الأسبوع الأول

1. Virus	قطعة برنامج يمكن إرفاقها ببرنامج أو ملف آخر
2. Worm	تشبه الى حد كبير الفيروس. التصميم هو نفسه، ولكن على عكس الفيروس، فإن الدودة قادرة على الانتقال من نظام إلى آخر دون أي تدخل بشري
3. Information Security	نظرية وممارسة للسماح فقط بالوصول للمعلومات للأشخاص في المؤسسة المصرح الهم برؤيتها
4. Confidentiality	سرية المعلومات: المعلومات غير متاحة للأشخاص غير المصرح لهم بمشاهدتها
5. Integrity	النزاهة في التعامل مع المعلومات: يمكن للناس أن يثقوا في أن المعلومات الموجودة في مؤسسة ما لم يتم العبث بها بطريقة أو بأخرى
6. Availability	توافر المعلومات عند طلبها: يمكن للأشخاص المصرح لهم بمشاهدة البيانات القيام بذلك عندما يحتاجون إلى الوصول
7. NIST CSF	إطار العمل (Framework) الصادر عن NIST
8. Identify	تساعد وظيفة تحديد الهوية في تطوير فهم تنظيمي لإدارة مخاطر الأمن السيبراني على الأنظمة والأشخاص والأصول والبيانات و القدرات
9. Protect	تحدد وظيفة الحماية الإجراءات الوقائية المناسبة لضمان تقديم خدمات البنية التحتية الحيوية
10. Detect	تحدد وظيفة الكشف الأنشطة المناسبة لتحديد وقوع حدث للأمن السيبراني
11. Respond	تتضمن وظيفة الاستجابة الأنشطة المناسبة لاتخاذ إجراء بشأن حادث أمن مكشوف تم اكتشافه
12. Recover	تحدد وظيفة الاسترداد، الأنشطة المناسبة للمحافظة على خطط المرونة واستعادة أي قدرات أو خدمات تعرّضت لخطر بسبب حادث الأمن السيبراني

الأسبوع الثاني

1. Cybercrime	الجريمة الالكترونية
2. Threat Actors	منفّذ التهديد
3. Hacking	القرصنة
4. Ransomware	هي طريقة هجوم شائعة جدًا تستخدمها الجهات الفاعلة في التهديدات التي تقوم بتشفير الملفات فيها وتتطلب الدفع لمفتاح فك التشفير
5. Denial of Service	محاولة خبيثة لتعطيل حركة المرور العادية لخادم أو خدمة أو شبكة مستهدفة من خلال التغلب على الهدف أو البنية التحتية المحيطة به مع تدفق بيانات الإنترنت
6. Malware	نوع من أنواع البرامج الخبيثة
7. IOT	هو امتداد الاتصال بالإنترنت في الأجهزة المادية والأشياء اليومية
8. OWASP	Open Web Application Security Project هو مجتمع عبر الإنترنت ينتج مقالات ومنهجيات ووثائق وأدوات وتقنيات متوفرة مجانًا في مجال أمان تطبيقات الويب https://owasp.org
9. Cyberwarfare	الحرب الإلكترونية
10. Hacktivism	هو استخدام أجهزة الحاسوب والشبكات الحاسوبية لتعزيز أجندة سياسية
11. Backdoor	تعليمات برمجية ضارة تثبت نفسها على جهاز كمبيوتر للسماح للمهاجم بالوصول https://ar.wikipedia.org/wiki/حوسبة)_خلفي_باب)
12. Botnet	على غرار الباب الخلفي، فهو يسمح للمهاجم بالوصول إلى النظام، لكن جميع أجهزة الكمبيوتر المصابة بنفس الروبوتات تتلقى نفس التعليمات من خادم تحكم واحد https://ar.wikipedia.org/wiki/بوت_نت
13. Downloader	رمز ضار موجود فقط لتنزيل رمز ضار آخر
14. Information Stealing malware	البرامج الضارة التي تجمع المعلومات من كمبيوتر الضحية وعادةً ما ترسلها إلى المهاجم
15. Launcher	برنامج ضار يستخدم لإطلاق برامج ضارة أخرى

16. Rootkit	الكود الضار المصمم لإخفاء وجود الكود الآخر
17. Scareware	البرامج الضارة المصممة لتخويف مستخدم مصاب في شراء شيء ما
18. Spam-sending malware	البرامج الضارة التي تصيب جهاز المستخدم ثم تستخدم هذا الجهاز لإرسال رسائل غير مرغوب فيها
19. Trojan Horse	برنامج يبدو أنه مفيد أو مشروع أو يمتلك الوظيفة المطلوبة، ولكنه يخفي بالفعل حمولة ضارة، ويدعو المستخدم إلى تشغيلها
20. Phishing	على الرغم من أنه ليس برنامجًا ضارًا بالفعل، فقد أصبح التصيد مؤخرًا مصدر قلق حقيقي للأمان. يتم توجيه المستخدمين إلى موقع ،ويب موثوق به على ما يبدو وخداعهم لإعطاء معلومات شخصية مثل كلمات مرور أو تفاصيل بطاقة الائتمان، إلخ
21. Zombie	تتحكم برامج Zombie في جهاز الكمبيوتر الخاص بك وتستخدمه و اتصاله بالإنترنت لمهاجمة أجهزة الكمبيوتر أو الشبكات الأخرى أو القيام بأنشطة إجرامية أخرى
22. Adware	الغرض منه هو عرض تلك الإعلانات المنبثقة المزعجة
23. Hijacker	البرامج الإعلانية التي تلحق نفسها بمستعرض الويب الخاص بك مثل Chrome أو Firefox أو Internet Explorer وتعرض إعلانات متقطعة في المستعرض الخاص بك إما عن طريق إنشاء النوافذ المنبثقة أو عن طريق حقن الإعلانات مباشرة في الصفحات التي تتصفحها
24. IDS	أنظمة كشف التسلل
25. Tripwires	كشف التغييرات الحرجة للملفات
26. Configuration checking tools	التحقق من نقاط ضعف النظام المستهدف
27. Honey pots	طعم لمجرمي الإنترنت. غالبًا ما يتصرفون كمعلومات حساسة (كإغراء للمجرمين)، ويبقون المجرم "متصلاً" لفترة طويلة بما يكفي للتركيز على مواقعهم وتخزين أدلة الجريمة الإلكترونية نفسها
28. Anomaly detection systems	تحديد سلوك غير طبيعي على مضيف أو شبكة
29. NIDS	أنظمة كشف التسلل القائمة على الشبكة
30. HIDS	أنظمة كشف التسلل المستندة إلى المضيف

31. Password Management Software	برامج إدارة كلمات المرور: يمكنك استخدام هذا البرنامج للسماح لك بتحديد كلمات مرور أكثر تعقيدًا وتخزينها بشكل آمن في نظام محمي
32. Email encryption software	برامج تشفير البريد الالكتروني: تشفير رسائل البريد الإلكتروني و المرفقات من وقت ضغط المرسل زر "إرسال" حتى الوصول إلى المستلم، مما يجعل من غير المحتمل اختراق المحتويات المهمة أو الوصول إليها على طول الطريق
33. Firewalls	جدران الحماية: مشاهدة كل من حركة المرور الواردة والصادرة على شبكتك وتمنع الأشياء التي تعتقد أنها ذات طبيعة مشبوهة
34. Antivirus	مكافحة الفيروسات: حاسمة في حماية أنظمة الكمبيوتر من التطفل والفيروسات والهجمات الرقمية الضارة

الأسبوع الثالث

1. Adversary	كيان يهاجم أو يشكل تهديدًا للنظام
2. Attack	اعتداء على أمن النظام ينبع من تهديد ذكي
3. Countermeasure	جهاز أو إجراء أو تقنية تقلل من تهديد أو ضعف أو هجوم عن طريق القضاء عليه أو منعه، عن طريق تقليل الضرر الذي يمكن أن يسببه، أو اكتشافه والإبلاغ عنه بحيث يمكن اتخاذ الإجراء التصحيحي
4. Risk	توقع الخسارة معبراً عنه كاحتمال أن يستغل تهديد معين مشكلة عدم حصانة معينة نتيجة ضارة معينة
5. Security Policy	مجموعة من القواعد والممارسات التي تحدد أو تنظم كيفية عمل النظام أو مؤسسة توفر خدمات الأمن لحماية موارد النظام الحساسة والضرورية
6. System Resource (Asset)	البيانات الواردة في نظام المعلومات؛ أو خدمة يقدمها نظام؛ أو قدرة النظام، مثل طاقة المعالجة أو عرض نطاق الاتصال؛ أو عنصر من معدات النظام
7. Threat	احتمال انتهاك الأمان، والذي يحدث عندما يكون هناك ظرف أو قدرة أو إجراء أو حدث، يمكن أن ينتهك الأمن ويسبب ضرراً. أي أن التهديد خطر محتمل قد يستغل ثغرة أمنية
8. Vulnerability	عيب أو ضعف في تصميم النظم أو تنفيذها أو تشغيلها وإدارتها والتي يمكن استغلالها لانتهاك السياسة الأمنية للنظام
9. Exposure	الكشف غير المصرح به عن المعلومات
10. Interception	اعتراض حركة مرور البيانات
11. Inference	استنباط حركة مرور البيانات
12. Intrusion	التدخل، مثلاً: خصم حصل على معلومات حساسة بالتغلب على أنظمة حماية ال Access Control
13. Masquerade	التحايل، مثلاً: محاولة من قبل مستخدم غير مصرح له للوصول إلى نظام من خلال التظاهر كمستخدم مخول
14. Falsification	التزييف: وهو تبديل أو تغيير معلومات رسمية أو تقديم معلومات وهمية في قاعدة البيانات

15. Repudiation	ينكر المستخدم إرسال البيانات أو يرفض المستخدم تلقي البيانات أو امتلاكها
16. Incapacitation	الهجوم على توافر النظام
17. Corruption	الهجوم على سلامة النظام
18. Obstruction	عرقلة النظام: تتمثل إحدى طرق عرقلة تشغيل النظام في التداخل مع الاتصالات عن طريق تعطيل ارتباطات الاتصال أو تغيير معلومات التحكم في الاتصال
19. Usurpation	اغتصاب السلطة
20. Misappropriation	الاختلاس: من الممكن أن يشمل سرقة الخدمة
21. Misuse	سوء الاستخدام: يمكن أن يحدث عن طريق المنطق الخبيث أو القراصنة الذين حصلوا على وصول غير مصرح به إلى النظام
22. Passive Network Attacks	الهجمات العابرة: وهي في طبيعة التنصت، أو مراقبة البث. الهدف من المهاجم هو الحصول على المعلومات التي يتم إرسالها
23. Active Network Attacks	الهجمات النشطة: وهي محاولات لتغيير موارد النظام أو التأثير على عملها. تتضمن الهجمات النشطة بعض التعديلات على دفق البيانات أو إنشاء دفق خاطئ

الأسبوع الرابع

1. Fraud aaS	الاحتيال كخدمة: الصناعات الأكثر تضرراً من الاحتيال هي البنوك. وتم تطوير عدد كبير من التهديدات في العصر الرقمي لتوليد خسائر للمستخدمين، تحديداً في قطاع بطاقات الائتمانأو امتلاكها
2. Malware aaS	البرامج الضارة كخدمة: خدمة لسرقة البيانات وكلمات المرور، والتجسس على أنشطة المستخدمين، وإرسال الرسائل غير المرغوب فيها، و الوصول للأجهزة المصابة والتحكم فيها عن بُعد
3. Ransomware aaS	حملات الفدية كخدمة: الخدمة التي تستخدم فيها الأدوات لتنفيذ حملات الفدية
4. Attacks aaS	الهجمات كخدمة DDOS كخدمة نموذجية. يستخدم أيضًا لنشر المزيد من الأكواد الضارة، أو إرسال رسائل جماعية غير مرغوب فيها أو حتى استخدامها للحصول على عملات البيتكوين
5. Substantive Law	القانون الموضوعي: يحدد حقوق ومسؤوليات الموضوعات القانونية والتي تشمل الأشخاص والمنظمات والدول
6. Procedural Law	القانون الإجرائي: يرسم العمليات والإجراءات الواجب اتباعها لتطبيق القانون الموضوعي والقواعد لتمكين تطبيق القانون الموضوعي
7. Preventive Law	القانون الوقائي: يركز القانون الوقائي على التنظيم وتخفيف المخاطر
8. Capacity Building	بناء القدرات: تعليم المستخدمين كيفية منع الجرائم الإلكترونية