



# **100Cyber-3: Cybersecurity Foundation**

**Dr. Mohammed Alshahrani**  
**[moaalshahrani@nu.edu.sa](mailto:moaalshahrani@nu.edu.sa)**

**First Lecture**

**Sunday, Sep. 15 2024**

# Today...

---


- مفاهيم بالأمن السيبراني
- الفرق بين أمن المعلومات والأمن السيبراني
- أهداف الأمن السيبراني
- ابرز مخاطر الأمن السيبراني
- انواع الهجمات في الأمن السيبراني
- اساليب هجمات الإختراق السيبراني
- اجراءات الوقاية من الإختراق السيبراني
- مخاطر الفضاء السيبراني على الأطفال خصوصا و الشباب
- وصايا للحفاظ على صغار السن من الفضاء السيبراني
- وصايا حول اختيار كلمة المرور
- كيف تحمي بيانات المؤسسة من الاختراق السيبراني

# Course Description

- introduces cybersecurity, the fundamental principles of identifying risk, the foundation for protecting information assets by implementing security controls. In addition, you will explore the legal and ethical basis for cybersecurity work. The course aligns with the compTI security +certification alongside CYBER150 it will prepare you to take the CompTIA Security +exam by providing coverage of the objectives. This course is a prerequisite CYBER150



# Course Objectives

- apply foundational cybersecurity concepts.
  - Assess the security posture of an enterprise environment and recommend appropriate security solutions.
  - Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
- 

# Assessment Tasks for Students

Assessment task	Percentage of Total Assessment Score
Quizzes and HomeWorks	10%
Midterm 1	20%
project	20%
Final Exam	50%

# Required Textbooks

## Essential References

- CompTIA Integrated CertMaster Learn + Labs for Security+, ISBN: 978-1-64274-336-4
- CompTIA CertMaster Practice for Security+, ISBN: 978-1-64274-333-3
- Cyber Security: The complete guide to cyber threats and protection, 2nd edition, BCS, 2022, David Sutton, ISBN-10: 1780175957
- Security in Computing, 6th edition Published by Addison-Wesley Professional (July 26, 2023) © 2024

## Electronic Materials

- CompTIA Integrated CertMaster Learn + Labs for Security+, ISBN: 978-1-64274-336-4
- CompTIA CertMaster Practice for Security+, ISBN: 978-1-64274-333-3
- CompTIA LMS

# مفاهيم الأمن السيبراني cybersecurity

- ماذا نقصد بكلمة **سيبراني**: يقصد بها الفضاء الإلكتروني أو فضاء الانترنت.
- **الفضاء الإلكتروني أو فضاء الانترنت**: مصطلح يطلق على عناصر الوسط الذي تتواجد فيه البيانات الرقمية وأمكن تخزينها والتعامل معها. وتضم كل من أجهزة الحاسب والهواتف الذكية وأنظمة الشبكات والبرمجيات وحوسبة المعلومات ونقل وتخزين البيانات ومستخدمي كل هذا العناصر.
- **الأمن السيبراني** الأمن السيبراني هو ممارسة حماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والشبكات والبيانات من الهجمات الخبيثة. يشمل الأمن السيبراني تقنيات وإجراءات بشرية لحماية الأنظمة من الوصول غير المصرح به أو التهديدات.

# الفرق بين أمن المعلومات والأمن السيبراني يتمثل في نطاق كل منهما والتركيز على المجالات المختلفة التي يسعى كل منهما لحمايتها:

## • أمن المعلومات (Information Security)

• **النطاق:** أمن المعلومات هو مفهوم أوسع يركز على حماية جميع أنواع المعلومات، سواء كانت رقمية أو غير رقمية، من الوصول غير المصرح به، أو التعديل، أو فقدان. يشمل حماية البيانات بغض النظر عن شكلها، سواء كانت محفوظة على الورق، في أجهزة إلكترونية، أو حتى مخزنة في العقول البشرية.

• **الهدف:** يهدف إلى ضمان سرية (Confidentiality)، سلامة (Integrity)، وتوافر (Availability) المعلومات المعروف باسم مثلث (CIA).

## • المجالات:

- حماية الوثائق الورقية
- حماية البيانات الرقمية المخزنة على أجهزة الكمبيوتر أو في قواعد البيانات
- حماية المعلومات التي يتم تداولها شفهيًا أو كتابيًا

## • الأمثلة:

- وضع سياسة قوية لتخزين الوثائق الحساسة
- تنفيذ إجراءات مثل النسخ الاحتياطي لحماية المعلومات الهامة والمعلومات الرقمية من الهجمات الإلكترونية.



# الفرق بين أمن المعلومات والأمن السيبراني يتمثل في نطاق كل منهما والتركيز على المجالات المختلفة التي يسعى كل منهما لحمايتها:

- الأمن السيبراني (Cybersecurity)
- **النطاق:** الأمن السيبراني هو جزء من أمن المعلومات ولكنه يركز على حماية الأنظمة، الأجهزة، الشبكات، والبيانات الموجودة في الفضاء الإلكتروني أو المتصلة بالإنترنت من الهجمات الإلكترونية. بمعنى آخر، يركز الأمن السيبراني بشكل خاص على حماية المعلومات الرقمية والبنية التحتية التقنية.
- **الهدف:** يهدف إلى حماية الأنظمة والشبكات من التهديدات الإلكترونية مثل الهجمات السيبرانية، الفيروسات، برامج الفدية، التصيد الاحتيالي، وغيرها من الهجمات الرقمية.
- **المجالات:**
  - حماية الأجهزة والشبكات من الهجمات السيبرانية
  - الدفاع ضد البرمجيات الخبيثة (Malware)
  - مراقبة التهديدات واكتشاف الاختراقات في الأنظمة
- **الأمثلة:**
  - تركيب جدران نارية (Firewalls) وأنظمة كشف التسلل
  - تأمين شبكات الشركات ضد هجمات الاختراق
- **الخلاصة:**
  - أمن المعلومات يشمل جميع جوانب حماية المعلومات سواء كانت فيزيائية أو رقمية.
  - الأمن السيبراني يركز فقط على حماية الأنظمة والشبكات والبيانات في الفضاء الإلكتروني.
  - باختصار، الأمن السيبراني هو مجال فرعي من أمن المعلومات مخصص لحماية المعلومات الرقمية من الهجمات الإلكترونية.

# أهداف الأمن السيبراني

- تهدف بشكل أساسي إلى حماية المعلومات الرقمية، والأنظمة، والشبكات من التهديدات السيبرانية والهجمات الإلكترونية. تتمحور هذه الأهداف حول مجموعة من المبادئ الأساسية التي تُعرف باسم مثلث CIA، بالإضافة إلى جوانب أخرى تتعلق بالاستمرارية والامتثال. وفيما يلي الأهداف الرئيسية للأمن السيبراني:

## 1. السرية (Confidentiality)

- الهدف هو حماية المعلومات من الوصول غير المصرح به أو الكشف عنها للأشخاص أو الجهات التي لا تملك الإذن.
- أمثلة:

- استخدام تقنيات التشفير لحماية البيانات.
- فرض ضوابط وصول قوية مثل المصادقة الثنائية (MFA) للتأكد من أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى المعلومات الحساسة.

## 2. سلامة المعلومات (Integrity)

- الهدف هو ضمان أن المعلومات تبقى صحيحة وغير معدلة أو مدمرة بدون إذن.
- أمثلة:

- استخدام تقنيات مثل الهاش (Hashing) لضمان أن البيانات لم يتم تغييرها أثناء النقل.
- أنظمة إدارة الوصول التي تتحكم في من يمكنه تعديل أو حذف المعلومات.

## 3. التوافر (Availability)

- الهدف هو ضمان أن الأنظمة والمعلومات متاحة عند الحاجة إليها للأشخاص المصرح لهم بذلك.
- أمثلة:

- ضمان وجود نسخ احتياطية من البيانات والأنظمة.
- إنشاء خطط استمرارية العمل (BCP) للتعامل مع الأعطال أو الهجمات مثل هجمات حجب الخدمة (DDoS).

# أهداف الأمن السيبراني

## 4. المصادقة (Authentication)

- الهدف هو التحقق من هوية المستخدمين أو الأنظمة التي تطلب الوصول إلى البيانات.
- أمثلة:

- استخدام كلمات مرور قوية وأنظمة تحقق متعددة العوامل للتأكد من أن الشخص الذي يحاول الوصول إلى النظام هو الشخص المصرح له بذلك.

## 5. التتبع والمساءلة (Accountability)

- الهدف هو تتبع جميع الأنشطة التي تتم على النظام لضمان أن جميع المستخدمين يمكن تتبعهم في حالة حدوث مشكلة أو خرق.
- أمثلة:

- تسجيل الأنشطة على الأنظمة واستخدام سجلات التدقيق (Audit Logs) لتتبع الأنشطة الخبيثة.

## 6. المرونة (Resilience)

- الهدف هو ضمان أن الأنظمة يمكن أن تتعافى بسرعة بعد الهجمات أو الأعطال وتستمر في العمل بشكل طبيعي.
- أمثلة:

- وضع خطط للتعافي من الكوارث (DRP).
- استخدام بنية تحتية مرنة وقابلة للتكيف مع التهديدات المتغيرة.

## أهداف الأمن السيبراني

### 7. الامتثال (Compliance)

- الهدف هو الامتثال للقوانين واللوائح المعمول بها في مجال حماية المعلومات والخصوصية.
- أمثلة:
  - الامتثال لتشريعات مثل اللائحة العامة لحماية البيانات (GDPR) أو معايير صناعة بطاقات الدفع (PCI-DSS)

### 8. إدارة المخاطر (Risk Management)

- الهدف هو تحديد المخاطر السيبرانية وتقليل تأثيرها على الأنظمة والمعلومات.
- أمثلة:
  - تقييم المخاطر وتطوير استراتيجيات للتخفيف منها، مثل تطبيق تدابير أمنية إضافية أو تقليل الاعتماد على الأنظمة الحساسة.

# أهداف الأمن السيبراني

## الخلاصة:

- الأمن السيبراني يهدف إلى حماية السرية، سلامة المعلومات، وتوافر الأنظمة، إضافةً إلى المصادقة، التتبع، المرونة، الامتثال، وإدارة المخاطر. كل هذه الأهداف تهدف إلى توفير بيئة آمنة تضمن استمرارية العمل وحماية المعلومات الرقمية من التهديدات السيبرانية.

# المخاطر التي تواجه الأمن السيبراني

• المخاطر التي تواجه الأمن السيبراني اليوم، وتتنوع هذه المخاطر بناءً على نوع الهجمات والأساليب التي يستخدمها المهاجمون. فيما يلي أبرز مخاطر الأمن السيبراني:

## 1. البرمجيات الخبيثة (Malware)

- البرمجيات الخبيثة تشمل الفيروسات، وبرامج التجسس، وبرامج الفدية، وأحصنة طروادة ((Trojans، وغيرها. هذه البرمجيات تهدف إلى تدمير الأنظمة أو سرقة المعلومات.
- مثال: *WannaCry* هو هجوم ببرنامج الفدية أدى إلى تشفير بيانات ملايين المستخدمين حول العالم، وطالب بفدية ل فك تشفيرها.

## 2. هجمات التصيد الاحتيالي (Phishing)

- هجمات التصيد الاحتيالي تهدف إلى خداع المستخدمين للكشف عن معلوماتهم الحساسة مثل كلمات المرور أو تفاصيل بطاقات الائتمان، عن طريق رسائل بريد إلكتروني أو مواقع إلكترونية مزيفة.
- مثال: يحصل المستخدم على رسالة بريد إلكتروني تدّعي أنها من مصرفه، تطلب منه تحديث بياناته عبر رابط وهمي يؤدي إلى موقع تصيد.

## 3. هجمات حجب الخدمة الموزعة (DDoS)

- تهدف هجمات حجب الخدمة إلى إغراق خادم أو شبكة معينة بعدد هائل من الطلبات، مما يؤدي إلى تعطيل الخدمة وجعلها غير متاحة للمستخدمين الشرعيين.
- مثال: في عام 2016، هجوم *DDoS* على مزود *DNS Dyn* أدى إلى تعطيل العديد من المواقع الكبيرة مثل تويتر وأمازون.

## 4. الهجمات الداخلية (Insider Threats)

- التهديدات الداخلية تحدث عندما يقوم شخص داخل المنظمة (موظف، مقاول، أو شريك) بإساءة استخدام صلاحياته للوصول إلى المعلومات الحساسة أو تعطيل النظام.
- مثال: موظف ساخط يقوم بتسريب معلومات حساسة أو تثبيت برمجيات خبيثة على الشبكة الداخلية للشركة.

# المخاطر التي تواجه الأمن السيبراني

## 5. الثغرات غير المصححة (Unpatched Vulnerabilities)

- عدم تحديث البرمجيات أو الأنظمة بانتظام يمكن أن يترك ثغرات يمكن استغلالها من قبل القرصنة. هذه الثغرات تكون عادة في البرمجيات التي لم تتلقَ تصحيحات الأمان الضرورية.
- مثال: اختراق Equifax في عام 2017 كان بسبب ثغرة غير مصححة في برنامج Apache Struts، مما سمح للقرصنة بسرقة معلومات شخصية لملايين المستخدمين.

## 6. هجمات البرامج الفدية (Ransomware)

- البرامج الفدية تشفر ملفات المستخدمين وتطالب بدفع فدية مقابل استعادة الوصول إلى الملفات. هذه الهجمات شائعة جدًا في المؤسسات الكبيرة مثل المستشفيات أو البنوك.
- مثال: الهجمات على المستشفيات التي تستخدم البرامج الفدية تؤدي إلى تشفير سجلات المرضى، مما يوقف العمليات الطبية حتى يتم دفع الفدية.

## 7. الهجمات على سلسلة التوريد (Supply Chain Attacks)

- هجوم سلسلة التوريد يحدث عندما يقوم المهاجمون باستهداف مزود أو شريك في سلسلة توريد الشركة لزرع برامج خبيثة أو استغلال الثغرات للوصول إلى الأنظمة الرئيسية.
- مثال: هجوم SolarWinds في عام 2020 حيث تم استغلال تحديث برمجي مشبوه من مزود موثوق به لاختراق أنظمة العديد من الشركات والحكومات.

## 8. الهندسة الاجتماعية (Social Engineering)

- تعتمد هجمات الهندسة الاجتماعية على خداع الأفراد للكشف عن معلومات حساسة أو تنفيذ إجراءات معينة من خلال الاستغلال النفسي.
- مثال: يتصل المخترق بموظف ويدعي أنه من قسم الدعم الفني ويطلب منه كلمة المرور لتحديث النظام.

## 9. التهديدات المتقدمة المستمرة (APT - Advanced Persistent Threats)

- الهجمات المتقدمة المستمرة هي هجمات طويلة الأمد تقوم بها جهات ذات قدرات عالية، غالبًا ما تكون دول أو مجموعات منظمة. الهدف هو سرقة المعلومات الحساسة أو التجسس على الأنظمة.
- مثال: مجموعة APT28 الروسية قامت بهجمات طويلة الأمد ضد مؤسسات حكومية وعسكرية بهدف التجسس.

# المخاطر التي تواجه الأمن السيبراني

## 10. تهديدات إنترنت الأشياء (IoT Threats)

- مع تزايد استخدام أجهزة إنترنت الأشياء ((IoT)، تزداد المخاطر المرتبطة بها، حيث أن العديد من هذه الأجهزة تأتي بتدابير أمنية ضعيفة، مما يجعلها هدفاً للهجمات.
- مثال: اختراق كاميرات المراقبة المنزلية المتصلة بالإنترنت أو أجهزة التوجيه (Routers) التي تُستخدم للدخول إلى الشبكات المنزلية.

## 11. سرقة الهوية (Identity Theft)

- سرقة الهوية هي استخدام معلومات شخصية مثل أسماء المستخدمين وكلمات المرور أو أرقام بطاقات الائتمان للوصول إلى الحسابات أو ارتكاب جرائم باسم الضحية.
- مثال: يقوم أحد المخترقين بسرقة بيانات البطاقة الائتمانية للمستخدم من خلال هجوم تصيد أو اختراق قاعدة بيانات، ثم يستخدمها لإجراء عمليات شراء غير مصرح بها.
- الخلاصة:
- الأمن السيبراني يواجه العديد من المخاطر التي تتطور باستمرار. من بين هذه المخاطر: البرامج الخبيثة، التصيد الاحتيالي، هجمات حجب الخدمة، التهديدات الداخلية، الثغرات غير المصححة، هجمات الفدية، والهجمات على سلسلة التوريد. لذلك، يجب أن تكون المؤسسات على دراية بهذه المخاطر وأن تتخذ التدابير اللازمة لتقليل تأثيرها.



# المخاطر التي تواجه الأمن السيبراني

ما هي أنواع الهجمات؟

هناك العديد من أنواع الهجمات السيبرانية التي يستخدمها القراصنة والمهاجمون لاستهداف الأنظمة والشبكات والمعلومات. كل نوع من هذه الهجمات له تقنيات واستراتيجيات مختلفة لتحقيق هدفه. فيما يلي أبرز أنواع الهجمات السيبرانية:

1. الهجمات بالبرمجيات الخبيثة (Malware Attacks): البرمجيات الخبيثة هي أي برامج أو تعليمات برمجية ضارة يتم إدخالها إلى جهاز الكمبيوتر أو الشبكة بهدف التسبب في ضرر أو سرقة معلومات.

• أمثلة على البرمجيات الخبيثة:

- الفيروسات: برامج تنتشر عبر إصابة ملفات أخرى وتدمير البيانات.
- الدودة (Worms): تنتشر عبر الشبكات وتستغل الثغرات الأمنية.
- أحصنة طروادة (Trojans): تبدو كبرامج شرعية لكنها تحتوي على شيفرات خبيثة.
- برامج الفدية (Ransomware): تشفر بيانات المستخدمين وتطالب بفدية لفك التشفير.
- برامج التجسس (Spyware): تراقب الأنشطة السرية للمستخدمين مثل تسجيل لوحة المفاتيح.

# المخاطر التي تواجه الأمن السيبراني

## 2. التصيد الاحتيالي (Phishing Attacks)

- التصيد الاحتيالي هو محاولة خداع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو تفاصيل بطاقات الائتمان
- عن طريق إرسال رسائل بريد إلكتروني أو رسائل تبدو وكأنها من مصادر موثوقة.

### • أنواع التصيد الاحتيالي:

- **التصيد التقليدي:** يتم عن طريق البريد الإلكتروني الذي يحتوي على رابط لموقع مزيف.
- **التصيد بالرمح (Spear Phishing):** هجوم مستهدف يوجه إلى فرد معين أو منظمة.
- **التصيد عبر الهاتف (Vishing):** التصيد الاحتيالي عبر الهاتف لطلب معلومات شخصية.
- **التصيد عبر الرسائل النصية (Smishing):** يتم من خلال الرسائل النصية التي تحتوي على روابط خبيثة.

## 3. هجمات حجب الخدمة (Denial of Service - DoS)

- هجوم حجب الخدمة (DoS) هو محاولة تعطيل خدمة أو شبكة بجعلها غير متاحة للمستخدمين من خلال إغراق الخادم بالطلبات.
- **هجوم حجب الخدمة الموزع (DDoS):** يتم بواسطة العديد من الأجهزة التي تعمل معًا لإغراق الخادم بالطلبات، مما يجعله
- غير قادر على الاستجابة للمستخدمين الشرعيين.

# المخاطر التي تواجه الأمن السيبراني

## 4. الهجمات باستخدام الثغرات الأمنية (Exploitation Attacks)

• استغلال الثغرات الأمنية يعني استغلال نقطة ضعف في نظام أو برنامج معين للسيطرة عليه أو الوصول إلى معلومات حساسة.  
• أمثلة:

- **هجمات الحقن (Injection Attacks):** مثل هجوم حقن SQL الذي يستغل ضعفاً في قاعدة البيانات لسرقة المعلومات أو تعديلها.
- **تجاوز المصادقة (Authentication Bypass):** استغلال ثغرات المصادقة للوصول غير المصرح به إلى الأنظمة.

## 5. هجمات رجل في الوسط (Man-in-the-Middle - MitM)

• **في هجمات رجل في الوسط،** يقوم المهاجم باعتراض الاتصال بين طرفين (مثل المستخدم والخادم) دون أن يعلم الطرفان بذلك، ليقوم بسرقة البيانات أو تعديلها.  
• **مثال:** هجوم على شبكة Wi-Fi عامة حيث يتم اعتراض البيانات المتبادلة بين المستخدم والخادم.

## 6. الهجمات على كلمات المرور (Password Attacks)

• هي محاولات لسرقة أو كسر كلمات المرور للدخول إلى الحسابات أو الأنظمة.  
• أنواع الهجمات:

- **الهجمات بالقوة الغاشمة (Brute Force Attack):** محاولة تخمين كلمة المرور من خلال تجريب كافة التشكيلات الممكنة.
- **هجوم القاموس (Dictionary Attack):** استخدام قائمة من الكلمات الشائعة لتخمين كلمة المرور.
- **هجمات إعادة استخدام كلمات المرور:** استغلال كلمات المرور التي تم تسريبها سابقاً لاختراق حسابات أخرى.

# المخاطر التي تواجه الأمن السيبراني

## 7. الهندسة الاجتماعية (Social Engineering Attacks)

الهندسة الاجتماعية هي محاولة خداع الأشخاص للكشف عن معلومات حساسة أو تنفيذ إجراءات معينة من خلال استغلال الثقة أو الخداع النفسي.  
• أمثلة:

• **التنكر (Pretexting):** ادعاء المهاجم أنه شخصية شرعية للحصول على معلومات.

• **الإغراء (Baiting):** تقديم شيء مغري مثل جهاز USB يحتوي على برامج خبيثة.

## 8. الهجمات المتقدمة المستمرة (Advanced Persistent Threats - APT)

التهجمات المتقدمة المستمرة هي هجمات طويلة الأمد تستهدف المؤسسات أو الحكومات. يستخدم المهاجمون تقنيات متقدمة ويظلون داخل النظام لفترة طويلة لجمع المعلومات الحساسة.

• **مثال:** هجمات التجسس التي تنفذها دول قومية على حكومات أو شركات أخرى للحصول على أسرار صناعية أو عسكرية.

# المخاطر التي تواجه الأمن السيبراني

## 9. هجمات سلسلة التوريد (Supply Chain Attacks)

• في هجمات سلسلة التوريد، يتم استهداف الشركات أو الموردين المتعاملين مع الهدف الرئيسي. يتمكن المهاجم من اختراق أنظمة الشركات الموردة أو الشركاء للوصول إلى الهدف.  
• مثال: هجوم *SolarWinds* في 2020 حيث تم اختراق برنامج إدارة الشبكة الذي تستخدمه العديد من الشركات الكبرى والحكومات.

## 10. التهديدات الداخلية (Insider Threats)

• التهديدات الداخلية تأتي من الأشخاص الذين لديهم وصول شرعي إلى الأنظمة أو المعلومات (موظفين، مقاولين، أو شركاء) لكنهم يستغلون هذا الوصول بطريقة غير قانونية.  
• مثال: موظف ساخط يقوم بسرقة بيانات سرية من الشركة وبيعها للمنافسين.

## 11. هجمات الاستهداف (Zero-Day Attacks)

• هجمات الاستهداف تستغل ثغرات غير معروفة سابقًا في البرمجيات أو الأنظمة، والتي لم يتم تصحيحها بعد من قبل الشركة المطورة. تُعتبر هذه الهجمات خطيرة لأن المستخدمين والمطورين لم يكونوا على دراية بوجودها.  
• مثال: استغلال ثغرة جديدة في متصفح إنترنت شائع قبل أن يتم إصلاحها من خلال التحديثات.

# المخاطر التي تواجه الأمن السيبراني

الخلاصة:

تتنوع الهجمات السيبرانية وفقاً للتقنيات والأساليب المستخدمة. من أشهرها الهجمات بالبرمجيات الخبيثة، التصيد الاحتيالي، هجمات حجب الخدمة، وهجمات كلمات المرور. يجب على المؤسسات والأفراد أن يكونوا على دراية بهذه الأنواع من الهجمات لاتخاذ التدابير الوقائية المناسبة وحماية أنظمتهم ومعلوماتهم.

# أساليب الهجمات في الأمن السيبراني

- أساليب الهجمات في الأمن السيبراني متنوعة وتتطور باستمرار مع تطور التكنولوجيا. يستخدم المهاجمون
- تقنيات مبتكرة لاستهداف الأنظمة والشبكات، سواء كانت هذه الهجمات تهدف إلى سرقة
- البيانات أو تعطيل الخدمات أو الحصول على مكاسب مالية. فيما يلي أهم أساليب هجمات الأمن السيبراني:

## 1. الهجمات بالقوة الغاشمة (Brute Force Attack)

- تعتمد هذه الهجمات على محاولة تخمين كلمات المرور أو مفاتيح التشفير من خلال تجربة جميع التشكيلات
- الممكنة حتى يتم العثور على التشكيل الصحيح.
- أسلوب العمل: يقوم المهاجم بتشغيل برامج تختبر كلمات مرور مختلفة بسرعة كبيرة.
- التقنيات المستخدمة: برامج مثل *John the Ripper* أو *Hydra* تُستخدم لتجربة مئات الآلاف من كلمات المرور خلال ثوانٍ.

# أساليب الهجمات في الأمن السيبراني

## 2. هجمات التصيد الاحتيالي (Phishing)

- هجوم التصيد الاحتيالي يعتمد على خداع المستخدمين لجعلهم يفصحون عن معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.
- أسلوب العمل: يتم إرسال بريد إلكتروني أو رسالة تبدو وكأنها من مصدر موثوق (مثل البنك)، وتطلب من الضحية تقديم معلوماته من خلال موقع مزيف.
- التقنيات المستخدمة: تقنيات التزييف البصري وتصميم المواقع المشابهة لتلك الأصلية لخداع الضحية.

## 3. الهندسة الاجتماعية (Social Engineering)

- الهندسة الاجتماعية تعتمد على التفاعل البشري لخداع الأفراد وإقناعهم بالكشف عن معلومات حساسة أو اتخاذ إجراءات معينة تتيح للمهاجم الوصول إلى الأنظمة.
- أسلوب العمل: المهاجم يتصل بالضحية ويدّعي أنه من الدعم الفني، ويطلب كلمة المرور لتحديث الحساب أو لإصلاح مشكلة ما.
- التقنيات المستخدمة: الإقناع النفسي، والتلاعب بالثقة.



# أساليب الهجمات في الأمن السيبراني

## 4. هجمات حقن (SQL Injection) SQL

- في هذا النوع من الهجمات، يستغل المهاجم ثغرات في استعلامات قواعد البيانات لإدخال أوامر SQL غير متوقعة، ما يسمح له بالتلاعب في البيانات أو الوصول إليها.
- أسلوب العمل: يدخل المهاجم سطرًا من أوامر SQL في حقل إدخال مثل نموذج تسجيل الدخول، مما يؤدي إلى تغيير استعلام قاعدة البيانات لصالحه.
- التقنيات المستخدمة: استغلال استعلامات SQL غير محمية وإدخال أوامر خبيثة مباشرة في قواعد البيانات.

## 5. هجمات حجب الخدمة الموزعة (DDoS)

- تعتمد هجمات DDoS على إغراق النظام المستهدف أو الخادم بعدد هائل من الطلبات غير الشرعية مما يؤدي إلى تعطيل الخدمة أو إيقافها.
- أسلوب العمل: يستخدم المهاجم شبكة من الأجهزة المصابة (البوت نت) لإرسال عدد كبير من الطلبات إلى الخادم، مما يتسبب في زيادة الحمل على الخادم ويعطله.
- التقنيات المستخدمة: شبكات بوت نت، وأجهزة تم اختراقها مسبقًا مثل الكاميرات الذكية أو أجهزة التوجيه (routers)

## أساليب الهجمات في الأمن السيبراني

### 6. هجمات رجل في الوسط (Man-in-the-Middle – MitM)

- في هذه الهجمات، يقوم المهاجم بالتنصت أو اعتراض الاتصالات بين طرفين دون علمهما، مما يسمح له بسرقة أو تعديل البيانات.
- أسلوب العمل: يضع المهاجم نفسه بين المستخدم والموقع الذي يتصل به (مثل بين مستخدم وخادم البنك)، ويسرق البيانات المتبادلة بينهما.
- التقنيات المستخدمة: برمجيات اعتراض مثل *Wireshark* أو الهجمات على شبكات Wi-Fi غير آمنة.

### 7. هجمات التلاعب بالبروتوكولات (Protocol Manipulation)

- يقوم المهاجم باستغلال نقاط الضعف في بروتوكولات الاتصال المستخدمة في الشبكات مثل بروتوكول DNS أو HTTP.
- أسلوب العمل: على سبيل المثال، يمكن للمهاجم تنفيذ هجوم تحويل (DNS Spoofing) لتحويل المستخدمين من المواقع الأصلية إلى مواقع مزيفة.
- التقنيات المستخدمة: استغلال الثغرات في طبقات الشبكة مثل طبقة النقل أو التطبيق.

## 8. هجمات البرمجيات الخبيثة (Malware Attacks) أساليب الهجمات في الأمن السيبراني

- البرمجيات الخبيثة تتنوع ما بين الفيروسات، الديدان (Worms)، وأحصنة طروادة (Trojans)، وكلها تهدف إلى إلحاق الضرر بالنظام أو سرقة المعلومات.
- أسلوب العمل: يقوم المهاجم بتهيئة برنامج خبيث على جهاز الضحية، يمكنه أن يؤدي مهام خبيثة مثل تدمير البيانات أو التجسس على المستخدم.
- التقنيات المستخدمة: برمجيات خبيثة تنتشر عبر البريد الإلكتروني أو من خلال التنزيلات من مواقع غير موثوقة.

## 9. هجمات تجاوز المصادقة (Authentication Bypass)

- يتم استغلال ثغرات في أنظمة المصادقة لتجاوز عمليات تسجيل الدخول والدخول إلى النظام دون الحاجة إلى تقديم بيانات الاعتماد الصحيحة.
- أسلوب العمل: يقوم المهاجم باستغلال ثغرة أمنية مثل تذكر الجلسة غير الآمن أو إعادة تشغيل الطلبات لإعادة استخدام بيانات اعتماد جلسة سابقة.
- التقنيات المستخدمة: هجمات إعادة تشغيل الجلسات (Session Replay) أو سرقة ملفات تعريف الارتباط (Cookies Hijacking).

# أساليب الهجمات في الأمن السيبراني

## 10. الهجمات على إنترنت الأشياء (IoT Attacks)

- مع زيادة استخدام أجهزة إنترنت الأشياء (IoT)، يستهدف المهاجمون هذه الأجهزة التي غالبًا ما تكون أمانها ضعيفًا.
- أسلوب العمل: استغلال ضعف الأمان في أجهزة IoT مثل كاميرات المراقبة أو أجهزة التوجيه، والسيطرة عليها لتنفيذ هجمات أكبر مثل DDoS.
- التقنيات المستخدمة: استغلال ثغرات الأجهزة الذكية أو استخدام برامج ضارة مصممة خصيصًا للأجهزة المتصلة بالإنترنت.

## 11. هجمات الاستهداف (Zero-Day Attacks)

- الهجمات الاستهدافية تستغل الثغرات الجديدة التي لم يتم الكشف عنها بعد أو لم يتم إصدار تصحيح أمني لها.
- أسلوب العمل: يقوم المهاجم بتطوير استغلال لثغرة غير معروفة في برنامج أو نظام قبل أن تتمكن الشركة المطورة من تصحيحها.
- التقنيات المستخدمة: تطوير واستغلال نقاط الضعف المكتشفة حديثًا قبل إصدار تحديثات الأمان.

# أساليب الهجمات في الأمن السيبراني

## الخلاصة:

- أساليب الهجمات السيبرانية متنوعة وتشمل تقنيات معقدة مثل هجمات القوة الغاشمة، الهندسة الاجتماعية، التصيد الاحتيالي، واستغلال الثغرات. بالإضافة إلى ذلك، تعتمد الهجمات مثل DDoS والهجمات على إنترنت الأشياء على استخدام تقنيات متطورة لإغراق الأنظمة وتعطيلها. يجب أن تكون الشركات والأفراد على دراية بهذه الأساليب من أجل تطبيق تدابير الحماية المناسبة.