الفصل الأول: مقدمة في الأمن السيبراني

الأمن السيبراني لم يعد مجرد مهارة تقنية، بل أصبح اليوم عنصرًا استراتيجيًا يمسُّ كل قطاع في العالم: الحكومات، الشركات، البنوك، المستشفيات، وحتى المستخدم العادي.
العالم الرقمي لم يعد مكانًا بسيطًا... بل منظومة معقدة متعددة الطبقات.
كل نقرة، كل اتصال، كل بيانات نُرسلها — تصبح جزءًا من "ساحة قتال رقمية" غير مرئية.

المهاجمون لا يحتاجون قوة جسدية، ولا سلاح حقيقي...
سلاحهم الوحيد: **المعلومة + الوصول + الفهم**.

من هنا يأتي دور الأمن السيبراني.

الأمن السيبراني Cybersecurity هو علم وتقنيات لحماية:

- البيانات
- الأنظمة
- الشبكات
- المستخدمين
- التطبيقات
- الخدمات الرقمية

من أي اختراق – استغلال – تدمير – تعطيل – تجسس – أو العبث غير المصرّح به.

الأمن السيبراني ليس مجرد مضاد فيروسات Antivirus
وليس مجرد كلمة "Hacking" في الأفلام.

هو منظومة هندسية كاملة
تحتاج إلى:

- تحليل
- فهم بروتوكولات
- هندسة مخاطر
- دفاعات طبقية Layered Defense
- استجابة للحوادث Incident Response
- تحقيقات رقمية Digital Forensics

وسيكون هذا الكتاب رحلة من البداية إلى مستوى الفهم الاحترافي.

ليس هدفنا أن "نعرف المصطلحات" فقط...
بل نبني "تفكير أمني" Security Mindset

لأن أقوى سلاح في عالم الأمن السيبراني ليس برنامجًا...
بل العقل.

الفصل الثاني: لماذا الأمن السيبراني مهم؟

العالم اليوم يعيش في "اقتصاد البيانات".
المعلومة أصبحت أهم من الذهب، وأخطر من السلاح التقليدي.

الدول الآن لا تحتاج حرب دبابات لتدمّر دولة أخرى...
يكفي أن تضرب:

- نظام الكهرباء
- شبكة المستشفيات
- نظام البنوك
- أو شبكة الإنترنت الوطنية

لتسقط دولة كاملة خلال دقائق!

الهجمات السيبرانية اليوم:

- تغيّر نتائج انتخابات
- تسقط شركات مليار دولار
- تسرق بيانات ملايين الأشخاص
- توقف مطارات عن العمل
- وتفتح أبواب الخوف لدى الحكومات

لهذا السبب: **الأمن السيبراني أصبح ضرورة وطنية واستراتيجية**

وليس وظيفة تقنية فقط.

أمثلة تجعل الصورة أوضح:

- إذا تم اختراق بنك ← العملاء يفقدون أموالهم
- إذا تم اختراق مستشفى ← مرضى قد يموتون بسبب توقف الأجهزة
- إذا تم اختراق شركة اتصالات ← كل المكالمات والرسائل تصبح مكشوفة
- إذا تم اختراق شركة طاقة ← الكهرباء تنقطع عن مدينة كاملة

الهجوم السيبراني اليوم = تأثير حقيقي على أرض الواقع
ليس مجرد "خطأ تقني" داخل جهاز.

الأمن السيبراني يحمي:

المجال	ماذا يحمي؟
المدنيين	الخصوصية – الحسابات – الرسائل
الشركات	البيانات – العملاء – الأرباح
الحكومات	الأمن الوطني – المؤسسات – البنية التحتية
الجيش	أسرار الدفاع – الاتصالات – الخطط العسكرية

لهذا أصبح الأمن السيبراني:

علم + صناعة + أمن قومي

وليس مجالًا جانبيًا.

الفصل الثالث: مثلث CIA (أساس الأمن السيبراني)

قبل ما نفهم الهجمات والاختراقات والتقنيات، لابد نفهم الأساس العلمي الذي يقوم عليه الأمن السيبراني.
هذا الأساس يسمى:

CIA Triad

وهو ليس له علاقة بالمخابرات الأمريكية كما يعتقد البعض،
بل هي ثلاثة مفاهيم تشكّل "ركائز الأمن السيبراني":

---

1) Confidentiality — السريّة

المقصود بالسريّة هو منع أي شخص غير مخوّل من الوصول للبيانات.

الهدف هنا: البيانات لا يراها إلا من يحق له رؤيتها

مثل:

- **كلمات المرور**
- **أرقام البطاقات البنكية**
- **ملفات الشركات الداخلية**

تُحمى عن طريق:

- **التشفير Encryption**
- **التحكم بالصلاحيات Access Control**
- **كلمات مرور قوية**

---

2) Integrity — سلامة البيانات

تعني أن البيانات تبقى صحيحة ولم يتم التلاعب بها.

الهدف: المعلومات تبقى كما هي بدون تغيير خبيث أو خطأ

مثال:

- **تخيلي مهاجم يغيّر رقم حساب بنكي أثناء التحويل**

هذا هجوم على سلامة البيانات

تقنيات حمايتها:

- **Hashing**
- **Signatures**
- **Checksums**

---

3) Availability — التوافرية

المقصود هو أن النظام يجب أن يعمل متى احتجناه.

الهدف: النظام لا يتوقف — والموارد متاحة دائماً

تخيلي لو:

- موقع مستشفى توقف عن العمل وقت عملية جراحية

هذا كارثة

هجمات الـ DDoS
(الهجمات الموزعة)
هي أشهر مثال لضرب "التوافرية".

لماذا CIA Triad مهم؟

لأن أي نظام أو شركة أو شبكة يجب أن تضمن الثلاثة معًا:

العنصر	ماذا يضمن؟
Confidentiality	ما حد يقدر يشوف البيانات
Integrity	ما حد يقدر يغيّر البيانات
Availability	النظام دائماً شغّال

هذه الركائز الثلاث هي الهوية الأساسية للأمن السيبراني.

وكل شيء في هذا العلم (تقنيات — هجمات — حماية)
نرجع له في النهاية لفهم كيف يؤثّر على CIA Triad.

الفصل الرابع: أنواع الهجمات السيبرانية (Attacks Types)

الهجمات السيبرانية ليست كلها نوع واحد.
المهاجمون لديهم طرق مختلفة، وأهداف مختلفة، وأدوات مختلفة.

هنا أهم الأنواع الأساسية والجوهرية:

1) Malware Attacks

الهجوم الذي يعتمد على "برمجيات خبيثة" يتم زرعها داخل النظام.

أنواع الـ Malware كثيرة مثل:

- **Virus (فيروس)**
- **Worm (ديدان)**
- **Trojan (حصان طروادة)**
- **Ransomware (فدية)**

غالبًا تأتي من:

- **روابط مزيفة**
- **ملفات مرفقة**
- **USB ملوث**

---

2) Phishing Attacks

الهجوم عن طريق "خداع المستخدم".

مثل:

- **رسالة ايميل تشبه البنك**
- **صفحة تسجيل دخول مزيفة**
- **رابط fake log in**

الهدف: سرقة معلومات تسجيل الدخول.

---

3) DDoS Attacks

الهجوم على "التوافرية Availability".

الهجوم يشغل السيرفر بكمية طلبات ضخمة
لدرجة أنه ينهار ويتوقف عن العمل.

هذا الهجوم يدمّر شركات إذا لم يكون عندهم دفاعات قوية.

---

4) Man-in-the-middle Attack (MiTM)

الهجوم الذي يقوم فيه المهاجم بالجلوس "وسط الاتصال" بين جهازين.

مثال: أنتِ ترسلين بيانات ← الشخص الثالث يقرأها ويعدّلها قبل أن تصل.

---

5) Password Attacks

هجمات تعتمد على كسر كلمات المرور:

- **Brute Force (تجربة احتمالات كثيرة بسرعة)**
- **Dictionary attacks**
- **Credential Stuffing**

كلها تهدف للوصول لحساب بدون إذن.

---

6) Zero-Day Attacks

هذا أخطر نوع.

هجوم يستغل ثغرة جديدة لم يتم اكتشافها بعد.
يعني حتى الشركة المصنّعة ما تدري عنها.

هذي الهجمات قيمتها ملايين أحيانًا.

هذه الأنواع الأساسية والهامة.
والفصل القادم نبدأ ندخل أعمق... ونفصل كل نوع.

الفصل الخامس: البرمجيات الخبيثة (Malware)

Malware هي اختصار لـ:
Malicious Software = برمجيات خبيثة

وهي برامج يتم إنشاؤها بهدف:

- **التخريب**
- **السرقة**

- **التجسس**
- **التدمير**
- **السيطرة على الأنظمة**

المهاجم يستخدمها كـ "سلاح" داخل الجهاز أو الشبكة.

الناس العاديين يسمونها كلها "فيروس"
لكن علميًا... كلمة Malware تشمل عدة أنواع مختلفة
كل نوع له طريقة هجوم مختلفة.

الانواع الأساسية للـ Malware:

---

1) Virus – الفيروس

برنامج يلتصق بملف سليم ثم ينتشر.

الهدف: إصابة أكبر عدد من الأنظمة

ينتشر عادة عبر:

- **ملفات مصابة**
- **برامج مقرصنة**
- **الفلاش USB**

---

2) Worm – الديدان

أخطر من الفيروس

لأنها تنتشر بدون الحاجة لملف.

يعني الدودة تنتشر عبر الشبكة تلقائيًا
من جهاز إلى جهاز بدون تدخل.

---

3) Trojan – حصان طروادة

الاسم مأخوذ من قصة طروادة

يظهر كبرنامج مفيد (مثل لعبة – برنامج – كراك)
لكن بداخله كود خطير يتم تنفيذه عند فتحه.

الهجوم الأقوى في Trojans هو "الخداع".

---

4) Ransomware – برمجيات الفدية

هذا يعتبر الآن أخطر نوع في العالم.

الفكرة: البرنامج يقفل ملفات الضحية بتشفير قوي
ثم يطلب "فدية" (فلوس) لفك التشفير.

شركات ضخمة أُغلقت بسبب ransomware.

---

5) Spyware – برامج التجسس

هذا النوع لا يخرّب جهازك
لكن يسجل:

- **ما تكتب**
- **ما تفتح**
- **ما تشاهد**
- **مواقعك**

ويرسلها للمهاجم بصمت.

---

6) Keylogger – مسجّل لوحات المفاتيح

نوع خاص من Spyware

يسجّل جميع الأحرف اللي تكتبينها على الكيبورد
مثل كلمات السر ـــ محادثات ـــ أرقام بطاقات

لماذا malware خطيرة؟

لأنها "غير مرئية" في أغلب الأحيان.
تدخل النظام بهدوء
وتعمل بدون ما يشعر المستخدم.

وهنا تظهر أهمية:

- **أدوات الحماية**
- **الكشف عن السلوك Behavior Analysis**
- **threat intelligence**

الفصل السادس: الهندسة الاجتماعية (Social Engineering)

"أضعف جدار حماية في أي نظام هو الإنسان نفسه."

حتى أقوى الأنظمة التقنية يمكن اختراقها إذا تم خداع الشخص الذي يستخدمها.
وهذا بالضبط ما تفعله الهندسة الاجتماعية.

ما هي الهندسة الاجتماعية؟

هي فنّ التلاعب بالبشر نفسيًا
حتى يقوموا بأفعال تساعد المهاجم بدون ما يشعرون.

المهاجم لا يحتاج سلاحًا، فقط يحتاج أن يجعلك:

- **تفتح رابطًا خبيثًا**
- **أو تشارك كلمة السر**
- **أو تضغط على ملف ملوّث**
- **أو تكشف معلومة صغيرة تساعده في الهجوم**

أمثلة حقيقية لهجمات Social Engineering

1. **Email phishing (تصيّد بالبريد)**
   يُرسل المهاجم رسالة بريد تشبه رسالة رسمية من البنك أو الشركة
   فيها رابط مزيف ← المستخدم يضغط عليه ← يعطي بياناته.

2. **Phone call attack (خداع عبر الهاتف)**
   المهاجم يتّصل ويدّعي أنه من الدعم الفني
   ويطلب كلمة مرور أو كود تأكيد.

3. **Baiting (الطُعم)**
   يضع المهاجم USB أمام الباب مكتوب عليها "رواتب الموظفين"
   الفضول يجعل أحدهم يفتحها ← الجهاز يُصاب بفيروس.

4. **Pretexting (اختلاق قصة)**
   المهاجم يختلق سيناريو كامل (مثل موظف في الشركة أو مسؤول بنك)
   للحصول على معلومة صغيرة.

5. **Tailgating (الدخول خلف شخص)**
   الهجوم المادي: المهاجم يدخل مبنى الشركة خلف موظف دون تصريح.

لماذا الهندسة الاجتماعية خطيرة؟

لأنها لا تستهدف الأجهزة... بل تستهدف الثقة.

يمكنك حماية جهازك بجدار ناري وبرامج متقدمة،
لكن من الصعب حماية نفسك من مكالمة أو رسالة مصممة بإتقان.

كيف نحمي أنفسنا؟

- **لا تثق بأي رسالة تطلب بياناتك**
- **لا تفتح روابط مجهولة**
- **تأكد من عنوان البريد الإلكتروني دائمًا**
- **استخدم تحقق بخطوتين (Two-Factor Authentication)**
- **كن دائم الشك والتحقق قبل التصرف**

"الهندسة الاجتماعية لا تُخترق الأنظمة، بل تُخترق العقول."

الفصل السابع: التشفير (Cryptography)

مقدمة

التشفير هو لغة السر في العالم الرقمي.
حين نفهم التشفير، نفهم كيف تُحمى البيانات أثناء التخزين والنقل، وكيف تُثبت الهوية، وكيف نضمن سلامة الرسائل.
التشفير ليس سحرًا بل علوم رياضية وهندسة تطبيقية تجمع بين الرياضيات، نظرية الأعداد، وبُنى البروتوكولات.

لماذا التشفير مهم؟

لأن البيانات بلا تشفير تساوي معلومات مكشوفة.
التشفير يحفظ:

- **السرية (Confidentiality): لا يطلع على البيانات إلا المخوّل.**
- **السلامة (Integrity): يؤكد أن البيانات لم تُغيّر.**
- **المصادقة (Authentication): يؤكّد من أرسل الرسالة.**
- **الانكار غير ممكن (Non-repudiation): المرسل لا يستطيع إنكار إرساله.**

التشفير لبّ كل تطبيقات الأمن: الشبكات، البريد، الدفع الإلكتروني، التخزين السحابي، الاتصالات العسكرية، وواجهات الإنترنت الحساسة.

المفاهيم الأساسية

1. المفتاح (Key)

التشفير يعتمد على مفتاح سري أو زوج مفاتيح. المفتاح هو ما يجعل الشيفرة قابلة للعكس (أو لا قابلة للعكس) حسب النوع.

2. الخوارزمية (Algorithm)

قواعد رياضية لتحويل النص الواضح Plaintext إلى نص مشفّر Ciphertext وبالعكس.

3. الأهداف

- **سرّية: لا يُقرأ النص المشفّر بدون المفتاح.**
- **سلامة: التلاعب يكتشف.**
- **مصادقة: التأكد من هوية المرسل.**

- **عدم إنكار: إثبات أن المرسل هو فعلاً المرسل.**

أنواع التشفير الأساسية

أ) التشفير المتماثل (Symmetric Cryptography)

- **يعتمد على مفتاح واحد مشترك بين المرسل والمستقبل.**
- **المرسل والمستقبل يستخدمان نفس المفتاح للتشفير وفك التشفير.**
- **أمثلة مشهورة: 3DES ،(AES (Advanced Encryption Standard.**
- **ميزات: سريع وفعّال للبيانات الكبيرة.**
- **عيب: مشكلة توزيع المفاتيح ـــ كيف تشارك المفتاح بأمان مع الطرف الآخر؟**

استخدام عملي: تشفير الأقراص الصلبة، قنوات VPN، تشفير ملفات النسخ الاحتياطي.

ب) التشفير غير المتماثل (Asymmetric / Public-Key Cryptography)

- **يعتمد على زوج مفاتيح: مفتاح عام Public Key ومفتاح خاص Private Key.**
- **أيُّ شخص يمكنه تشفير برسالتك باستخدام المفتاح العام، لكن فقط صاحب المفتاح الخاص يستطيع فك التشفير.**
- **أمثلة مشهورة: RSA, ECC (Elliptic Curve Cryptography).**
- **مزايا: يسهّل تبادل المفاتيح ومصادقة الهوية.**
- **عيوب: أبطأ من التشفير المتماثل عند التعامل مع كميات بيانات كبيرة، لذا غالبًا يُستخدم لتبادل مفاتيح التشفير المتماثل (hybrid).**

استخدام عملي: تبادل مفاتيح TLS، توقيعات رقمية، تشفير البريد الإلكتروني.

ج) التجزئة (Hashing)

- **دالة تأخذ مدخلًا وتنتج مُخرَجًا ثابت الطول (hash).**
- **خصائص مهمة: لا رجعة (one-way)، حساس لأقل تغيير، تصادمية صعبة (صعوبة إيجاد مدخلين بنفس الهاش).**
- **أمثلة: SHA-256, SHA-3, MD5 (قديم وغير آمن الآن).**
- **استخدامات: التحقق من سلامة الملفات، تخزين كلمات المرور (مع ملح Salt)، التحقق من توقيع رقمي.**

د) التواقيع الرقمية (Digital Signatures)

- **عملية تضمن المصادقة وعدم الإنكار وسلامة الرسالة.**
- **عادةً تُستخدم الخوارزميات غير المتماثلة: المرسل يوقّع الرسالة بمفتاحه الخاص، والمستقبل يتحقق بالتوقيع باستخدام المفتاح العام.**

- أمثلة: RSA signatures, ECDSA (Elliptic Curve Digital Signature Algorithm).

بروتوكولات وتطبيقات شائعة

- TLS/SSL: تشفير اتصالات الويب (HTTPS).
- PGP / GPG: تشفير وتوقيع البريد الإلكتروني.
- SSH: إدارة الأجهزة عن بعد بمصادقة وتشفير قوي.
- VPN (IPSec, OpenVPN): إنشاء قنوات آمنة بين شبكات.
- Disk encryption (BitLocker / LUKS): تشفير كامل للقرص.

أمثلة عملية مبسطة

مثال 1 — تبادل مفتاح آمن (Hybrid Encryption)

1. الطرف A ينشئ مفتاحًا متماثلاً عشوائيًا (AES key).
2. A يشفر البيانات باستخدام AES.
3. A يشفر مفتاح AES باستخدام مفتاح B العام (RSA).
4. يرسل A إلى B: [RSA(encrypt(AES_key)), AES(Ciphertext)].
5. B يفك RSA ليحصل على AES_key، ثم يفك AES للحصول على البيانات.

هذا يجمع سرعة AES مع أمان توزيع مفاتيح RSA.

مثال 2 — توقيع رقمي

1. يكتب المستخدم رسالة.
2. يحسب هاش الرسالة (SHA-256).
3. يشفّر الهَاش بمفتاحه الخاص → هذا هو التوقيع.
4. المُستقبل يحسب هاش الرسالة بنفس الخوارزمية ويستخدم المفتاح العام للتحقق من التوقيع: إذا تطابقا، فالرسالة أصلية ولم تُغير.

مسائل أمنية مهمة في التشفير

1. إدارة المفاتيح (Key Management)

أضعف حلقات التشفير غالبًا تكون في إدارة المفاتيح: تخزين المفاتيح، تدويرها، سحبها عند الخطر.
مفاتيح مسربة = فشل الحماية كامل.

2. الطول والمقاييس (Key Length & Parameters)

- **RSA: طول المفتاح المقترح حالياً ≥ 2048 بت، يفضّل 3072 أو 4096 للبيانات الحساسة.**
- **ECC: توفر أمان بنفس قوة RSA لكن بمفاتيح أقصر (مثلاً ،Curve25519 secp256r1).**

3. الملح والتمليح (Salt) وPBKDF

عند تخزين كلمات المرور يجب استخدام ملح Salt وبدائل تجزئة قوية مثل ,PBKDF2, bcrypt scrypt, أو Argon2 لتقليل فعالية هجمات القوة الغاشمة.

4. دور randomness (العشوائية)

توليد أرقام عشوائية عالية الجودة (CSPRNG) أمر حاسم — مفاتيح ضعيفة عشوائياً تُفسد التشفير.

5. جوانب عملية: side-channels و implementation bugs

الهجمات قد لا تستهدف الخوارزمية نفسها بل تنفيذها: تسريبات عبر الزمن، استهلاك الطاقة، ثغرات في المكتبات، سوء استخدام البروتوكولات (مثال: ضعف في TLS أو استخدام إصدارات قديمة).

أفضل الممارسات (Best Practices)

- **استخدمي مكتبات مشهورة ومُحدّثة (OpenSSL مدعومة جيدًا مع الحذر، libsodium للمهمات الحديثة).**
- **لا تبتكري خوارزميات بنفسك؛ الاعتماد على المواصفات القياسية.**
- **إدارة مفاتيح آمنة: تخزين مفاتيح خاصة في HSM أو Key Vault.**
- **تدوير المفاتيح بشكل دوري وسياسة سحب عند الشك.**
- **استخدام TLS مُهيأ بشكل صحيح: تعطيل البروتوكولات القديمة، تفعيل HSTS، استخدام شهادات قوية.**
- **تخزين كلمات المرور باستخدام Salt + Argon2 أو bcrypt.**

خاتمة الفصل

التشفير هو حجر الأساس الذي يضمن سرية وسلامة ومصداقية كل شيء في الأمن السيبراني. لكنه ليس حلًا منفردًا؛ يجب دمجه مع سياسات قوية، إدارة مفاتيح محكمة، ووعي بشري.
في الفصول القادمة سنغوص في بروتوكولات الشبكات، وتأمين التطبيقات، وكيفية تطبيق تقنيات التشفير عمليًا في سيناريوهات حقيقية.

الفصل الثامن: أساسيات الشبكات Network Fundamentals

قبل أن نفهم الأمن السيبراني على مستوى احترافي، يجب أن نفهم الشبكات، لأن كلّ هجوم، وكل دفاع، وكل Packet، وكل Data — تتحرك عبر شبكة.

بدون فهم الشبكات... لا يمكن فهم السايبر.

ما هي الشبكة؟

الشبكة هي مجموعة أجهزة يتم توصيلها معًا لتبادل البيانات.

مثلًا:

- **موبايل ←→ راوتر ←→ إنترنت**
- **كمبيوتر ←→ سيرفر ←→ قاعدة بيانات**

أي هجوم سيبراني يحدث داخل شبكة أو عبر شبكة.

عناصر الشبكة الأساسية

العنصر	الوظيفة
الجهاز (Host)	مثل هاتفك أو كمبيوترك
الراوتر Router	يوجّه حركة البيانات
السويتش Switch	يربط الأجهزة داخل نفس الشبكة
المودم Modem	يربط البيت بالإنترنت

السيرفر Server	**يقدم خدمة (مثل موقع – بريد – قاعدة بيانات)**

أنواع الشبكات

النوع	الشرح
LAN	**شبكة محلية داخل منزل/شركة صغيرة**
WAN	**شبكة واسعة مثل الإنترنت**
WLAN	**شبكة لاسلكية (WiFi)**
MAN	**شبكة مدن (Municipal Area Network)**

الإنترنت هو WAN ضخم يصل كل شبكات العالم ببعض.

البروتوكولات

البروتوكول = لغة الشبكة

أهم بروتوكولات الشبكات:

البروتوكول	الدور
TCP	**يضمن وصول البيانات بدون فقد**

UDP	أسرع — بدون ضمان
HTTP/HTTPS	تصفّح المواقع
DNS	تحويل أسماء المواقع إلى عناوين IP
DHCP	يعطي الأجهزة IP تلقائيًا
FTP	نقل الملفات

بدون DNS — ما تقدرين تدخلين "google.com"
كان لازم تكتبي عنوان IP بدل اسم الموقع.

ما هو الـ IP Address ؟

رقم يعرّف الجهاز داخل الشبكة

مثلاً:

192.168.1.10 ← عنوان جهاز داخل الشبكة المنزلية
بينما عنوان الإنترنت يكون public ويتغيّر غالبًا.

الـ Ports (المنافذ)

الـ Port مثل "باب خدمة" داخل الجهاز.

مثال:

Port	بروتوكول	خدمة

80	HTTP	موقع عادي
443	HTTPS	موقع مشفّر
22	SSH	إدارة أجهزة عن بعد
53	DNS	طلبات أسماء الدومينات

لما مهاجم يفحص جهاز – أول شيء يبحث عنه: المنافذ المفتوحة.

Layers of Networking

الطبقات الأكثر استخدامًا للدراسة هي:

(OSI Model (7 Layers

لكن في الأمن السيبراني نركز عادةً على:

الطبقة	الوظيفة
Layer 3 Network	IP Address routing
Layer 4 Transport	TCP / UDP
Layer 7 Application	HTTP, FTP, DNS…

الهجمات ← غالبًا تستهدف Layer 7 (طبقة التطبيقات) لأنها الأعلى والأغنى بالبيانات.

لماذا الشبكات مهمة للأمن؟

لأن كل فعل في الأمن السيبراني هو في النهاية "Traffic" داخل الشبكة.

- **Packet Capture**
- **Attack Surface**
- **Intrusion Detection**
- **Threat Hunting**
- **Firewall Rules**

كلها مبنية على فهم الشبكات.

قاعدة ذهبية:
"الذي لا يفهم الشبكات — لا يمكن أن يصبح محترف أمن سيبراني."

الفصل التاسع: تأمين تطبيقات الويب (Web Application Security)

تطبيقات الويب هي أي خدمة تعمل من خلال متصفح (Browser):

- **مواقع**
- **منصات**
- **لوحات تحكم**
- **أنظمة تسجيل دخول**
- **متاجر إلكترونية**

هذه الأنظمة أكثر شيء يُستهدف في العالم لأن: الكل يستخدمها والنت فيها مفتوح 24 ساعة.

لماذا Web Security مهم؟

لأن معظم بيانات العالم تمر عبر تطبيقات الويب:

- **تسجيل دخول مستخدمين**
- **كلمات مرور**
- **عمليات شراء**
- **بيانات مالية**
- **بيانات حساسة**

وأي نقطة ضعف في الموقع = مهاجم واحد قد يحصل على كل شيء.

أشهر أنواع الثغرات في الويب:

1) SQL Injection

هجوم يدخل فيه المهاجم أوامر SQL داخل مدخلات الموقع
فيغيّر استعلام قاعدة البيانات.

مثال: إذا كان الموقع لا يتحقق من المدخلات
يقدر المهاجم يدخل:

' OR '1'='1

فتظهر له قاعدة البيانات كاملة.

---

2) XSS — Cross Site Scripting

المهاجم يحقن JavaScript داخل الصفحة
فيقوم المتصفح بتنفيذه.

الهدف:

- **سرقة Cookies**
- **سرقة Sessions**
- **تنفيذ أكواد باسم الضحية**

---

3) CSRF — Cross-Site Request Forgery

استغلال جلسة المستخدم لجعله ينفّذ أمر دون علمه.

مثال: المستخدم مسجّل دخول في البنك
المهاجم يرسله رابط
بمجرد الضغط → يتم تحويل الأموال من حسابه!

---

4) Broken Authentication

الأخطاء في نظام الدخول (Login)
مثل:

- **عدم وجود rate limit**
- **كلمات سر ضعيفة**
- **session غير محمية**

هذا يعطي فرصة سهلة للاستيلاء على الحساب.

---

5) Insecure Direct Object Access (IDOR)

وهي أن المهاجم يغيّر رقم بسيط في الرابط ويحصل على بيانات شخص آخر

مثال:

user?id=123/

يغيرها:

user?id=124/

ويشوف بيانات شخص آخر!

كيف نحمي تطبيقات الويب؟

- **Validate inputs — التحقق من المدخلات**
- **Escape output — منع إدخال أكواد ضارة**
- **HTTPS دائمًا — بدون HTTP**
- **كلمات مرور قوية + hash قوي**
- **Session Management محترم**
- **Multi Factor Authentication**
- **استخدام OWASP Top 10 كمرجع**

منظمة OWASP هي المرجع الأول لتأمين الويب.

خلاصة الفصل:

Web Security هو البحر الكبير الذي يجلس فيه الجميع — الشركات، الحسابات، الخدمات، المستخدمين.

هذه هي الجبهة التي يهاجمها الهاكرز يوميًا.

المحترف في Web Security هو شخص خطير... ومحترم جدًا في المجال

الفصل العاشر: الأمن السحابي (Cloud Security)

الأمن السحابي أصبح أساس كل شركة حديثة.
زمان كانت البيانات داخل السيرفرات في مبنى الشركة،
الآن أغلب البيانات موجودة في "سيرفرات سحابيّة" عند شركات مثل:

- **(AWS (Amazon Web Services**
- **Microsoft Azure**
- **(Google Cloud (GCP**

السبب؟
لأن السحابة توفر:

- **سرعة**
- **كفاءة**
- **تخزين ضخم**
- **خدمات جاهزة**
- **تكاليف أقل**

لكن...
الخطر أصبح أكبر.

البيانات لم تعد داخل "غرفة IT" في الشركة
صارت موزعة عبر Data Centers في العالم.

لماذا الأمن السحابي مهم؟

لأن "خطأ إعداد بسيط" في إعدادات السحابة
قد يفتح بيانات ملايين العملاء للعالم!

ولأن الشركات لم تعد تبني أمان من الصفر...
هم يعتمدون على خدمات جاهزة.

وهنا تأتي المشكلة:

السحابة ليست آمنة بحد ذاتها...
الأمان مسؤولية مشتركة.

مسؤولية الأمان في السحابة

هناك مفهوم مهم جدًا في المجال:

Shared Responsibility Model
يعني نموذج المسؤولية المشتركة.

السحابة مسؤولة عن:

- **حماية البنية التحتية**
- **Hardware**
- **Physical security**

العميل (الشركة) مسؤولة عن:

- **التحكم بالوصول**
- **البيانات**
- **الإعدادات**
- **تفعيل التشفير**
- **الحسابات والصلاحيات**

مثال واضح:

AWS تحمي السيرفر
لكن أنتِ المسؤولة عن من يستطيع الدخول إلى السيرفر.

ما هي نقاط الخطر الأساسية في Cloud Security؟

1. **Misconfiguration — إعدادات خاطئة**
   (أخطر شيء — وأشهر سبب اختراقات سحابة)

2. **Weak Access Control — صلاحيات واسعة بدون قيود**

3. **عدم استخدام تشفير Encryption**

4. **عدم مراقبة الـ Logs**
   (بدون Logs = ما تعرفي من دخل ومن خرج)

5. **عدم تفعيل MFA — المصادقة الثنائية**

أفضل ممارسات حماية السحابة

- **Principle of Least Privilege**
  (أعطِ كل مستخدم أقل صلاحية ممكنة فقط لما يحتاجه)
- **استخدام IAM Policies بذكاء**
- **تفعيل Encryption at Rest & in Transit**
- **تفعيل MFA**
- **مراقبة مستمرة عبر CloudWatch / CloudTrail**
- **فحص الإعدادات عبر Security Center**

خلاصة

السحابة = القوة و السرعة
لكن الخطر الحقيقي فيها ليس "الثغرة"
بل الخطأ البشري في الإعدادات

80% من اختراقات Cloud تأتي من Misconfiguration
وليس من ثغرة تقنية.

وهذا ما يجعل الأمن السحابي فنًّا + علمًا في نفس الوقت.

الفصل الحادي عشر: أنواع الهاكرز (Types of Hackers)

ليس كل "هاكر" مجرم.
هذه جملة لازم يفهمها أي شخص يدخل مجال الأمن السيبراني.

الهاكر عبارة عن "عقل يفهم النظام أكثر مما هو ظاهر للآخرين"
لكن كيف يستخدم هذا العقل؟ هذا هو الفاصل.

هناك 3 أنواع أساسية — عالمياً معترف بها:

---

1) White Hat Hackers — القبعة البيضاء

هذا النوع هو "الهاكر الأخلاقي".

- **يعمل مع الشركات**
- **يختبر الأنظمة بطريقة قانونية**
- **يكشف ثغرات ويساعد على سدّها**
- **هدفه حماية الأنظمة**

وظيفته اسمها غالبًا: Ethical Hacker / Pentester / Security Researcher

هذا هو النوع الذي نبني عليه Cybersecurity الصحيح.

---

2) Black Hat Hackers — القبعة السوداء

هذا هو الهاكر المجرم.

- **يعمل بدون إذن**
- **يسرق بيانات**
- **يبتز شركات**
- **يخترق بنظام غير قانوني**

هدفه مادي — إضرار — تجسس — فوضى.

هذا الذي نراه في الأخبار و ransomware gangs.

---

3) Grey Hat Hackers — القبعة الرمادية

هذا النوع "بين الاثنين".

ليس شرير دائمًا، وليس أخلاقي دائمًا.

مثال: يكشف ثغرة ويبلغ عنها... لكن بدون إذن منه أن يفحص النظام.

يستكشف الأنظمة كفضول — ليس من أجل أذى دائم
لكن ليس قانوني 100%.

خلاصة بسيطة

النوع	نيته	قانوني؟
White Hat	**حماية**	**✓ قانوني**
Black Hat	**ضرر / سرقة**	**✗ غير قانوني**
Gray Hat	**بين الإثنين**	**منطقة رمادية**

معلومة مهمة:

معظم أفضل المهندسين الأمنيين في العالم بدأوا من "فضول"
لكن الفرق الحقيقي هو أنه:

الاحتراف = استخدام المعرفة للدفاع و الحماية
وليس للهجوم غير القانوني.

الفصل الثاني عشر: الاستجابة للحوادث (Incident Response)

الاختراق ليس سؤال "هل سيحدث؟"
الاختراق سؤال "متى سيحدث؟"

حتى الشركات الضخمة بأعلى مستوى حماية تتعرض لهجمات.
وهنا يأتي دور "Incident Response" — وهو علم إدارة الحوادث الأمنية.

هذا المجال يعتبر جزء أساسي من Cyber Operations.

ما هو Incident Response؟

هو مجموعة خطوات وإجراءات يتم اتباعها عند اكتشاف أي هجوم أو ثغرة لكي نحتوي الضرر، ونقلل التأثير، ونرجع الأنظمة للعمل بسرعة.

بمعنى آخر:

عندما يحدث اختراق… Incident Response هو الخطة التي تنقذ الشركة.

مراحل الـ Incident Response الرسمية

يوجد 6 مراحل معتمدة عالمياً:

1. **Preparation – التحضير**
   - **سياسة أمنية**
   - **فريق مستعد**
   - **أدوات مراقبة**
   - **نسخ احتياطي (بدون تحضير = كارثة)**
2. **Identification – تحديد الحادث**
   - **هل حدث اختراق فعلاً؟**
   - **هل الحادث خطير؟**
   - **تحليل Logs & Alerts**
3. **Containment – الاحتواء**
   - **عزل الأنظمة المصابة**
   - **منع انتشار الهجوم**
   - **وقف الخسائر**
4. **Eradication – القضاء على التهديد**
   - **حذف البرمجيات الخبيثة**

- تنظيف الأنظمة
- إغلاق الثغرة

5. **Recovery** – الاستعادة

- إعادة الأنظمة للعمل الطبيعي
- مراقبة بعد التعافي
- التأكد أن المهاجم لا يزال داخل النظام

6. **Lessons Learned** – الدروس المستفادة

- تحليل ما حدث
- تحسين السياسات
- كتابة تقرير رسمي
- تطوير الدفاع للمستقبل

لماذا Incident Response مهم؟

لأنه يقلل الخسائر.

بدون Incident Response:

- الشركة قد تخسر ملايين
- بيانات العملاء تضيع
- سمعة الشركة تتدمر
- قد تصل لدرجة إيقاف النشاط

مع Incident Response القوي:

- يتم وقف الاختراق بسرعة
- يتم احتواء الهجوم
- يتم إنقاذ البيانات
- يتم تصحيح الثغرات

ما هي الأدوات المستخدمة عادة؟

- **SIEM systems (مثل Splunk — QRadar — ELK)**
- **Endpoint Detection & Response**
- **Forensic tools**

- **Packet analysers مثل Wireshark**
- **Threat Intelligence platforms**

الخلاصة

Incident Response هو الفرق بين: شركة تنهار في يوم واحد
و
شركة تقف على رجلها وتتعافى باحتراف.

المحترف في Incident Response هو "جندي غرفة العمليات".

الفصل الثالث عشر: التحقيق الجنائي الرقمي (Digital Forensics)

التحقيق الجنائي الرقمي هو العلم الذي يهتم بجمع الأدلة الرقمية وتحليلها بعد وقوع حادث أمني أو اختراق، بهدف معرفة ما الذي حدث بالضبط، وكيف حدث، ومن قام به، ومتى حدث، ثم توثيق النتائج بشكل يمكن الاعتماد عليه قانونيًا.

بمعنى آخر: التحقيق الجنائي الرقمي هو "كشف الحقيقة الرقمية" بعد الهجوم.

لماذا التحقيق الجنائي الرقمي مهم؟

لأنَّ الشركات إذا تعرّضت لهجمة بدون تحقيق جنائي:

- **لن تعرف من المخترق**
- **لن تعرف كيف دخل**
- **لن تعرف كم جلس داخل النظام**
- **ولن تعرف ما الذي سرقه**

التحقيق الجنائي هو الذي يحوّل الفوضى إلى صورة واضحة.

أنواع التحقيق الجنائي الرقمي

النوع	الشرح

Computer Forensics	**تحليل أجهزة الكمبيوتر وأنظمة التشغيل**
Mobile Forensics	**تحليل الهواتف وأجهزة الجوال**
Network Forensics	**تحليل حركة الشبكة والـ Traffic**
Cloud Forensics	**تحليل الأنظمة الموجودة في السحابة**
Memory Forensics	**تحليل الذاكرة RAM للبحث عن آثار الأوامر والبرامج**

مراحل التحقيق الجنائي الرقمي

1. **تحديد الأدلة (Identification)**
   تحديد أين توجد الأدلة: جهاز، شبكة، ذاكرة، سيرفر

2. **حفظ الأدلة (Preservation)**
   نسخ البيانات بطريقة خاصة بدون تغييرها
   لأن تغيير الأدلة يُفقدها قيمتها القانونية

3. **تحليل الأدلة (Analysis)**
   فحص الملفات، مراجعة السجلات، تحليل الشبكة، البحث عن آثار البرمجيات الخبيثة

4. **التوثيق (Documentation)**
   كتابة تقرير دقيق يشرح النتائج وخط سير التحقيق

5. **التقديم (Presentation)**
   تسليم التقرير للإدارة أو المحكمة أو الجهات المختصة

أدوات يستخدمها المحققون الجنائيون

- **Autopsy**
- **FTK**
- **EnCase**
- **Volatility (للذاكرة)**
- **Wireshark (للشبكات)**

هذه الأدوات تساعد في رؤية ما لا يراه المستخدم العادي.

خلاصة الفصل

التحقيق الجنائي الرقمي ليس مجرد "تحليل جهاز"،
هو عملية علمية متكاملة تكشف الحقيقة وتحوّل البيانات إلى أدلة.

بدون Digital Forensics تبقى الشركة عمياء بعد الهجوم.

الفصل الرابع عشر: استخبارات التهديدات (Threat Intelligence)

استخبارات التهديدات هي علم جمع وتحليل معلومات عن الهجمات والجهات المهاجمة، بهدف منع الاختراقات قبل حدوثها.
هي ليست دفاع بعد وقوع الهجوم... بل دفاع "قبل" الهجوم.

نظام الأمن السيبراني بدون Threat Intelligence هو مثل حارس واقف... لكنه أعمى.

ما هي Threat Intelligence؟

هي معلومات دقيقة عن:

- **من يهاجم؟**
- **ما هي تقنياته؟**
- **ما هي أدواته؟**
- **ما هي الثغرات التي يستغلها؟**

- ما هي أهدافه؟
- أين ينتشر؟
- ما هي مؤشرات الإختراق (IoCs)؟

وتُحوّل هذه المعلومات إلى "قرارات دفاعية".

أنواع Threat Intelligence

النوع	الشرح
Strategic	معلومات عالية المستوى لصناع القرار
Operational	معلومات عن نشاط الهجمات الحالية
Tactical	تقنيات وأساليب المهاجمين (TTPs)
Technical	عناوين IP / Domains / Hashes ضارة

ما الذي تبحث عنه Threat Intelligence؟

- بنية المهاجم
- أدوات المهاجم
- بنية الـ Command & Control
- الـ Malware samples
- حملات Phishing جديدة
- Zero-Day Exploits
- Dark Web activity

مصادر Threat Intelligence

- منصات عالمية
- قواعد بيانات ثغرات CVE
- Dark Web Monitoring
- Threat Feeds
- Security Vendors
- SOC reports

أمثلة على منصات مصادر تهديد (بشكل عام من غير روابط):

- feed معلومات يومية عن هجمات جديدة
- تقارير شركات الأمن العالمية
- مواقع CVE والثغرات

لماذا Threat Intelligence مهم؟

لأنه يجعل الشركة:

- تعرف "عدوها" قبل أن يهجم
- تتنبأ بالهجمات قبل وقوعها
- تحسّن الدفاعات بدقة
- ترفع أداء SOC
- تقلل ردّات الفعل العشوائية

بدون Threat Intelligence الدفاع مثل واحد يقاتل في ظلام.

خلاصة الفصل

Threat Intelligence هو "دماغ الأمن السيبراني".
هو الذي يحوّل المعلومات إلى معرفة... والمعرفة إلى حماية.

الفصل الخامس عشر: أنظمة الكشف عن التسلل (IDS) وأنظمة منع التسلل (IPS)

بعد أن تعرّفنا على الهجمات والتحقيق الجنائي واستخبارات التهديدات، نصل الآن إلى واحدة من أهم أدوات الدفاع في الأمن السيبراني:
أنظمة الكشف والمنع

هذه الأنظمة موجودة في قلب الشبكات الكبيرة، وتعمل كـ "عيون" المراقبة الدقيقة داخل الشبكة.

ما هو IDS؟

IDS = Intrusion Detection System
يعني: نظام كشف التسلل

وظيفته الأساسية:

- **يراقب حركة الشبكة (Network Traffic)**
- **يبحث عن أنماط هجمات**
- **يعطي تنبيه عند وجود نشاط مشبوه**

لكن لا يمنع الهجوم
فقط يكشف ويُبلّغ.

هذا النظام "يراقب".

ما هو IPS؟

IPS = Intrusion Prevention System
يعني: نظام منع التسلل

وظيفته:

- **يراقب مثل IDS**
- **لكن يتدخل ويمنع الهجوم مباشرة**

مثال: إذا اكتشف طلب SQL Injection
يقوم بحجبه لحظيًا.

هذا النظام "يراقب + يتصرف".

الفرق بين IDS و IPS

النظام	ماذا يفعل؟
IDS	يكتشف الهجمات ويعطي تنبيه
IPS	يكتشف الهجمات ويمنعها مباشرة

أمثلة عملية

- **IDS مثل كاميرا مراقبة: تشوف السارق وتبلغ**
- **IPS مثل شرطي أمن مسلح: يشوف السارق — ويوقفه**

أنواع IDS / IPS

هناك نوعان أساسيان:

1. **(Network-based (NIDS / NIPS**
   تراقب الشبكة كاملة

2. **(Host-based (HIDS / HIPS**
   تراقب جهاز معين (مثل سيرفر محدد)

لماذا هذه الأنظمة مهمة؟

لأنها:

- **تكتشف الهجمات فور حدوثها**
- **تمنع الهجمات في المرحلة المبكرة**
- **تقلل أضرار الاختراق**
- **تعطي SOC رؤية واضحة للتهديدات**

بدون IDS / IPS
الشبكة "عمياء".

أشهر أمثلة لأنظمة IDS / IPS

- **Snort**
- **Suricata**
- **Palo Alto IPS**
- **Cisco FirePOWER**

خلاصة الفصل

IDS = عيون المراقبة
IPS = الحارس الذي يمنع الهجوم

وجودهما معًا في الشبكة هو ركيزة دفاع أساسية في أي مؤسسة.

الفصل السادس عشر: الجدار الناري (Firewall)

الجدار الناري هو أول خط دفاع في أي شبكة.
هو الحارس الذي يقف عند "بوابة الدخول" ويقرّر:

- **هذا الترافيك يسمح له بالدخول**
- **هذا الترافيك يتم منعه**

الجدار الناري ليس برنامجًا بسيطًا،
بل هو "سياسة + قواعد + تحليل".

ما هو Firewall؟

هو نظام يقوم بـ:

- **تحليل حركة البيانات (Traffic)**
- **تطبيق قواعد Access Control**

- **السماح بالاتصال أو منعه**

الجدار الناري يعمل بين الشبكة الداخلية والشبكات الخارجية (مثل الإنترنت).

لماذا نحتاج Firewall؟

لأن الإنترنت مليء بهجمات ومحاولات مسح ports ومحاولات دخول.

بدون Firewall شبكة الشركة مثل "بيت بدون باب".

أنواع Firewalls

النوع	الشرح
Packet Filtering Firewall	**يقرر بناءً على IP و Port فقط**
Stateful Firewall	**يتابع حالة الاتصال ويحضر السياق**
Application Layer Firewall	**يفحص محتوى التطبيق نفسه (Layer 7)**
Next-Gen Firewall NGFW	**جدار حديث يجمع IDS/IPS وتحليل عميق**

أمثلة على Firewalls مشهورة:

- **Palo Alto Networks**
- **Fortinet FortiGate**
- **Cisco ASA**
- **Check Point**

كيف يعمل Firewall؟

يستخدم قواعد اسمها "ACL) "Access Control List)
وتحدد مثلاً:

- **هذا IP مسموح يدخل**
- **هذا Port ممنوع**
- **هذا بروتوكول محظور**
- **هذا نطاق DNS غير موثوق**

مثال بسيط:

deny tcp any any port 23

هذا يعني:
حظر أي اتصال بروتوكول TCP على port 23 لأن Telnet غير آمن.

علاقة Firewall مع الدفاع العميق

Firewall لوحده ليس كافيًا
لكن هو أساس في "طبقات الحماية" Defense-in-depth

خلاصة الفصل

Firewall هو "البوابة الأمنية" الأصلية في الشبكات.

وكل محترف أمن سيبراني يجب أن يفهمه لأنه محور كل بنية حماية.

الفصل السابع عشر: إدارة الثغرات (Vulnerability Management)

الثغرات الأمنية هي "أبواب مفتوحة" في الأنظمة والتطبيقات،
وإذا لم يتم اكتشافها ومعالجتها — سيستخدمها المهاجمون للدخول.

إدارة الثغرات ليست خطوة واحدة، بل عملية مستمرة طوال حياة النظام.

ما هي إدارة الثغرات؟

هي عملية:

1. **اكتشاف الثغرات**
2. **تصنيفها**
3. **تقييم خطورتها**
4. **معالجتها (تحديث – إغلاق – حذف)**
5. **متابعة تطبيق الإصلاح**

الهدف:
تقليل سطح الهجوم قدر الإمكان.

لماذا إدارة الثغرات مهمة؟

لأن 70% من الهجمات التي تحصل في العالم
هي بسبب ثغرة موجودة "من زمان" ولم تُصلّح.

المهاجم لا يحتاج سحر
يكفيه استغلال خطأ بسيط لم يتم إصلاحه.

مراحل إدارة الثغرات

المرحلة	الشرح
Discovery	**اكتشاف الثغرات عبر scanners**
Prioritization	**تحديد الأكثر خطورة**
Remediation	**إصلاح أو تحديث أو إغلاق**
Verification	**التأكد من أن الثغرة أُغلقت فعلاً**

Reporting **توثيق كل العمليات لعدم تكرار الأخطاء**

أدوات إدارة الثغرات

- **Nessus**
- **OpenVAS**
- **Qualys**
- **Rapid7 Nexpose**

هذه الأدوات تفحص الأنظمة وتظهر قائمة ثغرات مع تقييم خطورتها.

تصنيف خطورة الثغرات

هناك نظام عالمي اسمه:

CVSS Score

يقيم الثغرة من 0 إلى 10

المستوى	التقييم
10 – 9.0	خطير جدًا (Critical)
8.9 – 7.0	عالي High
6.9 – 4.0	متوسط Medium
3.9 – 0.1	منخفض Low

الثغرات "الأعلى خطورة" يجب معالجتها أولًا.

علاقة إدارة الثغرات مع باقي الأمن

- **Penetration Testing يعتمد على الثغرات**
- **Threat Intelligence يحدد ما هو مستهدف حالياً**
- **Incident Response يتوقع هجمات من ثغرات معروفة**

بدون إدارة ثغرات، الأمن مجرد كلام.

خلاصة الفصل

الهجوم لا يبدأ من السماء
الهجوم يبدأ من "ثغرة".

والمحترف هو من يقلل الثغرات قبل أن يجدها المهاجم.

الفصل الثامن عشر: اختبار الاختراق (Penetration Testing)

اختبار الاختراق هو "الهجوم الأخلاقي" بهدف قياس قوة الدفاع. الهدف منه ليس التدمير... بل اكتشاف الثغرات قبل أن يكتشفها المهاجم الحقيقي.

الهاكر الأخلاقي (المختبر) يقوم بمحاكاة هجوم حقيقي
لكن بشكل قانوني — وبإذن من الشركة.

لماذا نحتاج اختبار اختراق؟

لأنك لا تستطيع أن تعرف جودة دفاعك
إلى أن يأتي شخص يحاول اختراقه.

Pen-Testing يكشف أخطاء تقنية لا يمكن أن تراها بالعين
حتى لو كانت أنظمتك تبدو "جيدة".

أنواع اختبار الاختراق

النوع	الشرح
Black Box	المختبر لا يعرف أي معلومات عن النظام
White Box	المختبر يعرف كل التفاصيل (كود – بنية – قواعد)
Grey Box	المختبر يعرف معلومات جزئية فقط

المراحل الأساسية لاختبار الاختراق

1. Reconnaissance جمع معلومات عن الهدف (مثل الـ IP – DNS – اسم الشركة – تقنيات الويب)
2. Scanning فحص المنافذ ← الخدمات ← الثغرات المحتملة
3. Exploitation استغلال الثغرة (أمر ← حقن ← payload ← bypass)
4. Privilege Escalation رفع الصلاحيات من مستخدم عادي إلى Admin / Root
5. Post-Exploitation تحليل البيانات ← استخراج معلومات ← توسع في الشبكة
6. Reporting كتابة تقرير رسمي بالنتائج والثغرات والخطورة والحلول

أدوات يستخدمها مختبر الاختراق

- Nmap
- Metasploit Framework
- Burp Suite
- SQLmap

- **Wireshark**
- **Hydra**
- **John the Ripper**

هذه الأدوات "أسلحة الباحث الأمني" في المعمل.

الفرق بين Pentesting و Hacking

Pentester	Hacker خبيث
يعمل بإذن	يعمل بدون إذن
الهدف حماية	الهدف ضرر أو سرقة
يكتب تقرير وحلول	يخفي أثره

خلاصة الفصل 18

اختبار الاختراق ليس مجرد "هجوم تقني"
هو عملية علمية تكشف نقاط الضعف قبل أن تُستغل.

بدون Pentesting → الأمن مجرد نظري.

الفصل التاسع عشر: أُطر ومعايير الأمن السيبراني (Security Frameworks & Standards)

عند بناء أمن سيبراني فعّال في مؤسسة، لا يكفي وجود أدوات وحدها — تحتاج إلى منهجية منظمة تُوجّه السياسات، العمليات، الأدوار، والتقنيات. هذه المنهجية توجد على شكل أُطر ومعايير قياسية (Frameworks & Standards).

لماذا نحتاج أُطر الأمان؟

- **توحيد الممارسات عبر المؤسسة**
- **ضمان الامتثال للقوانين واللوائح (Compliance)**
- **إدارة المخاطر بطريقة منهجية**
- **قياس مستوى النضج الأمني وتتبع التحسينات**
- **تسهيل المراجعات والتدقيقات (Audits)**

الأطر تعطي "خريطة طريق" واضحة لتحويل الأمن من حالة عشوائية إلى نظام مهني.

أشهر الأُطر والمعايير وماذا تعني

1) ISO/IEC 27001

- **معيار دولي لنظام إدارة أمن المعلومات (ISMS).**
- **يركز على إنشاء سياسات، عمليات، تقييم مخاطر، ضبط وصول، وتحسين مستمر.**
- **يعتمد على عملية PDCA) Plan-Do-Check-Act).**
- **مفيد للمؤسسات التي تريد شهادة رسمية تُظهر التزامها بالأمن.**

2) NIST Cybersecurity Framework (CSF)

- **إطار عملي صدر عن المعهد الوطني الأمريكي للمعايير والتقنية.**
- **مبني حول خمس وظائف رئيسية: Identify, Protect, Detect, Respond, Recover.**
- **مرن ويمكن تكييفه للشركات الحكومية أو الخاصة.**
- **يُستخدم كثيرًا في بيئات البنية التحتية الحيوية.**

3) CIS Controls (Center for Internet Security)

- **مجموعة من الضوابط العملية (Controls) مرتبة حسب الأولوية.**
- **توفر خطوات تقنية محددة (مثل الحماية من البرمجيات الخبيثة، إدارة الثغرات).**
- **مفيد للمؤسسات التي تريد خارطة تنفيذ تقنية سريعة وفعّالة.**

4) PCI-DSS

- **معيار أمني خاص ببطاقات الدفع (Payment Card Industry Data Security Standard).**
- **إلزامي للشركات التي تتعامل ببيانات بطاقات الدفع.**
- **يتضمن متطلبات مشددة حول تشفير، تسجيل الدخول، ومراجعة الأنشطة.**

5) SOC 2

- معيار تقرير للمدققين يقيّم ضوابط الأمن والخصوصية المتعلّقة بخدمات السحابة.
- يتبناه مزودو الخدمات السحابية لإثبات مستوى النضج في الضوابط.

6) MITRE ATT&CK

- ليست إطارًا للامتثال، بل قاعدة معرفية للهجمات (TTPs).
- تُستخدم لفهم سلوك المهاجمين، تحليل الهجمات، وتصميم اكتشافات متقدمة.
- مهم لربط Threat Intelligence مع Detection وResponse.

كيف نختار الإطار المناسب لمؤسستك؟

اعتمدي على ثلاث معايير رئيسية:

1. الهدف (هل تريدين شهادة؟ هل تعملين في قطاع مصرفي؟ هل تحتاجين امتثال قانوني؟)
2. حجم وقيود المؤسسة (شركة ناشئة vs مؤسسة كبيرة)
3. المخاطر والموارد (ميزانية، مهارات فريق، تقنيات موجودة)

مثال عملي:

- شركة تتعامل ببطاقات الدفع → ابدأي بـ PCI-DSS + NIST.
- شركة خدمات سحابية → SOC2 + CIS Controls + MITRE للرد.

خطوات تطبيق إطار أمني عمليًا (منظومة قابلة للتنفيذ)

1. Gap Analysis

- قيّمي الوضع الحالي مقابل متطلبات الإطار.
- سجّلي الفجوات والأولويات.

2. Risk Assessment

- حدّدي الأصول الحيوية، التهديدات، والتأثيرات.
- صنفي المخاطر حسب الأولوية.

3. Governance & Policies

- اكتبّي سياسات أمنية واضحة (Access, Acceptable Use, Data Classification).
- حدّدي المسؤوليات والأدوار.

4. **Technical Controls**

   - **طبّقي الضوابط التقنية من CIS / NIST: إدارة الأصول، إدارة التحديثات، EDR، MFA، تشفير.**

5. **Processes & Playbooks**

   - **أنشئي عمليات Incident Response, Backup, Patch Management.**
   - **صمّمي playbooks للحوادث الشائعة.**

6. **Monitoring & Measurement**

   - **فعّلي SIEM، سجّلي مؤشرات الأداء (KPIs) ومؤشرات النضج (Maturity Metrics).**

7. **Training & Awareness**

   - **درّبي الموظفين، نفّذي اختبارات Phishing، وقيّمي الوعي بانتظام.**

8. **Audit & Continuous Improvement**

   - **قومّي بمراجعات دورية، اختبارات اختراق، وتحسين مستمر.**

الربط بين الأُطر: نهج هجين عملي

ليس من الضروري الالتزام بإطار واحد فقط. أفضل المؤسسات تبني نهجًا هجينيًا:

- **استخدمي NIST CSF كخريطة استراتيجية (Identify → Protect → Detect → Respond → Recover).**
- **طبّقي CIS Controls كقائمة تحقق تقنية يومية.**
- **إن كنتِ تتعاملين بمدفوعات فالتزمي بـ PCI-DSS للمقتضيات القانونية.**
- **استخدمي MITRE ATT&CK لفهم سلوك الخصم وتحسين قواعد الكشف.**
- **إذا أردتِ شهادة رسمية، جهّزي ISO 27001.**

قياس النضج (Maturity Models)

لتعرفي مدى تقدمك، استخدمي مقياس نضج من 1 إلى 5، حيث:

1. **Initial — ممارسات غير رسمية.**

2. **Managed — عمليات متكررة لكن غير موثقة جيدًا.**
3. **Defined — سياسات موثقة وعمليات واضحة.**
4. **Measured — مراقبة وقياس، تحسّن مدعوم بالبيانات.**
5. **Optimized — تحسين مستمر، أتمتة، وقيادة استراتيجية.**

هدفك أن تصعدي من مستوى إلى مستوى عبر خطط سنوية.

نصائح عملية للمديرين والمهندسات

- **لا تحاولي تنفيذ كل شيء مرة واحدة — ابدئي بالأولوية (High-impact, Low-effort controls).**
- **اجعلي مؤشر قابل للقياس: مثلاً تقليل الثغرات الحرجة بنسبة 80% خلال 6 أشهر.**
- **اجمعي تقارير بسيطة وقابلة للقراءة للمدير (dashboards مع مؤشرات أساسية).**
- **استثمري في التدريب — أدوات قوية بدون كفاءات لا تفيد.**
- **احفظي نسخ من السياسات والإجراءات ودوّني عمليات التغيير (Change log).**

خاتمة الفصل

الأُطر والمعايير هي خارطة الطريق التي تحوّل الأمن من نشاط عشوائي إلى نظام عملي متين.
الفرق بين شركة تصدق بوجود أمن وبين شركة تملك أمنًا فعليًا — هو وجود إطار منظم، تطبيق عملي، ومراجعة مستمرة.

الفصل العشرون: الخاتمة ومسار المهنة في الأمن السيبراني

بعد هذا الكتاب الطويل الذي أخذنا فيه رحلة عبر أساسيات الأمن السيبراني، مراحله، أدواته، أنظمته، طبقاته، مسؤولياته، وتقنياته، نصل الآن للخطوة الأهم:

كيف تتحولين من قارئة إلى مهندسة أمن سيبراني فعلية؟

النجاح في هذا المجال لا يعتمد على الحظ...
ولا على الموهبة فقط...
بل يعتمد على:

- **الفضول الحقيقي**
- **الاستمرارية**

- **الممارسة العملية**
- **بناء عقلية تفكير أمني (Security Mindset)**

لماذا الأمن السيبراني مجال مختلف؟

لأن الأمن السيبراني ليس معرفة "ثابتة".
الأمن السيبراني "متغيّر" و "حيّ".

هناك ثغرات جديدة كل يوم،
أدوات جديدة كل يوم،
هجمات جديدة كل يوم.

لو توقفت عن التعلم — تتراجع.
لو استمريت — تتفوق.

خارطة الطريق لبناء مهندس/مهندسة أمن سيبراني

1. **لغة إنجليزية قوية**
   لأن كل المحتوى العالمي، الأدوات، التقارير — بالإنجليزية.

2. **فهم الشبكات بعمق**
   لأن الأمن = Traffic + Packets + Protocols.

3. **لينُكس Linux**
   لأنه نظام الباحث الأمني الأول.

4. **تعلّم Web Security وبالأخص OWASP Top 10.**

5. **أدوات الأمن العملي مثل:**
   Nmap — Burp Suite — Metasploit — Wireshark.

6. **مشاريع عملية / Labs**
   ممارسة حقيقية على أنظمة افتراضية.

أهم صفات الباحث الأمني الناجح

- **يشك دائمًا — لا يثق في المدخلات ولا المواقع ولا الروابط**
- **لا يقبل بما يراه على السطح — يحلل العمق**
- **يسأل "لماذا؟" قبل "كيف؟"**
- **لا يخاف من الفشل — لأن كل تجربة = خبرة**

الأمن السيبراني ليس وظيفة... الأمن السيبراني سلاح

سلاح الدفاع عن:

- **خصوصية الناس**
- **اقتصاد الدول**
- **بيانات الشركات**
- **مستقبل التقنية**

ومهندسة الأمن السيبراني ليست مجرد موظفة...
هي خط الدفاع الأول.

ختام

إذا وصلت إلى هنا — فأنت الآن تمتلك أساسًا معرفيًا متينًا يمكن البناء عليه...
وهذا الكتاب هو بداية "هوية مهنية" لك — وليس نهاية.

أنت الآن لا تمشي في طريق جاهز
أنت تصنع طريقك.

استمر في التعلّم — كل يوم — ولو خطوة صغيرة.
وفي يوم ما...

ستصبح أنت المصدر
وليس المتعلّم فقط.
