محور الشبكات – المحاضرة (3)

أمنية الشبكات: المفاهيم والأهداف وأدوات الحماية وبروتوكولات الأمان

Network Security: Concepts, Objectives, Defense Tools and Security Protocols

المرحلة	الثانية – الدراسة الصباحية	**المادة**	الحاسوب
الإعداد	أ.م.د. حيدر حسن محمد **م.م. اثير اسماعيل فاضل**	**المدة المقترحة**	ساعتان (نظري + نشاط)

أهداف المحاضرة (Learning Objectives)

بعد انتهاء المحاضرة يكون الطالب قادراً على أن:

1. يعرّف أمنية الشبكات (Network Security) ويميزها عن الأمن السيبراني وأمن المعلومات.
2. يشرح مثلث CIA وأهداف AAA وعدم الإنكار (Non-repudiation) بأمثلة.
3. يفرّق بين التهديد (Threat) والثغرة (Vulnerability) والمخاطر (Risk) ويطبّق معادلة المخاطر.
4. يتعرف على أدوات الدفاع: Firewall, IDS/IPS, VPN, Encryption, MFA, SIEM.
5. يفصّل بروتوكولات الأمان: TLS/HTTPS, SSH, IPsec, WPA2/WPA3, SFTP, DNSSEC.
6. يصمم خطة حماية مبسطة لشبكة نادٍ أو قاعة رياضية.

خارطة المحاضرة (Lecture Map)

المحور	العنوان	الجانب التطبيقي
1	مفهوم أمنية الشبكات وأهدافها (Concept & Objectives)	مثلث CIA
2	أهمية الأمن ومكوناته (Importance & Components)	إحصاءات وجداول
3	المخاطر والتهديدات والثغرات (Risk Management)	مصفوفة المخاطر
4	أدوات الدفاع (Defense Tools)	مقارنات
5	بروتوكولات الأمان بالتفصيل (Security Protocols)	بطاقات بروتوكولات
6	الدفاع بالعمق والأطر والمعايير (Defense in Depth & Standards)	NIST / ISO 27001
7	خطة حماية لشبكة نادٍ رياضي ونشاط عملي	جدول تطبيقي

أولاً: مفهوم أمنية الشبكات (Network Security Concept)

أمنية الشبكات (Network Security) هي مجموعة الإجراءات والتقنيات والسياسات المصممة لحماية البنية الحاسوبية للشبكة وما تنقله من بيانات من **الوصول غير المصرح به** و**التعديل** و**التعطيل** و**السرقة**. وتشمل أي نظام مترابط من الأجهزة (حواسيب، خوادم، هواتف) يتبادل البيانات عبر وسائط سلكية أو لاسلكية، كالإنترنت والشبكات المحلية (LAN).

المفهوم	نطاقه	مثال
أمن المعلومات (Information Security)	حماية المعلومات بأي شكل: ورقي أو رقمي	حماية ملفات اللاعبين الورقية والرقمية
الأمن السيبراني (Cybersecurity)	حماية الأنظمة والشبكات والبيانات الرقمية من الهجمات	حماية موقع الاتحاد وحسابات التواصل

المفهوم	نطاقه	مثال
أمنية الشبكات (Network Security)	حماية الاتصال والبنية الشبكية والبيانات المنقولة	جدار ناري وWPA3 وVPN لشبكة النادي

أهداف أمنية الشبكات: مثلث CIA (The CIA Triad)

الهدف	المعنى	أبرز الخطر	وسيلة الحماية
السرية (Confidentiality)	إتاحة البيانات للمصرح لهم فقط	التجسس والتنصت وسرقة البيانات	التشفير (Encryption) والتحكم بالوصول
السلامة (Integrity)	حماية البيانات من التعديل أو التزييف	تعديل الملفات والرسائل أثناء النقل	الهاش (Hashing) والتوقيع الرقمي
التوافر (Availability)	استمرار الوصول إلى الشبكة والخدمات	هجمات DoS والأعطال والفدية	النسخ الاحتياطي والتكرار (Redundancy)

مثال رياضي (Sports Example)
قاعدة بيانات اللاعبين: **السرية** تمنع تسريب بياناتهم الصحية، و**السلامة** تمنع تغيير نتائج اختبارات اللياقة، و**التوافر** يضمن فتح النظام يوم التسجيل في البطولة.

أهداف مكملة (Supporting Objectives)

الهدف	المعنى	مثال
التحقق من الهوية (Authentication)	إثبات أنك أنت من تدّعي	كلمة مرور + رمز OTP
التفويض (Authorization)	تحديد ما يُسمح لك فعله بعد الدخول	المدرب يعدّل البرامج والاعب يقرأ فقط
المحاسبة (Accounting)	تسجيل ما تم من عمليات (Logs)	سجل من دخل النظام ومتى
عدم الإنكار (Non-repudiation)	عدم قدرة الطرف على إنكار فعله	التوقيع الرقمي على عقد لاعب

تُعرف العناصر الثلاثة الأولى بنموذج **AAA**.

ثانياً: أهمية أمنية الشبكات (Importance)

أصبحت الشبكات عماد الاقتصاد والحياة اليومية (بنوك، رعاية صحية، حكومات، تعليم، رياضة). وبدون أمن قوي قد تقود الثغرات إلى خسائر مالية كبيرة وسرقة بيانات وتعطيل خدمات حيوية، كما حصل في هجوم **WannaCry عام 2017** الذي أصاب مئات الآلاف من الأجهزة في أكثر من 150 دولة.

المؤشر	الدلالة
تقرير IBM «تكلفة اختراق البيانات» 2023: المتوسط العالمي نحو 4.45 مليون دولار للاختراق الواحد	الاختراق مكلف مالياً حتى للمؤسسات المتوسطة
تقرير Verizon DBIR 2023: العنصر البشري (خطأ، سوء استخدام صلاحيات، بيانات دخول مسروقة، هندسة اجتماعية) حاضر في نحو 74% من الاختراقات	الوعي والتدريب لا يقلان أهمية عن الأجهزة

ملحوظة: تُحدَّث هذه التقارير سنوياً، فراجع أحدث إصدار عند الاستشهاد.

ثالثاً: المكونات الأساسية لأمنية الشبكات (Core Components)

المكوّن	أمثلة	الدور
الأجهزة (Hardware)	جدار ناري (Firewall)، راوتر آمن (Secure Router)، مبدّل مُدار	ضبط حركة البيانات وعزل الشبكات
البرمجيات (Software)	برامج التشفير (TLS)، مضاد الفيروسات/EDR، نظام SIEM	الاكتشاف والتحليل والتشفير
الإجراءات (Procedures)	التحديثات الدورية، النسخ الاحتياطي، التدقيق (Auditing)	تقليل الثغرات وسرعة التعافي
الأشخاص (People)	التدريب على الوعي الأمني، سياسات الاستخدام المقبول	تقليل الأخطاء البشرية

الهدف النهائي: تقليل المخاطر إلى أدنى مستوى مقبول (Risk Management)، إذ لا يوجد أمن مطلق بنسبة 100%.

رابعاً: التهديد والثغرة والمخاطر (Threat, Vulnerability & Risk)

المفهوم	التعريف	مثال
التهديد (Threat)	حدث أو جهة قد تستغل ضعفاً وتسبب ضرراً (وفق NIST)	هاكر، فيروس، فيضان، موظف مهمل
الثغرة (Vulnerability)	نقطة ضعف في النظام أو الإجراءات	برنامج غير محدّث، كلمة مرور ضعيفة
المخاطر (Risk)	احتمال استغلال التهديد للثغرة × حجم الأثر	احتمال اختراق موقع البطولة × خسارة البيانات
الهجوم (Attack)	محاولة فعلية لاستغلال الثغرة	إرسال رسالة تصيد، إغراق الخادم
الاستغلال (Exploit)	الأداة أو الطريقة التي تستغل الثغرة	شيفرة تستغل ثغرة في بروتوكول

معادلة المخاطر (Risk Formula)

المخاطر (Risk) = احتمال الحدوث (Likelihood) × الأثر (Impact). فإذا كان الاحتمال مرتفعاً والأثر كبيراً صارت المخاطرة عالية وتستحق المعالجة أولاً.

مصفوفة المخاطر (Risk Matrix)

الاحتمال \ الأثر	أثر منخفض	أثر متوسط	أثر مرتفع
احتمال مرتفع	متوسطة	عالية	حرجة
احتمال متوسط	منخفضة	متوسطة	عالية
احتمال منخفض	منخفضة	منخفضة	متوسطة

خيارات معالجة المخاطر (Risk Treatment)

- **التخفيف (Mitigate):** تطبيق ضوابط تقلل الاحتمال أو الأثر (تحديث، تشفير، جدار ناري).
- **النقل (Transfer):** نقل جزء من الخطر إلى طرف آخر (تأمين سيبراني، استضافة موثوقة).
- **التجنب (Avoid):** إيقاف النشاط الخطر (إلغاء خدمة غير ضرورية مكشوفة للإنترنت).
- **القبول (Accept):** قبول خطر منخفض الأثر عن وعي وبقرار موثق.

خامساً: أدوات الدفاع الشبكي (Network Defense Tools)

1) الجدار الناري (Firewall)

جهاز أو برنامج يراقب حركة البيانات الداخلة والخارجة ويسمح أو يمنع وفق قواعد محددة.

النوع	كيف يعمل؟	ملاحظة
تصفية الحزم (Packet Filtering)	يفحص عناوين IP والمنافذ والبروتوكول	سريع وبسيط وأقل ذكاء
الحالة (Stateful Inspection)	يتتبع حالة الاتصالات ويسمح بالردود المشروعة فقط	الأكثر شيوعاً
الوكيل (Proxy / Application Gateway)	يفحص محتوى الطلب على مستوى التطبيق	حماية أعمق وأبطأ
الجيل التالي (NGFW)	يدمج فحص التطبيقات والتهديدات والتحكم بالهوية	للمؤسسات الكبيرة

2) أنظمة كشف ومنع الاقتحام (IDS vs. IPS)

وجه المقارنة	IDS – Intrusion Detection System	IPS – Intrusion Prevention System
الوظيفة	يكتشف وينبّه (Alert)	يكتشف ويمنع تلقائياً (Block)
الموقع	يراقب نسخة من الحركة (Passive)	يقع على مسار الحركة (Inline)
الأثر	لا يعطل الحركة لكنه لا يوقف الهجوم	قد يعطل حركة مشروعة عند الخطأ (False Positive)

3) الشبكة الافتراضية الخاصة (VPN – Virtual Private Network)

تنشئ نفقاً مشفّراً (Tunnel) بين جهازك وشبكة أخرى عبر الإنترنت، فتحمي بياناتك على الشبكات العامة وتتيح الوصول الآمن لموارد المؤسسة عن بُعد. تعتمد على بروتوكولات مثل **IPsec** و**OpenVPN** و**WireGuard**. **تنبيه:** لا يجعلك VPN مجهولاً أو محصناً من الفيروسات؛ بل يحمي الاتصال فقط.

4) التشفير والهاش والتوقيع الرقمي (Cryptography)

الأداة	المبدأ	أمثلة
تشفير متماثل (Symmetric)	مفتاح واحد للتشفير وفكه؛ سريع	AES-256
تشفير غير متماثل (Asymmetric)	مفتاح عام للتشفير ومفتاح خاص لفكه؛ أبطأ	RSA، ECC
الهاش (Hash)	بصمة ثابتة الطول للبيانات؛ لا يمكن عكسها؛ تكشف أي تغيير	SHA-256 (MD5 و SHA-1 ضعيفان)
التوقيع الرقمي (Digital Signature)	هاش مشفّر بالمفتاح الخاص يثبت المصدر والسلامة	توقيع العقود والبرمجيات
البنية الأساسية للمفاتيح (PKI)	جهات موثوقة (CA) تصدر الشهادات الرقمية	شهادة موقع HTTPS

5) أدوات أخرى (Other Controls)

- **المصادقة متعددة العوامل (MFA):** كلمة مرور + رمز/بصمة، وتقلل كثيراً من نجاح سرقة كلمات المرور.

- **تجزئة الشبكة (Network Segmentation) والمنطقة المحايدة (DMZ):** عزل الخوادم العامة (كموقع النادي) عن الشبكة الداخلية.
- **SIEM:** جمع السجلات (Logs) من الأجهزة وتحليلها لكشف السلوك المشبوه.
- **مضاد البرمجيات الخبيثة وEDR:** حماية الأجهزة الطرفية وكشف السلوك الضار.
- **إدارة التحديثات (Patch Management):** سد الثغرات المعروفة فور صدور التصحيحات.
- **النسخ الاحتياطي 3-2-1:** ثلاث نسخ، على وسيطين مختلفين، واحدة منها خارج الموقع.
- **الثقة الصفرية (Zero Trust):** «لا تثق بأحد افتراضياً: تحقق دائماً» حتى داخل الشبكة الداخلية.

سادساً: بروتوكولات الأمان بالتفصيل (Security Protocols in Detail)

تنقسم بروتوكولات الاتصال إلى قديمة تنقل البيانات كنص واضح، وأخرى حديثة مشفّرة. فيما يأتي أهم بروتوكولات الحماية (راجع المحاضرة الثانية لشرح البروتوكولات الأساسية):

أمان طبقة النقل *TLS – Transport Layer Security*	
الوظيفة	تشفير الاتصال وتوثيق الخادم وحماية سلامة البيانات؛ يخلف SSL.
آلية العمل	تفاوض على النسخة ومجموعة التشفير ← تحقق من الشهادة الرقمية ← تبادل مفاتيح (غير متماثل) ← تشفير الجلسة بمفتاح متماثل سريع.
الاستخدام	HTTPS (443)، البريد المشفّر، VPN، FTPS.
الإصدارات	TLS 1.2 وTLS 1.3 الموصى بهما؛ SSL وTLS 1.0/1.1 مهجورة.

الغلاف الآمن *SSH – Secure Shell*	
الوظيفة	إدارة الأجهزة عن بُعد ونقل الملفات بأمان؛ بديل Telnet.
الخصائص	المنفذ 22؛ تشفير كامل للجلسة؛ توثيق بكلمة مرور أو بمفاتيح عامة/خاصة (الأقوى).
الاستخدام	إدارة الخوادم وراوترات الشبكة، وSFTP لنقل الملفات.

أمان بروتوكول الإنترنت *IPsec – Internet Protocol Security*	
الوظيفة	تشفير وتوثيق حزم IP نفسها في طبقة الشبكة.
المكونات	AH (توثيق وسلامة) وESP (تشفير وتوثيق) وIKE (تبادل المفاتيح).
الوضعان	Transport Mode لحماية البيانات بين جهازين، وTunnel Mode لحماية حركة شبكة كاملة (VPN بين فرعين).
الاستخدام	وصل فرعين لمؤسسة عبر الإنترنت بنفق مشفّر.

حماية الشبكة اللاسلكية *WPA2 / WPA3 – Wi-Fi Protected Access*	
الوظيفة	تشفير وتوثيق الاتصال اللاسلكي (Wi-Fi).

التطور	WEP (مكسور) ← WPA3 ← WPA2 (AES-CCMP) ← WPA (أمان أقوى ضد تخمين كلمة المرور وSAE).
التوصية	استخدم WPA3 إن توفر وإلا WPA2 مع كلمة مرور طويلة؛ عطّل WPS وغيّر كلمة مرور الراوتر الافتراضية.

بروتوكولات نقل الملفات الآمنة *SFTP / FTPS*	
SFTP	نقل ملفات فوق SSH (المنفذ 22) بتشفير كامل.
FTPS	بروتوكول FTP محمي بطبقة TLS.
الفرق عن FTP	FTP العادي يرسل كلمة المرور والملفات بنص واضح.

امتدادات أمان DNS *DNSSEC / DoH – DNS Security*	
DNSSEC	يوقّع سجلات DNS رقمياً فيتأكد المستخدم أن الجواب لم يُزوَّر (يحمي السلامة لا السرية).
DoH (DNS over HTTPS)	يشفّر استعلامات DNS داخل HTTPS فيخفيها عن المتلصصين على الشبكة.

من البروتوكول غير الآمن إلى الآمن (Insecure → Secure)

غير آمن	البديل الآمن	ما الذي تغيّر؟
HTTP (80)	HTTPS (443)	إضافة تشفير TLS وتوثيق الخادم
FTP (21)	SFTP / FTPS	تشفير الدخول والملفات
Telnet (23)	SSH (22)	تشفير الجلسة والأوامر
POP3 / IMAP / SMTP	POP3S (995) / IMAPS (993) / SMTP+TLS (587)	حماية كلمة المرور ونص البريد
WEP / WPA	WPA2 / WPA3	خوارزميات تشفير أقوى
DNS عادي	DNSSEC / DoH	توثيق السجلات أو إخفاء الاستعلامات

سابعاً: الدفاع بالعمق (Defense in Depth)

لا تعتمد الحماية الجيدة على أداة واحدة؛ فإذا سقطت طبقة بقيت الأخرى. وتُبنى طبقات متعددة:

الطبقة	الضوابط	مثال في نادٍ رياضي
الفيزيائية (Physical)	أقفال وكاميرات وتحكم دخول لغرف الخوادم والمقسّمات	غرفة الراوتر مقفلة
الشبكة (Network)	جدار ناري، تجزئة، VPN، IDS/IPS	شبكة الضيوف منفصلة عن شبكة الإدارة
الجهاز (Host / Endpoint)	تحديثات، مضاد برمجيات، تشفير القرص	حواسيب المدربين محدّثة ومحمية
التطبيق (Application)	التحقق من المدخلات، MFA، HTTPS	موقع حجز التذاكر آمن

الطبقة	الضوابط	مثال في نادٍ رياضي
البيانات (Data)	تشفير، نسخ احتياطي، صلاحيات	بيانات اللاعبين الصحية مشفّرة
الأشخاص والسياسات (People & Policy)	تدريب، سياسة كلمات مرور، خطة استجابة	تعليمات للعاملين حول التصيد

ثامناً: الأطر والمعايير الدولية (Frameworks & Standards)

المعيار	المضمون
NIST Cybersecurity Framework (CSF 2.0)	إطار أمريكي مفتوح بست وظائف: الحوكمة (Govern)، التعرف (Identify)، الحماية (Protect)، الكشف (Detect)، الاستجابة (Respond)، التعافي (Recover)
ISO/IEC 27001	معيار دولي لإنشاء نظام إدارة أمن المعلومات (ISMS) وقابل للاعتماد والتدقيق
CIS Controls	قائمة ضوابط عملية مرتبة بالأولوية لتحصين الأنظمة والشبكات
NIST SP 800-30	دليل تقدير المخاطر (Risk Assessment)

تاسعاً: خطة حماية مبسطة لشبكة نادٍ رياضي (Mini Security Plan – Applied Example)

السيناريو (افتراضي): نادٍ رياضي لديه موقع حجز، وشبكة Wi-Fi للمدربين واللاعبين، وحاسوب إدارة يحفظ بيانات الأعضاء ومدفوعاتهم.

الأصل (Asset)	التهديد المحتمل	الخطر	الضابط المقترح
موقع الحجز	حقن/تعطيل DDoS	عالٍ	HTTPS، جدار تطبيقات، تحديثات، نسخ احتياطي
شبكة Wi-Fi	دخول غير مصرح، رجل في الوسط	متوسط	WPA3/WPA2 وكلمة مرور قوية، شبكة ضيوف منفصلة
حاسوب الإدارة	فدية وتصيد	حرج	تحديثات، MFA، مضاد برمجيات، نسخ 3-2-1، تدريب
بيانات الأعضاء	تسريب أو تعديل	عالٍ	تشفير وصلاحيات ومراجعة سجلات

عادات أمان شخصية (Personal Security Habits)

7. غيّر اسم الشبكة وكلمة مرور الراوتر الافتراضية وفعّل WPA2/WPA3.
8. حدّث نظام الهاتف والحاسوب والراوتر باستمرار.
9. استخدم مدير كلمات مرور وMFA لحساباتك المهمة.
10. تجنب الشبكات العامة للعمليات المالية، واستخدم VPN موثوقاً عند الضرورة.
11. لا تفتح مرفقات أو روابط غير متوقعة، وتحقق من المرسل.
12. احتفظ بنسخة احتياطية من ملفاتك المهمة خارج جهازك.

عاشراً: نشاط صفّي (Class Activity)

المطلوب (مجموعات): اختاروا منشأة رياضية (قاعة لياقة، مدرسة، اتحاد) وأكملوا:

البند	إجابة المجموعة
أهم ثلاثة أصول (Assets)	
تهديد محتمل لكل أصل	
تقدير الخطر (احتمال × أثر)	
ثلاثة ضوابط مقترحة	
بروتوكولات آمنة ستستخدمونها	

حادي عشر: مسرد المصطلحات (Glossary)

المصطلح (Term)	المعنى
CIA Triad	السرية والسلامة والتوافر
AAA	التوثيق والتفويض والمحاسبة
Firewall	جدار ناري
IDS / IPS	كشف / منع الاقتحام
VPN	شبكة افتراضية خاصة
Encryption	تشفير
Hash	دالة بصمة لا تُعكس
Digital Signature	توقيع رقمي
PKI / CA	بنية المفاتيح العامة / جهة إصدار الشهادات
MFA	مصادقة متعددة العوامل
SIEM	إدارة معلومات وأحداث الأمن
Zero Trust	الثقة الصفرية
Patch	تحديث تصحيحي
Risk	المخاطر
Defense in Depth	الدفاع بالعمق

ثاني عشر: أسئلة تدريبية (Practice Questions)

أولاً: اختيار من متعدد (Multiple Choice)

1) أي عنصر من CIA تحميه إجراءات الهاش والتوقيع الرقمي؟

أ) السرية
ب) السلامة
ج) التوافر
د) المحاسبة

2) الفرق بين IDS وIPS أن IPS:

أ) يكتشف فقط

ب) يكتشف ويمنع تلقائياً

ج) يشفّر البيانات

د) يحذف الفيروسات

3) المخاطر (Risk) تساوي:

أ) الثغرة + التهديد

ب) الاحتمال × الأثر

ج) عدد الأجهزة × السرعة

د) التشفير × الهاش

4) البديل الآمن لـ Telnet هو:

أ) FTP

ب) HTTP

ج) SSH

د) SMTP

5) أقوى بروتوكولات حماية الواي فاي الحالية:

أ) WEP

ب) WPA

ج) WPA2 فقط

د) WPA3

ثانياً: صح أم خطأ (True / False)

1. القفل في المتصفح يعني أن الموقع آمن من الاحتيال بالضرورة. ( )
2. VPN يحمي الاتصال المشفّر لكنه لا يغني عن مضاد الفيروسات. ( )
3. يوجد أمن مطلق بنسبة 100% عند استخدام جدار ناري. ( )
4. النسخ الاحتياطي يدعم هدف التوافر. ( )

ثالثاً: أسئلة قصيرة (Short Answer)

1. عرّف أمنية الشبكات واذكر أهدافها الثلاثة الرئيسة.
2. ميّز بين التهديد والثغرة والمخاطر بمثال رياضي.
3. اشرح الفرق بين FTP وSFTP.

رابعاً: أسئلة تطبيقية (Applied)

1. اقترح خمسة ضوابط لحماية شبكة قاعة رياضية صغيرة وبيّن كل ضابط يحمي أي هدف من CIA.
2. ما الفرق بين الدفاع بالعمق والاعتماد على جدار ناري واحد؟

الإجابات النموذجية (Answer Key)

القسم	الإجابة
اختيار من متعدد	1-ب ، 2-ب ، 3-ب ، 4-ج ، 5-د
صح / خطأ	1-خطأ ، 2-صح ، 3-خطأ ، 4-صح

ملخص المحاضرة (Summary)

- أمنية الشبكات حماية للاتصال والبيانات، وتقوم على مثلث CIA وتدعمها AAA وعدم الإنكار.

- تُدار المخاطر بمعادلة الاحتمال × الأثر، وتُعالج بالتخفيف أو النقل أو التجنب أو القبول.
- لا تعتمد الحماية على أداة واحدة: جدران نارية وVPN وتشفير وMFA وSIEM ونسخ احتياطي وتدريب، مع استخدام البروتوكولات الآمنة (TLS, SSH, IPsec, WPA3).

المصادر والمراجع (References)

1. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0. 2024.
2. NIST. SP 800-30 Rev.1: Guide for Conducting Risk Assessments. 2012. | SP 800-41 Rev.1: Guidelines on Firewalls and Firewall Policy. 2009. | SP 800-207: Zero Trust Architecture. 2020.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
4. Center for Internet Security. CIS Critical Security Controls, v8.
5. Stallings W. Network Security Essentials: Applications and Standards. Pearson (latest edition).
6. Saltzer JH, Schroeder MD. The protection of information in computer systems. Proc IEEE. 1975;63(9):1278–1308.
7. IBM Security. Cost of a Data Breach Report 2023 (and later editions).
8. Verizon. 2023 Data Breach Investigations Report (DBIR) (and later editions).
9. Rescorla E. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. IETF; 2018. | Ylonen T, Lonvick C. RFC 4253: The Secure Shell (SSH) Transport Layer Protocol. 2006.
10. Wi-Fi Alliance. WPA3 Specification (latest version).

إعداد: **أ.م.د. حيدر حسن محمد**
م.م. اثير اسماعيل فاضل
مدرسي المادة