م. محمد نصيف مصطفى العاني
خريج كلية الهندسة – الجامعة التكنولوجية
قسم هندسة الحاسبات
ماجستير هندسة حاسبات / تخصص ذكاء اصطناعي – تركيا / أنقرة
دكتوراه حالياً في هندسة الحاسبات / تخصص ذكاء اصطناعي – ماليزيا

Eng. Mohammed Nsaif Mustafa Al-Ani
Bachelor's Degree in Computer Engineering – University of Technology
Master's Degree in Computer Engineering (Artificial Intelligence) – Ankara, Turkey
Ph.D. Candidate in Computer Engineering (Artificial Intelligence) – Malaysia

🧠🎓 المحاضرة الثانية: أنواع الهجمات السيبرانية

مقدمة

تُعدّ الهجمات السيبرانية من أخطر التحديات في العصر الرقمي الحديث، إذ تستهدف البيانات والأنظمة والخدمات عبر الإنترنت لتحقيق أهداف مختلفة مثل السرقة أو التخريب أو التجسس أو الابتزاز.
تتنوع هذه الهجمات حسب أسلوب المهاجم، والأدوات المستخدمة، ونوع النظام المستهدف.

تصنيف الهجمات السيبرانية

يمكن تصنيف الهجمات إلى ثلاث فئات رئيسية:

1. **هجمات تستهدف الأفراد:(Personal Attacks)**
مثل سرقة الحسابات أو الاحتيال المالي أو الابتزاز الإلكتروني.
2. **هجمات تستهدف المؤسسات:(Organizational Attacks)**
مثل اختراق قواعد البيانات، أو تسريب معلومات العملاء، أو تعطيل الخدمات.
3. **هجمات ترعاها دول:(State-Sponsored Attacks)**
وهي هجمات متقدمة تستهدف البنى التحتية الحيوية لأغراض سياسية أو عسكرية.

أبرز أنواع الهجمات

◇ *أولاً: البرمجيات الخبيثة (Malware)*

هي برامج تُصمَّم لإلحاق الضرر بجهاز الحاسوب أو سرقة البيانات.
أنواعها تشمل:

- **الفيروسات (Viruses):** تنتشر داخل الملفات وتصيب الأنظمة.
- **الديدان (Worms):** تنتقل ذاتيًا عبر الشبكات دون تدخل المستخدم.
- **أحصنة طروادة (Trojans):** تبدو برامج طبيعية لكنها تفتح بابًا خلفيًا للمخترق.
- **برمجيات الفدية (Ransomware):** تقوم بتشفير الملفات وتطلب فدية لفكها.

📌 **أمثلة واقعية:**
هجوم *WannaCry* عام 2017 أصاب أكثر من 200 ألف جهاز في 150 دولة.

◇ *ثانيًا: هجمات التصيّد (Phishing Attacks)*

هي رسائل بريد إلكتروني أو روابط مزيفة تحاول إقناع المستخدم بإدخال معلومات حساسة.
غالبًا ما تُقلّد مواقع حقيقية مثل البنوك أو شبكات التواصل الاجتماعي.

أنواع التصيّد:

- التصيّد العام (Phishing): استهداف عدد كبير من المستخدمين.
- التصيّد الموجّه (Spear Phishing): استهداف شخص أو مؤسسة محددة.
- التصيّد عبر الرسائل النصية (Smishing).
- التصيّد عبر المكالمات الهاتفية (Vishing).

📌 **مثال:**
رسالة مزيفة من بنك تطلب "تحديث بيانات الحساب"، وبمجرد الضغط على الرابط يتم سرقة كلمة المرور.

◇ *ثالثًا: هجمات حجب الخدمة (DoS) و (DDoS Attacks)*

هي هجمات تُغرق الخادم بطلبات وهمية كثيرة تجعله غير قادر على الاستجابة للمستخدمين الحقيقيين.

- **DoS (Denial of Service):** مصدر واحد للهجوم.
- **DDoS (Distributed Denial of Service):** آلاف الأجهزة تشارك في الهجوم بشكل متزامن.

📌 **مثال:**
تعطيل موقع تويتر عام 2016 بسبب هجوم DDoS باستخدام أجهزة إنترنت الأشياء (IoT).

---

٥ رابعًا: هجمات كلمات المرور (Password Attacks)

تهدف إلى سرقة كلمات المرور أو كسرها، وتشمل:

- **الهجوم بالقوة الغاشمة (Brute Force):** تجربة جميع الاحتمالات.
- **هجوم القاموس (Dictionary Attack):** استخدام كلمات شائعة أو معروفة.
- **الهجوم عبر سرقة الملفات.(Credential Dumping)**

📌 **طرق الحماية:**

- استخدام كلمات مرور قوية (أحرف كبيرة + صغيرة + رموز + أرقام).
- تفعيل المصادقة الثنائية.(Two-Factor Authentication)

---

٥ خامسًا: الهندسة الاجتماعية (Social Engineering)

هي أسلوب يعتمد على **خداع الإنسان بدلاً من اختراق النظام**.
يستغل المهاجم الثقة أو الفضول أو الخوف للوصول إلى المعلومات.

أشهر أساليبها:

- انتحال الهوية.(Pretending to be IT support)
- إرسال ملفات مغرية تحتوي على برمجيات خبيثة.
- المكالمات المزيفة لطلب كلمة السر.

📌 **الوقاية:**
التدريب والوعي الأمني أهم وسيلة لمواجهتها.

---

٥ سادسًا: هجمات استغلال الثغرات (Exploitation Attacks)

تُستخدم فيها أدوات متقدمة لاختراق الأنظمة عبر ثغرات لم يتم إصلاحها.(Zero-Day Exploits)
📌 **مثال:**
استغلال ثغرة في نظام Windows قبل إصدار التحديث الأمني.

مراحل تنفيذ الهجوم السيبراني

1. **الاستطلاع (Reconnaissance):** جمع معلومات عن الهدف.
2. **الفحص (Scanning):** البحث عن منافذ وثغرات.
3. **الاستغلال (Exploitation):** استخدام الثغرة لاختراق النظام.
4. **التحكم (Access & Control):** تثبيت أدوات تحكم عن بعد.

5. **المحو (Cover Tracks):** حذف آثار الهجوم لتجنّب الاكتشاف.

الخلاصة

الأمن السيبراني لا يقتصر على الأدوات فقط، بل يبدأ من **الوعي والمعرفة**.
معرفة أنواع الهجمات وأساليبها تساعد على فهم طريقة تفكير المهاجم، مما يُسهّل الدفاع والاستجابة بسرعة.
