محور الشبكات – المحاضرة (4)

مفهوم التهديدات الشبكية وأنواعها: آلية الهجوم والتأثير والمواجهة

Network Threats: Concept, Types, Attack Mechanisms and Countermeasures

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

أهداف المحاضرة (Learning Objectives)

بعد انتهاء المحاضرة يكون الطالب قادراً على أن:

1. يعرّف التهديد الشبكي (Network Threat) ويصنفه بحسب الأصل والدافع والأسلوب.
2. يميز بين التهديد والثغرة والهجوم والاستغلال، وبين أنواع المهاجمين (Threat Actors).
3. يشرح مراحل الهجوم (Cyber Kill Chain).
4. يفصّل ثمانية أنواع رئيسة: Malware, DoS/DDoS, Phishing, MitM, Insider, Physical, Injection, Ransomware.
5. يربط كل هجوم بالبروتوكول المستهدف وأسلوب الوقاية.
6. يحلل حالات واقعية (WannaCry, GitHub, Colonial Pipeline…) ويستخلص دروسها.

خارطة المحاضرة (Lecture Map)

المحور	العنوان	الجانب التطبيقي
1	مفهوم التهديد وخصائصه (Concept & Characteristics)	جداول مقارنة
2	المهاجمون ودورة حياة الهجوم (Threat Actors & Kill Chain)	مخطط انسيابي
3	الأنواع الثمانية بالتفصيل (Eight Threat Types)	بطاقات تهديدات
4	تهديدات إضافية معاصرة (Additional Threats)	جدول
5	مصفوفة: التهديد ← البروتوكول ← الحماية	جدول ربط
6	دراسات حالة واقعية وسيناريو رياضي	تحليل
7	الاستجابة للحوادث، نشاط، وأسئلة	قائمة إجراءات

أولاً: مفهوم التهديدات الشبكية (Network Threats Concept)

التهديد الشبكي (Network Threat) هو أي حدث أو نشاط محتمل يهدف إلى **استغلال ثغرة (Vulnerability)** في الشبكة لإلحاق الضرر أو سرقة المعلومات أو تعطيل الخدمات. وتعرّفه معايير NIST بأنه إمكانية وقوع حدث يؤثر سلباً في أمن النظام. وقد يكون **متعمداً** (هجمات الهاكرز) أو **غير متعمد** (أخطاء المستخدمين أو الكوارث الطبيعية).

المصطلح	المعنى	مثال
التهديد (Threat)	ما قد يسبب الضرر	برنامج فدية، مهاجم، حريق
الثغرة (Vulnerability)	الضعف الذي يُستغل	نظام غير محدّث، كلمة مرور ضعيفة
الهجوم (Attack)	محاولة فعلية لاستغلال الثغرة	إغراق خادم بطلبات وهمية

المصطلح	المعنى	مثال
الاستغلال (Exploit)	الأداة التي تستغل الثغرة	شيفرة تستغل ثغرة SMB
الأثر (Impact)	حجم الخسارة الناتجة	توقف خدمة، تسريب بيانات

خصائص التهديدات الشبكية (Characteristics)

الخاصية	التصنيف	مثال
الأصل (Origin)	داخلي (Internal): موظف أو جهاز مصاب داخل الشبكة. خارجي (External): مهاجم عبر الإنترنت	موظف يسرّب بيانات / هاكر خارجي
الدافع (Motivation)	مالي، سياسي/أيديولوجي (Hacktivism)، تجسس، تخريب وانتقام، فضول واستعراض	فدية مقابل المال، تشويه موقع احتجاجاً
الأسلوب (Method)	تقني (برمجيات، شبكات) أو بشري (هندسة اجتماعية) أو مادي	فيروس / رسالة تصيد / سرقة جهاز
القصد (Intent)	متعمد (Intentional) أو غير متعمد (Accidental)	هجوم / حذف ملف بالخطأ

آثار التهديدات (Impacts)

نوع الأثر	التفصيل	مثال
مالي (Financial)	خسائر مباشرة كدفع الفدية، وغير مباشرة كفقدان ثقة العملاء	فدية Ransomware
تشغيلي (Operational)	تعطل الخدمات وتوقف الأعمال	DDoS على موقع بيع التذاكر
قانوني وأخلاقي (Legal & Ethical)	انتهاك الخصوصية والغرامات (مثل GDPR) والضرر بالسمعة	تسريب بيانات رياضيين
أمني (Security)	سرقة بيانات حساسة تقود إلى احتيال وجرائم أكبر	انتحال هوية

من حيث الكلفة: قدّر تقرير IBM لعام 2023 متوسط كلفة الاختراق الواحد بنحو 4.45 مليون دولار، وربط تقرير Verizon DBIR 2023 نحو 74% من الاختراقات بالعنصر البشري (أخطاء أو سوء استخدام صلاحيات أو بيانات دخول مسروقة أو هندسة اجتماعية). تُحدَّث الأرقام سنوياً.

ثانياً: المهاجمون ودورة حياة الهجوم (Threat Actors & Attack Lifecycle)

نوع المهاجم	الوصف	الدافع الغالب
الهاكر ذو القبعة السوداء (Black Hat)	يخترق بصورة غير قانونية	ربح مالي أو تخريب
ذو القبعة البيضاء (White Hat)	مختبر اختراق مرخّص يكشف الثغرات لإصلاحها	حماية الأنظمة
ذو القبعة الرمادية (Gray Hat)	يخترق دون إذن لكن لإبلاغ المالك غالباً	فضول أو سمعة
مبتدئ يستخدم أدوات جاهزة (Script Kiddie)	قليل الخبرة يستعمل أدوات غيره	استعراض
ناشط اختراقي (Hacktivist)	هجمات لأهداف سياسية أو اجتماعية	أيديولوجيا

نوع المهاجم	الوصف	الدافع الغالب
عصابات الجريمة المنظمة (Cybercriminals)	جماعات تشغّل برامج فدية واحتيال	المال
جهات مدعومة من دول (Nation-state / APT)	هجمات متقدمة طويلة الأمد	تجسس وتأثير
الداخلي (Insider)	موظف أو متعاقد بصلاحيات مشروعة	انتقام أو مال أو خطأ

مراحل الهجوم المنظم (Cyber Kill Chain)

نموذج وضعته شركة Lockheed Martin يفسّر كيف يتقدم الهجوم، وقطع أي مرحلة يُفشله:

1. الاستطلاع *Reconnaissance* ← **2. التسلّح** *Weaponization* ← **3. التسليم** *Delivery* ← **4. الاستغلال** *Exploitation*

5. التثبيت *Installation* ← **6. القيادة والتحكم** *Command & Control* ← **7. تحقيق الهدف** *Actions on Objectives*

مثال (Example)

رسالة تصيد إلى موظف (تسليم) ← فتح مرفق ضار (استغلال) ← تثبيت برنامج تجسس (تثبيت) ← اتصاله بخادم المهاجم (قيادة وتحكم) ← سرقة قاعدة بيانات العملاء (تحقيق الهدف). ولو دُرِّب الموظف على التصيد لانقطعت السلسلة عند المرحلة الثالثة.

ثالثاً: أنواع التهديدات الشبكية الرئيسة بالتفصيل (Types of Network Threats)

نعرض كل تهديد بطريقة بطاقة موحّدة: **الوصف، آلية العمل، البروتوكول أو الطبقة المستهدفة، المثال الواقعي، الأثر، والحماية.**

1) البرمجيات الضارة (Malware Threats)

البرمجيات الضارة *Malware – Malicious Software*	
الوصف	برامج مصممة لإلحاق الضرر أو السيطرة أو التجسس دون إذن. تنتشر عبر البريد والمواقع والأجهزة المصابة والتطبيقات المزيفة.
آلية العمل	تصل للجهاز ← تنفّذ ← تثبّت نفسها ← تؤدي وظيفتها الضارة (حذف، سرقة، تجسس، تحكم).
البروتوكول / الطبقة	تنتقل عبر تطبيقات: SMTP/IMAP (مرفقات)، HTTP/HTTPS (تنزيلات)، SMB (انتشار داخلي).
الأثر	سرقة بيانات، إبطاء الشبكة، السيطرة الكاملة، وتحويل الأجهزة إلى شبكة بوت (Botnet).
الحماية	مضاد برمجيات/EDR، تحديثات، تعطيل الماكرو، تحميل من مصادر رسمية، فحص المرفقات، نسخ احتياطي.

النوع	الخاصية	مثال
فيروس (Virus)	يلتصق بملف شرعي وينتشر عند تشغيله بتدخل المستخدم	فيروسات الماكرو في الوثائق
دودة (Worm)	تنتشر ذاتياً عبر الشبكة دون تدخل المستخدم	WannaCry، ILOVEYOU (ينتشر ببريد مرفق)
حصان طروادة (Trojan)	يتنكر كبرنامج مفيد وينفّذ مهمة خفية	تطبيق مزيف على الهاتف

النوع	الخاصية	مثال
برامج التجسس (Spyware)	تراقب النشاط وتسرق كلمات المرور	Keylogger يسجل ضغطات المفاتيح
برامج الإعلانات (Adware)	تعرض إعلانات مزعجة وقد تتجسس	إضافات متصفح مشبوهة
جذور خفية (Rootkit)	تخفي وجودها وتمنح تحكماً عميقاً	تعديل نواة النظام

تصحيح مفاهيمي: يُصنَّف ILOVEYOU (عام 2000) تقنياً **دودة** (Worm) لا فيروساً؛ إذ انتشر آلياً عبر إرسال نفسه إلى جهات اتصال البريد. وكذلك WannaCry دودة تحمل حمولة فدية (Ransomware).

2) هجمات رفض الخدمة (DoS / DDoS Attacks)

رفض الخدمة والموزّع *DoS / DDoS – (Distributed) Denial of Service*	
الوصف	إغراق الشبكة أو الخادم بحركة مرور زائدة لمنع المستخدمين الشرعيين من الوصول. وDDoS نسخة موزعة تستخدم آلاف الأجهزة المصابة (Botnet).
آلية العمل	إرسال طلبات وهمية مستمرة حتى تنفد موارد الخادم أو عرض نطاق الشبكة.
البروتوكول / الطبقة	**TCP SYN Flood:** إرسال عدد هائل من SYN دون إكمال المصافحة الثلاثية فتمتلئ جداول الاتصالات النصف مفتوحة. **UDP/ICMP Flood:** إغراق بحزم. **HTTP Flood:** طلبات ويب كثيفة. **هجمات التضخيم (Amplification):** استغلال خوادم (DNS, NTP, Memcached) لتضخيم حجم الحركة.
مثال واقعي	هجوم GitHub في فبراير 2018 بتضخيم Memcached بلغ نحو 1.35 تيرابت/ثانية، وجرى تخفيفه خلال دقائق عبر خدمة حماية.
الأثر	توقف المواقع والخدمات لساعات أو أيام وخسائر مالية وسمعية.
الحماية	خدمات تخفيف DDoS وCDN، تحديد معدل الطلبات (Rate Limiting)، SYN Cookies، جدار ناري، توزيع الأحمال، وتعطيل الخدمات المضخِّمة المكشوفة.

1. المهاجم يتحكم بالبوت نت *Botnet* ◄ **2. الأجهزة المصابة ترسل آلاف الطلبات** ◄ **3. الخادم يمتلئ ولا يستجيب** ◄ **4. المستخدمون الشرعيون لا يصلون**

3) التصيد الاحتيالي (Phishing Attacks)

التصيد الاحتيالي *Phishing – Social Engineering by Message*	
الوصف	خداع المستخدم لكشف بيانات حساسة عبر رسائل أو مواقع مزيفة تبدو شرعية.
الأنواع	**Phishing** عام جماعي. **Spear Phishing** موجّه لشخص محدد. **Whaling** يستهدف المدراء. **Vishing** بالاتصال الصوتي. **Smishing** بالرسائل النصية. **Quishing** عبر رموز QR. **BEC (Business Email Compromise)** انتحال بريد مدير لطلب تحويل مالي.
آلية العمل	رسالة عاجلة ← رابط لموقع مقلّد ← إدخال بيانات الدخول ← سرقتها ← استخدامها للدخول إلى الشبكة.
البروتوكول / الطبقة	SMTP/IMAP للبريد، HTTP/HTTPS للمواقع المزيفة، DNS لنطاقات مشابهة (Typosquatting).
مثال واقعي	حملات تستهدف موظفي شركات للوصول إلى شبكاتها الداخلية، ورسائل مزيفة باسم مصارف أو شركات شحن.

الأثر	سرقة بيانات الدخول، ثم اختراقات أكبر؛ فهو غالباً نقطة البداية لهجمات أخرى كالفدية.
الحماية	تدريب الوعي، MFA، فحص الروابط، بوابات حماية البريد (SPF/DKIM/DMARC)، الإبلاغ عن الرسائل المشبوهة.

علامات الرسالة المشبوهة (Red Flags)
استعجال أو تهديد، خطأ لغوي، عنوان مرسل غريب أو مشابه، رابط لا يطابق النص الظاهر، طلب كلمة مرور أو رمز، مرفق غير متوقع.

4) هجمات الرجل في الوسط (Man-in-the-Middle – MitM)

الرجل في الوسط *MitM – Man-in-the-Middle*	
الوصف	يتدخل المهاجم بين طرفي اتصال (مستخدم وخادم) للتجسس أو تعديل البيانات دون علمهما.
آلية العمل	**Evil Twin:** شبكة Wi-Fi مزيفة بالاسم نفسه. **ARP Spoofing:** إيهام الأجهزة أن عنوان MAC للمهاجم هو البوابة فتمر البيانات عبره. **SSL Stripping:** خفض الاتصال من HTTPS إلى HTTP. **DNS Spoofing:** توجيه المستخدم إلى موقع مزيف.
البروتوكول / الطبقة	ARP (ربط البيانات)، HTTP/HTTPS، DNS، و802.11 Wi-Fi غير المشفّر.
مثال	التقاط بيانات دخول أو بطاقات في شبكة Wi-Fi مجانية في مقهى أو مطار.
الأثر	سرقة كلمات المرور والبيانات المالية، وتزوير الرسائل.
الحماية	HTTPS وVPN، HSTS على الشبكات العامة، WPA3/WPA2، التحقق من الشهادات، Dynamic ARP Inspection، DNSSEC، وتجاهل تحذيرات الشهادة.

5) التهديدات الداخلية (Insider Threats)

التهديدات الداخلية *Insider Threats*	
الوصف	تهديد من أشخاص داخل المنظمة (موظفون، متعاقدون، شركاء) يملكون صلاحيات مشروعة؛ إما **خبيث (Malicious)** أو **مهمل/غير متعمد (Negligent)**.
آلية العمل	استخدام الصلاحيات للوصول إلى بيانات أو تثبيت برمجيات ضارة أو إخراج معلومات، أو مشاركة كلمة مرور بالخطأ.
البروتوكول / الطبقة	عادةً يتجاوز الحماية الطرفية لأن النشاط يبدو مشروعاً: وصول عبر الشبكة الداخلية أو إرسال بيانات بالبريد/السحابة.
مثال	موظف غاضب يبيع بيانات الشركة، أو خطأ في تحديث يفتح ثغرة، أو مدرب يشارك كلمة مرور الحساب المشترك.
الأثر	يصعب كشفها لأنها لا تثير الإنذارات الخارجية، وتتسبب بتسريبات ضخمة.
الحماية	أقل الصلاحيات (Least Privilege)، فصل المهام، مراقبة السجلات (SIEM/DLP)، إنهاء صلاحيات المغادرين فوراً، وثقافة أمنية وسياسات واضحة.

6) التهديدات الفيزيائية (Physical Threats)

التهديدات الفيزيائية *Physical Threats*

الوصف	تهديدات تمس الأجهزة المادية للشبكة: كوارث طبيعية أو بشرية أو أعطال.
الأنواع	حرائق، فيضانات، زلازل، سرقة أجهزة، تخريب كابلات، انقطاع كهرباء، ارتفاع حرارة غرف الخوادم.
الأثر	تلف الكابلات والخوادم وقطع الاتصال وفقدان دائم للبيانات إذا لم توجد نسخ احتياطية.
مثال	تدمير مركز بيانات بإعصار، أو قطع كابل ألياف أثناء أعمال حفر.
الحماية	تحكم دخول وأقفال وكاميرات، مصادر طاقة احتياطية (UPS ومولد)، تكييف، أنظمة إطفاء، نسخ احتياطي خارج الموقع، ومواقع بديلة للتعافي (Disaster Recovery).

7) هجمات الحقن (Injection Attacks)

هجمات الحقن ***Injection – e.g., SQL Injection***	
الوصف	إدخال أوامر أو شيفرات ضارة عبر حقول الإدخال (نماذج الويب) فينفذها الخادم أو قاعدة البيانات كأنها أوامر مشروعة.
آلية العمل	التطبيق لا يتحقق من المدخلات (Input Validation) فيدمجها مباشرة في استعلام قاعدة البيانات، فيتغير معنى الاستعلام.
البروتوكول / الطبقة	طبقة التطبيق: طلبات HTTP/HTTPS إلى تطبيق ويب متصل بقاعدة بيانات.
مثال	اختراق مواقع التجارة الإلكترونية لسحب بيانات العملاء. ومن الأنواع: SQL Injection, Command Injection, XSS.
الأثر	تسريب قواعد بيانات كاملة أو تعديلها أو السيطرة على الخادم.
الحماية	**الاستعلامات المهيأة (Parameterized Queries)**، التحقق من المدخلات، أقل صلاحيات لحساب قاعدة البيانات، جدار تطبيقات ويب (WAF)، تحديث التطبيقات واختبار الاختراق.

8) برامج الفدية (Ransomware)

برامج الفدية ***Ransomware – Extortion Malware***	
الوصف	نوع من Malware يشفّر ملفات الضحية ويطالب بفدية (غالباً بعملة رقمية) مقابل مفتاح فك التشفير. وفي «الابتزاز المزدوج» يسرق البيانات أيضاً ويهدد بنشرها.
آلية العمل	الدخول (تصيد، ثغرة، RDP/VPN ضعيف) ← انتشار داخل الشبكة ← حذف النسخ الاحتياطية المتاحة ← تشفير الملفات ← رسالة الفدية.
البروتوكول / الطبقة	غالباً عبر SMTP (تصيد)، وثغرات SMB، وخدمات سطح المكتب البعيد RDP، وحسابات VPN دون MFA.
مثال واقعي	هجوم Colonial Pipeline في مايو 2021 الذي أدى إلى إيقاف عمليات خط الأنابيب الأمريكي مؤقتاً.
الأثر	توقف الأعمال، دفع مبالغ كبيرة، وفقدان بيانات إن لم توجد نسخ احتياطية سليمة، مع خطر تسريبها.
الحماية	نسخ احتياطي 3-2-1 غير متصل (Offline/Immutable)، تحديثات، MFA، تجزئة الشبكة، تقييد RDP، تدريب ضد التصيد، وخطة استجابة مجرّبة.

نصيحة (Tip)

تؤكد الجهات الأمنية الرسمية عادةً أن دفع الفدية لا يضمن استرجاع البيانات ويموّل المجرمين؛ ويبقى النسخ الاحتياطي السليم هو أفضل وسيلة للتعافي.

رابعاً: تهديدات إضافية معاصرة (Additional Contemporary Threats)

التهديد	الوصف	الحماية الأساسية
هجمات كلمات المرور (Password Attacks)	تخمين (Brute Force) أو استخدام كلمات مسربة (Credential Stuffing)	كلمات مرور فريدة وطويلة، MFA، قفل المحاولات
الهندسة الاجتماعية (Social Engineering)	خداع الإنسان بدل اختراق الجهاز	التدريب والتحقق عبر قناة ثانية
ثغرة اليوم الصفري (Zero-day)	ثغرة غير معروفة للمُصنّع ولا يوجد لها تصحيح بعد	الدفاع بالعمق، تقليل التعرّض، تحديث سريع
التنصت (Sniffing)	التقاط الحزم غير المشفرة في الشبكة	التشفير TLS/VPN وWPA3
انتحال العناوين (Spoofing)	انتحال IP أو MAC أو بريد لخداع الأنظمة	ترشيح الحزم، ARP Inspection، SPF/DKIM
التهديد المتقدم المستمر (APT)	اختراق طويل الأمد وخفي بغرض التجسس	SIEM، مراقبة السلوك، تجزئة الشبكة
بوت نت إنترنت الأشياء (IoT Botnet)	السيطرة على كاميرات وراوترات بكلمات مرور افتراضية (مثل Mirai 2016)	تغيير كلمات المرور الافتراضية وتحديث البرمجيات الثابتة
التعدين الخفي (Cryptojacking)	استغلال موارد جهازك لتعدين العملات الرقمية	مضاد برمجيات، حظر النصوص الضارة

خامساً: مصفوفة الربط: التهديد ← البروتوكول المستهدف ← الحماية (Threat–Protocol–Defense Matrix)

التهديد	البروتوكول / الطبقة	نقطة الضعف	الحماية
SYN Flood	TCP – النقل	المصافحة الثلاثية	SYN Cookies، تخفيف DDoS
ARP Spoofing	ARP – ربط البيانات	غياب التوثيق	Dynamic ARP Inspection، VPN
DNS Spoofing	DNS – التطبيق	ثقة الاستجابات غير الموقعة	DNSSEC، DoH
الشم (Sniffing)	HTTP / FTP / Telnet	نص غير مشفر	HTTPS / SFTP / SSH
انتحال البريد	SMTP	ضعف توثيق المرسل	SPF / DKIM / DMARC
الحقن	HTTP – تطبيق ويب	عدم التحقق من المدخلات	استعلامات مهيأة، WAF
التنصت / Evil Twin	Wi-Fi 802.11	شبكة مفتوحة أو ضعيفة	WPA3، VPN
الفدية	SMB / RDP / SMTP	ثغرات وتصيد وكلمات ضعيفة	تحديثات، MFA، نسخ احتياطي

سادساً: دراسات حالة واقعية (Real-World Case Studies)

الحالة 1: WannaCry (مايو 2017) – دودة وفدية

استغلت الدودة ثغرة في بروتوكول **SMB** في نظام Windows (عُرفت باسم EternalBlue)، وانتشرت ذاتياً عبر الشبكات مشفّرة الملفات ومطالبة بفدية. أصابت مئات الآلاف من الأجهزة في أكثر من 150 دولة وعطلت مؤسسات، منها مستشفيات في بريطانيا. وكانت مايكروسوفت قد أصدرت تحديثاً يسد الثغرة قبل الهجوم بأسابيع (نشرة MS17-010). الدرس: **التحديث المنتظم (Patch Management)** كان كفيلاً بمنع كارثة عالمية.

الحالة 2: GitHub DDoS (فبراير 2018)

تعرض موقع GitHub لهجوم تضخيم عبر خوادم Memcached المكشوفة للإنترنت، وبلغت ذروته نحو 1.35 تيرابت/ثانية، وكان من الأكبر وقتها. تحول الموقع إلى خدمة حماية متخصصة فاستعاد عمله خلال دقائق. الدرس: **التخطيط المسبق لخدمات تخفيف DDoS** وتأمين الخدمات المضخِّمة.

الحالة 3: Colonial Pipeline (مايو 2021) – فدية وبنية حرجة

أوقفت الشركة المشغلة لأكبر خط أنابيب وقود في الولايات المتحدة عملياتها مؤقتاً بعد هجوم فدية نفذته مجموعة DarkSide، فاضطربت إمدادات الوقود في الساحل الشرقي. وأفادت تقارير التحقيق بأن دخول المهاجمين تم عبر حساب VPN قديم بكلمة مرور مسرّبة دون مصادقة متعددة العوامل. ودفعت الشركة فدية بالبيتكوين، واستردت السلطات الأمريكية جزءاً منها لاحقاً. الدرس: **MFA وإدارة الحسابات القديمة** ضروريان، والبنى التحتية الحيوية هدف رئيس.

الحالة 4: ILOVEYOU (مايو 2000) – هندسة اجتماعية

انتشر ببريد يحمل عنوان «ILOVEYOU» ومرفقاً يبدو رسالة حب، فبادر ملايين المستخدمين إلى فتحه فأرسل نفسه تلقائياً إلى جهات اتصالهم وأتلف ملفات. الدرس: **العامل البشري هو الحلقة الأضعف** أحياناً، وأي مرفق غير متوقع مشبوه مهما كان مغرياً.

الحالة 5 (سيناريو افتراضي): بطولة وطنية وموقع تذاكر

السيناريو (Hypothetical)
قبل ساعة من فتح حجز تذاكر بطولة وطنية ينهار موقع الاتحاد بسبب آلاف الطلبات المتزامنة، ثم تصل رسائل لبعض المشجعين تعرض «تذاكر مضمونة» برابط مختلف الاسم قليلاً عن موقع الاتحاد.

التحليل: هجوم DDoS (توافر) متبوع بحملة تصيد/نطاق مزيف (Typosquatting). **الإجراء:** تفعيل خدمة تخفيف DDoS وCDN، وإعلان النطاق الرسمي الوحيد للتذاكر، وتحذير الجمهور، وإبلاغ مزود النطاق بإزالة الموقع المقلّد.

سابعاً: الاستجابة الأولية للحوادث (Incident Response Basics)

يحدد دليل NIST SP 800-61 دورة معالجة الحوادث الأمنية. للمستخدم والمؤسسة الصغيرة يمكن اختصارها:



الموقف	الإجراء الفوري للمستخدم
شككت بإصابة جهازك	افصله عن الشبكة (Wi-Fi/كابل)، لا تُطفئه إن طُلب منك الاحتفاظ بالأدلة، أبلغ المختص، ولا تدخل كلمات مرور من الجهاز
ضغطت رابط تصيد	غيّر كلمة المرور من جهاز آمن، فعّل MFA، أبلغ الجهة المعنية، وراقب الحساب
ظهرت رسالة فدية	افصل الجهاز، لا تدفع قبل استشارة المختصين، استعد من نسخة احتياطية سليمة، وأبلغ الجهات المختصة
موقع المؤسسة لا يستجيب فجأة	فعّل خطة DDoS، تواصل مع مزود الخدمة، وأبلغ المستخدمين بقناة بديلة

ثامناً: نشاط صفّي (Class Activity)

المطلوب (مجموعات): وزّعوا على المجموعات الثماني الأنواع (Insider، MitM، Phishing، DDoS، Malware، Ransomware، Injection، Physical)؛ على كل مجموعة تقديم بطاقة في دقيقتين:

البند	إجابة المجموعة
اسم التهديد (Threat Name)	
كيف يعمل؟	
البروتوكول أو الطبقة المستهدفة	
مثال رياضي	
طريقتان للوقاية	

تاسعاً: مسرد المصطلحات (Glossary)

المصطلح (Term)	المعنى
Threat / Vulnerability / Risk	تهديد / ثغرة / مخاطر
Exploit	أداة استغلال الثغرة
Malware	برمجيات ضارة
Worm	دودة: تنتشر ذاتياً
Trojan	حصان طروادة
Botnet	شبكة أجهزة مصابة يتحكم بها مهاجم
DDoS	رفض خدمة موزّع
SYN Flood	إغراق بطلبات SYN
Phishing	تصيد احتيالي
MitM	الرجل في الوسط
Ransomware	برمجيات الفدية
Injection	حقن شيفرة عبر المدخلات
Zero-day	ثغرة اليوم الصفري
APT	تهديد متقدم مستمر
Kill Chain	سلسلة مراحل الهجوم

عاشراً: أسئلة تدريبية (Practice Questions)

أولاً: اختيار من متعدد (Multiple Choice)

1) هجوم SYN Flood يستهدف أساساً:

أ) مصافحة TCP الثلاثية

ب) تشفير TLS

ج) بروتوكول SMTP فقط

د) كابلات الشبكة

2) البرمجية التي تنتشر ذاتياً عبر الشبكة دون تدخل المستخدم:

أ) Virus
ب) Worm
ج) Spyware
د) Adware

3) أفضل وسيلة لمواجهة هجوم Ransomware على المدى الطويل:

أ) دفع الفدية فوراً
ب) نسخ احتياطي سليم غير متصل مع تحديثات وMFA
ج) إطفاء الراوتر دائماً
د) تعطيل الإنترنت

4) الخطر الأكبر في الشبكات العامة غير المشفرة:

أ) ارتفاع حرارة الجهاز
ب) الرجل في الوسط والتنصت
ج) زيادة الإعلانات
د) بطء المعالج

5) الحماية الأساسية من SQL Injection:

أ) استعلامات مهيأة (Parameterized Queries) والتحقق من المدخلات
ب) تغيير لون الموقع
ج) زيادة ذاكرة الخادم
د) تعطيل HTTPS

ثانياً: صح أم خطأ (True / False)

1. التهديد الشبكي قد يكون غير متعمد كخطأ مستخدم أو كارثة طبيعية. ( )
2. DDoS يهدف أساساً إلى سرقة البيانات السرية. ( )
3. التهديدات الداخلية أصعب كشفاً لأنها لا تثير إنذارات خارجية. ( )
4. تحديث الأنظمة كان سيمنع انتشار WannaCry على نطاق واسع. ( )

ثالثاً: أسئلة قصيرة (Short Answer)

1. فرّق بين التهديد والثغرة والهجوم بمثال.
2. اشرح آلية SYN Flood وارتباطها بالمصافحة الثلاثية.
3. اذكر خمسة أنواع من التصيد (Phishing Types) وعرّف اثنين منها.

رابعاً: أسئلة تحليلية (Analytical)

1. حلّل هجوم Colonial Pipeline وفق مراحل Cyber Kill Chain واقترح مرحلة كان يمكن قطع السلسلة عندها.
2. قارن بين DDoS وRansomware من حيث الهدف الأمني (CIA) والأثر والحماية.
3. اقترح خطة مختصرة لحماية اتحاد رياضي من التصيد وDDoS خلال بطولة وطنية.

الإجابات النموذجية (Answer Key)

القسم	الإجابة
اختيار من متعدد	1-أ ، 2-ب ، 3-ب ، 4-ب ، 5-أ
صح / خطأ	1-صح ، 2-خطأ (هدفه التوافر) ، 3-صح ، 4-صح

ملخص المحاضرة (Summary)

- التهديد الشبكي استغلال محتمل لثغرة، ويُصنَّف بحسب الأصل والدافع والأسلوب.
- الأنواع الثمانية: Malware وDDoS وPhishing وMitM وInsider وPhysical وInjection وRansomware، ولكل منها بروتوكول أو نقطة ضعف مستهدفة وحماية محددة.
- أغلب الهجمات الكبرى استُغلت فيها ثغرات معروفة أو أخطاء بشرية؛ فالتحديث والتدريب وMFA والنسخ الاحتياطي والدفاع بالعمق أساس الوقاية.

المصادر والمراجع (References)

1. NIST. SP 800-61 Rev.2: Computer Security Incident Handling Guide. 2012. | SP 800-83 Rev.1: Guide to Malware Incident Prevention and Handling. 2013.
2. Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lockheed Martin; 2011.
3. Microsoft. Security Bulletin MS17-010 – Critical (2017).
4. GitHub Engineering. February 28th DDoS Incident Report (2018).
5. Antonakakis M, April T, Bailey M, et al. Understanding the Mirai botnet. Proc 26th USENIX Security Symposium; 2017.
6. U.S. Department of Justice. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 2021).
7. CISA. #StopRansomware Guide.
8. Verizon. 2023 Data Breach Investigations Report (DBIR) | IBM Security. Cost of a Data Breach Report 2023 (and later editions).
9. Stallings W. Network Security Essentials. Pearson (latest edition). | OWASP Foundation. OWASP Top 10 Web Application Security Risks.

إعداد: **أ.م.د. حيدر حسن محمد**

مدرس المادة