryptographic Key Management

- Cryptographic key management is the process of **generating**, **storing**, **distributing**, and **using** cryptographic keys.
- Key management is a critical aspect of cryptography, as it is essential to ensure that keys are secure and that they are not compromised.

إدارةمفتاح التشفير

- إدارةمفتاح التشفير هي عملية**توليد**و **التخزين**و **توزيع**، و**استخدام**مفاتيح التشفير.
- تعدإدارة المفاتيح جانباً مهماً من جوانب التشفير ،حيث إنه من الضروري التأكد من أن المفاتيحآمنة وعدم المساومة عليها.

56

Cryptographic Key Management

- There are a variety of key management techniques, including:
  - Key generation
  - Key distribution
  - Key storage
  - Key usage

إدارةمفتاح التشفير

هناكمجموعة متنوعة من تقنيات الإدارة الرئيسية ،بما في ذلك:

- توليدالمفتاح
- التوزيعالرئيسي
- تخزينالمفاتيح
- استخدامالمفتاح

57

Cryptographic Attacks

- Cryptographic attacks are **attempts** to break cryptographic systems.
- There are a variety of cryptographic attacks, including:
  - Brute-force attacks
  - Dictionary attacks
  - Side-channel attacks
  - Fault attacks
- Cryptographic systems must be designed to resist these attacks.

هجماتالتشفير

- هجماتالتشفير هي**محاولات**لكسر أنظمة التشفير.
- توجدمجموعة متنوعة من هجمات التشفير ، بما في ذلك:
  - هجماتالقوة الغاشمة
  - هجماتالقاموس
  - هجماتالقنوات الجانبية
  - الهجماتالخاطئة
- يجبتصميم أنظمة التشفير لمقاومة هذه الهجمات.

58

Cryptographic Applications

- Cryptography is used in a wide variety of applications, including:
  - Secure communication
  - Data protection
  - Authentication
  - Integrity verification
  - Non-repudiation
- Cryptography is an essential tool for securing information.

تطبيقاتالتشفير

- يستخدمالتشفير في مجموعة متنوعة من التطبيقات ، بما في ذلك:
  - اتصالآمن
  - حمايةالبيانات
  - المصادقة
  - التحققمن النزاهة
  - عدمالتنصل
- التشفيرهو أداة أساسية لتأمين المعلومات.

59

59

Cryptographic Best Practices

- There are a number of best practices that can be followed to improve the security of cryptographic systems.
- These best practices include:
  - Using strong algorithms and key lengths
  - Keeping software and algorithms up to date
  - Using secure key management practices
  - Educating users about cryptography

أفضل ممارسات التشفير

- هناك عدد من أفضل الممارسات التي يمكن اتباعها لتحسين أمان أنظمة التشفير.
- تتضمن أفضل الممارسات ما يلي:
  - استخدام خوارزميات قوية وأطوال المفاتيح
  - تحديث البرامج والخوارزميات
  - استخدام ممارسات إدارة المفاتيح الآمنة
  - تثقيف المستخدمين حول التشفير

60

60

Conclusion

- Cryptography is a powerful tool that can be used to protect information.
- By following the best practices outlined in this lecture, you can help to ensure that your information is

https://alfecorona.medium.com/understanding-pki-public-key-infrastructure-for-information-security-414ef5fe4f9f

61

61