الأكاديمية العربية الدولية
Arab International Academy

إسم المادة: القرصنة الأخلاقية

إسم المحاضِر: م.خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

من هو الهاكرز؟

أطلقت هذه الكلمة في الستينيات لتشير إلى المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودراية حيث أنهم كانوا يقدمون حلولا لمشاكل البرمجة بشكل تطوعي في الغالب.

بالطبع لم يكن الويندوز أو ما يعرف بالـ Graphical User Interface أو GUI قد ظهر في ذلك الوقت ولكن البرمجة بلغة بيسيك واللوغو والفور توران في ذلك الزمن كانت جديرة بالاهتمام.

ومن هذا المبدأ غدا العارفين بتلك اللغات والمقدمين العون للشركات المؤسسات والبنوك يعرفون بالهاكرز وتعني الملمين بالبرمجة ومقدمي خدماتهم للآخرين في زمن كان عددهم لا يتجاوز بضع ألوف على مستوى العالم أجمع.

لذلك فإن هذا الوصف له مدلولات إيجابية ولا يجب خلطه خطأ مع الفئة الأخرى الذين يسطون عنوة على البرامج يكسرون رموزها بسبب امتلاكهم لمهارات فئة الهاكرز الشرفاء.

ما هي القرصنة الأخلاقية ETHICAL HACKING

هي عملية فحص واختبار الشبكة الخاصه بك من اجل إيجاد الثغرات ونقاط الضعف والتي من الممكن أن يستخدمها الهاكرز. الشخص الذي يقوم بهذه العملية هو الهاكر الأبيض (white hacker) الذي يعمل على الهجوم على أنظمة التشغيل بقصد اكتشاف الثغرات بها بدون الحاق أي ضرر.

وهذا من الطبيعي يؤدى إلى زيادة معدلات الأمن لدى النظام الخاص بك.

أو بمعنى أخر هو أنسان له مهارات تعطيه إمكانية الفهم والبحث عن نقاط الضعف في أنظمة التشغيل المختلفة، وهذا الشخص يعتبر نفسه هاكرز حيث يستخدم نفس معرفته ونفس أدواته ولكن بدون أن يحدث أي ضرر.

ما الفرق بين الهاكرز الأخلاقي والهاكرز العشوائي؟

- الهاكرز الأخلاقي (ethical hacker) هو خريج هذه الشهادة أو ما يعادلها حيث يكتسب قوته من خلال خبرة أفضل هاكرز في العالم ويستخدمها في تحسين الوضع الأمني لأنظمة الشبكات المختلفة.

- الهاكرز العشوائي هو الهاكر المدمر.

في هذا القسم سوف نتحدث عن المواضيع التالية:

1- Information Security Overview.

لمحة عامة عن أمن المعلومات

2-Information Security Threats And Attack Vector.

تهديدات أمن المعلومات ونواقل الهجوم

3-Hacking Concepts. مفاهيم القرصنة

4- Hacking Phases. مراحل القرصنة

5- Types of Attacks. أنواع الهجوم

6- Information Security Controls. ضوابط أمن المعلومات

1- Information Security Overview

تعريف: هذا المصطلح يشير إلى الطريقة المستخدمة لحماية أي نوع من المعلومات الحساسة او بمعنى أخر وضع حائط أمن حول المعلومات المهمة

وذلك لحمايتها من قبل الاتي:

1- Unauthorized access الولوج الوصول الغير مصرح به.

2- Disclosure الكشف عن هذه المعلومات.

3- Alteration التعديل على هذه المعلومات.

4- Destruction تدمير هذه المعلومات.

المعلومات تعتبر من المصادر الهامة لذلك يجب أن تكون آمنة، وذلك لان وقوع هذه المعلومات في الأيدي الخطأ قد يسبب تهديدا كبيرا على البنية التي تخصها هذه المعلومات.

IC3:هو اختصار إلى Internet Crime complaint centre وهي شركة تعمل على رصد الهجمات الإلكترونية ثم إعطاء تقرير عن هذا والموقع الإلكتروني لها هو www.ic3.gov

DATA BREACH INVESTIGATIONS REPORT (VERIZON BUSINESS)

شركه تعمل على رصد أنواع الهجمات وغيرها ثم تسلى تقرير عن هذا والموقع الإلكتروني الخاص بهم هو:
www.verizonbusiness.com

1- Information Security Overview

مصطلحات هامة:

HACK VALUE: هو مفهوم بين الهاكرز على انه شيء مهم يستحق القيام به أو مثير للاهتمام أو بمعنى آخر هو قيمة العمل الذي سوف يقوم به

EXPLOIT: هي طريقة اختراق نظام المعلومات من خلال نقاط الضعف الموجودة فيه وهذا المصطلح يستخدم في أي هجمه من أي نوع على الأنظمة والشبكات ويمكن أن يكون أيضا عباره عن تطبيقات أخرى أو أوامر (commands).

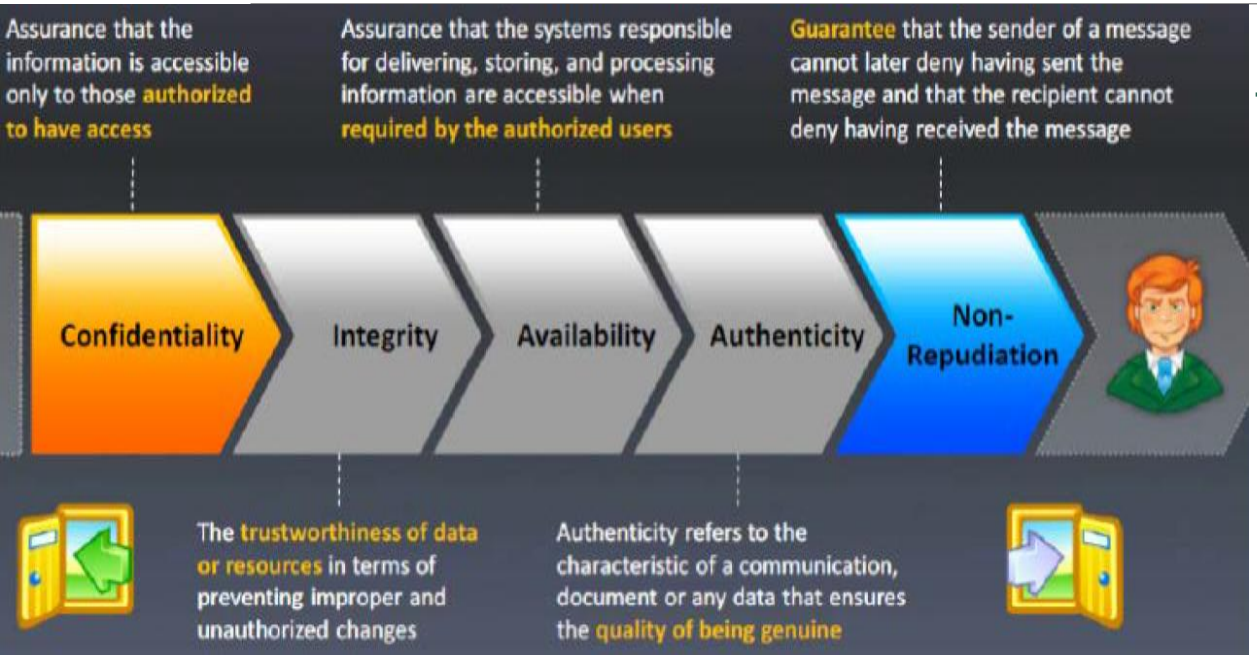
VULNERABILITY: هو مصطلح يعبر عن نقاط الضعف الثغرات، وقد تكون نقاط الضعف هذه إما نقاط ضعف في التصميم (design code) أو أخطاء error/bugs .

TARGET OF EVALUATION: هو نظام المعلومات أو الشبكات IT system أو برنامج أو محتوى يستخدم للوصول إلى درجه معينه من الأمن وهذا النوع يساعد في فهم وظائف وتقنيات ونقاط الضعف في الأنظمة والمنتجات.

ZERO-DAY ATTACK: هو عباره عن هجوم يستغل ثغره امنيه لم تكن معروفة مسبقا للمبرمجين في تطبيق كمبيوتر.

DAISY CHAINING: تعنى أن الهاكر الذي استطاع الوصول إلى قاعدة المعلومات فانه يعمل على تكملة أهدافه.

1- Information Security Overview



ELEMENT OF INFORMATION SECURITY عناصر أمن المعلومات:

هي الحالة التي يكون فيها عملية جعل المعلومات والبنية التحتية للأنظمة (Infrastructure) من الصعب سرقتها وتتكون من خمس مراحل:

1- الخصوصية: Confidentiality

2- السلامة: Integrity شكل البيانات منع أي تغير على البيانات

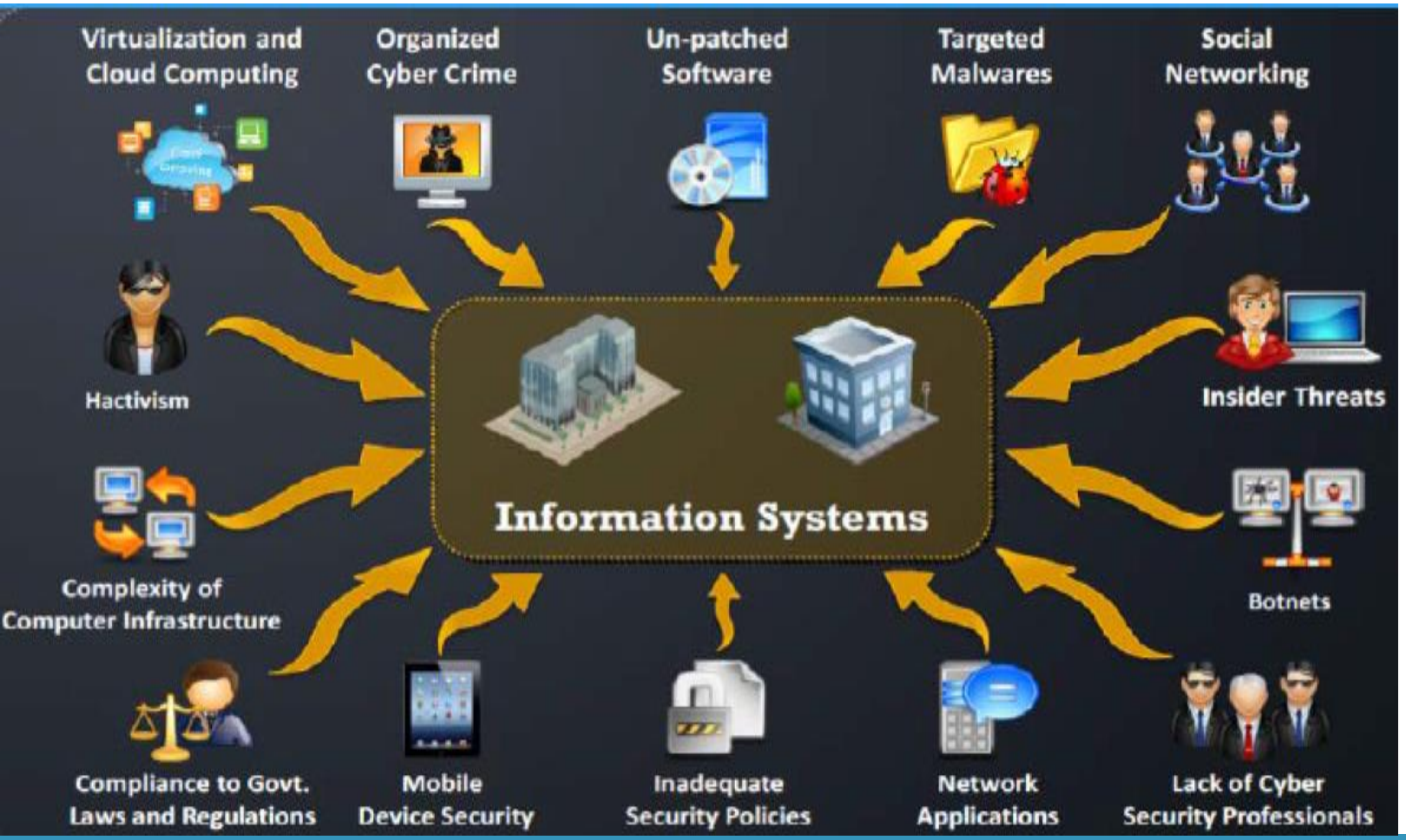
3- الإتاحة: Availability

4- المصادقة: Authenticity والأدوار الرئيسية من عملية المصادقة authentication تشمل الاتي:

- التأكد من هوية المستخدم قل هو هذا المستخدم من المعرف لديه أم لا.
- ضمان أن الرسالة القادمة منه أصلية ولم يتم التغير في محتوا اها
- تستخدم كل من biometric و smart cards والشهادة الرقمية digital certificate في التأكد من مصداقية البيانات.

5- عدم الإنكار (عدم التنصل): Non-repudiation

2-information Security Threats And Attack Vector: A- Attack Vector



في هذا الفصل سوف ندرس ما يلي:

A - Attack Vector من أين تأتى الهجمات؟
B- الهدف من وراء هذا الهجوم Goal of attack
C-التهديدات الأمنية المحتملة Security Threat

A- Attack Vector:

تمكن المهاجم من الاستفادة من الثغرات الموجودة في نظام المعلومات لحمل الهجوم الخاص به المسارات المتاحة التي ممن الممكن أن يستخدمها المهاجم في عملية القرصنة كالاتي تظهر في الشكل الجانبي.

2-information Security Threats And Attack Vector: B- Goal of attack

نلاحظ هنا أن أي هجوم يتكون من ثلاثة عناصر:

1- دافع الهجوم (Motive) وذلك لان أي هجوم إما ان يكون لهدف أو لدافع معين (motive, goal or objective) مثال لهذه الأهداف تعطيل استمرارية العمل (disrupting business continuity ، سرقة المعلومات، تنفيذ انتقام من مؤسسه معينه أو سرقة شيء ذات قيمه من مؤسسه ما.

هذه الأهداف تختلف من شخص إلى أخر على حسب الحالة العقلية للمهاجم الذي حمله على القيام بهذا العمل.

2- الطريقة (method) : بمجرد امتلاك المهاجم للهدف فانه يستخدم العديد من الطرق والأساليب لاستغلال

3- (نقاط الضعف Vulnerability): هو استغلال نقاط الضعف (exploit vulnerability) في نظام المعلومات information system أو في security policy في عملية الهجوم حتى يصل إلى تحقيق هدفه.

2-information Security Threats And Attack Vector: C- Security Threat

التهديدات الأمنية المحتملة تنقسم هنا إلى ثلاثة أقسام كالاتي:

1- التهديدات الطبيعية Natural Threats:

التهديدات الطبيعة تشمل الكوارث الطبيعية مثل الزلازل earthquake او الفيضانات floods أو الأعاصير hurricanes أو أي كارثة طبيعية أخرى التي لا يمكن إيقافها أو التحكم فيها.

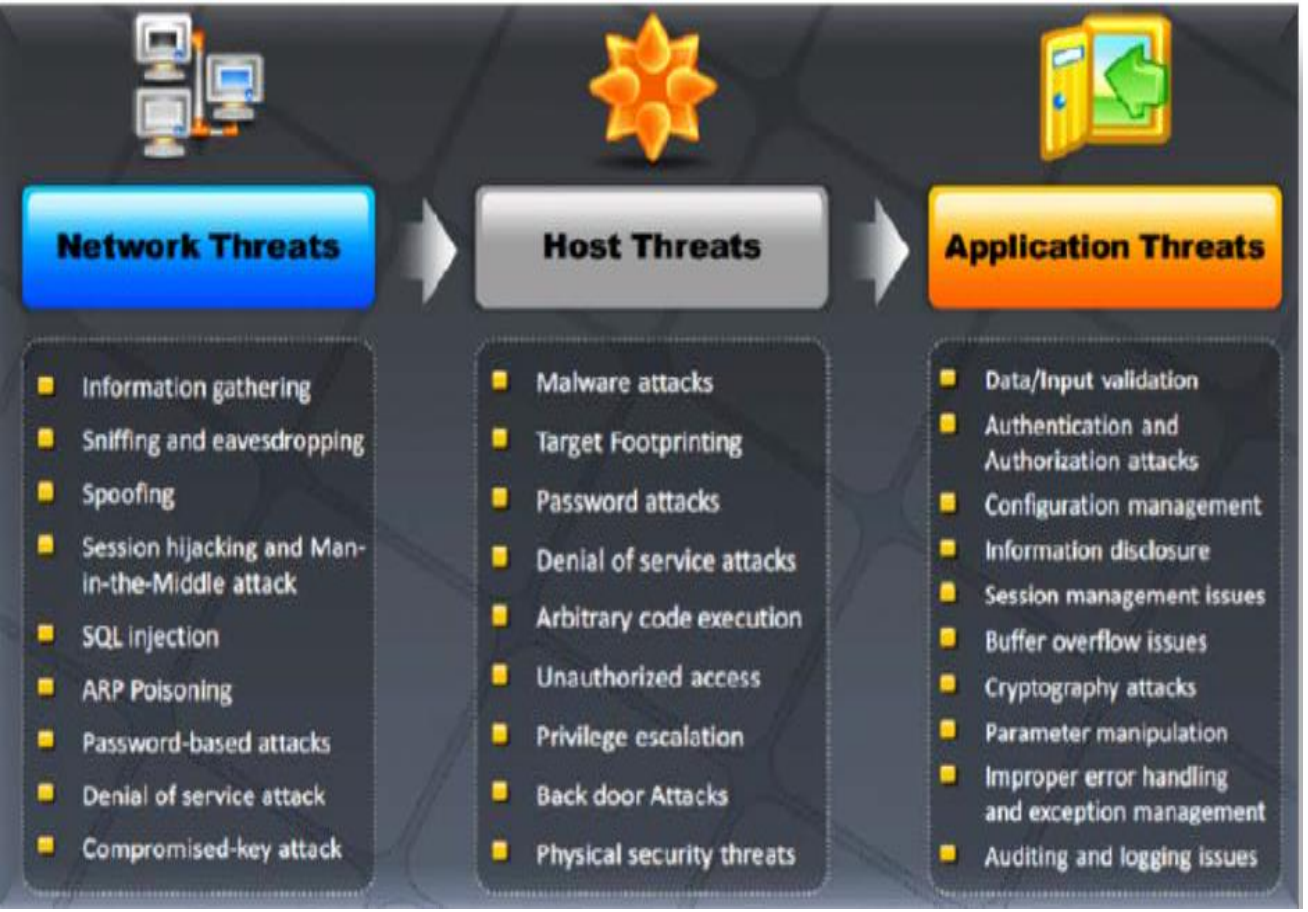
2- التهديدات الفيزيائية Physical Threats:

هذا النوع من التهديد ينتج نتيجة تلف أي جزء من الأجهزة المستخدمة سواء بواسطة الحريق أو الماء أو السرقة أو التداخلات الفيزيائية.

3- التهديدات البشرية Human Threat:

هذا النوع من التهديدات ينتج نتيجة الهجمات سواء من داخل المنظمة (Insider) أو من الخارج (Outsider).

2-information Security Threats And Attack Vector: C- Security Threat (Outsider Types)



Outsider Types:

A- Network Threats:

Information gathering
Sniffing and eavesdropping
Spoofing
Session hijacking and man-in-middle attack
SQL injection
ARP Poisoning 6 Denial of service attack
Password-based attack
Denial of service attack
Comprised key attack

2-information Security Threats And Attack Vector: C- Security Threat (Outsider Types)

B- Host Threats:

Malware attacks

Target Foot printing

Password attacks

Denial of service attacks

Arbitrary code execution

Privilege escalation

Unauthorized access

Back door attacks

Physical security threats

C- Application Threats:

Data/Input validation

Authentication and Authorization attacks

Configuration management

Information disclosure

Session management issues

Buffer overflow issues

Cryptography attacks 6 Parameter manipulation

Improper error handling and exception management

Auditing and logging issues

3-Hacking Concepts (Hacking & Ethical hacking)

ما هو الفرق بين الهاكر المدمر (Hacking) والهاكر الأخلاقي (Ethical hacking)؟

1- Hacking التهكير المدمر:

يشير إلى استغلال ثغرات الأنظمة vulnerability والأخلال بالضوابط الأمنية compromising security controls للحصول على الدخول الغير مصرح به unauthorized access لموارد النظام وهذا يشمل تعديل النظام (modifying system) أو بعض مميزات البرامج application features لتحقيق الهدف.

2- التهكير الأخلاقي Ethical hacking:

يشمل استخدام أدوات التهكير وبعض التقنيات والحيل التعريف الثغرات وذلك للتأكد من امن النظام وهذا يركز على استخدام تقنيه مشابهة للتهكير المدمر لكشف الثغرات في النظام الأمن.

3-Hacking Concepts (Hacker types)

Black Hats المخترق ذو القبعة السوداء :هم أفراد لديهم مهارات استثنائية في علم الحوسبة (computer science) - اللجوء إلى قشطة ضارة أو مدمرة، كما أنهم معروفين أيضا باسم كراكرز (crackers).

White Hats المخترق ذو القبعة البيضاء :هم أفراد يعتنقون مهارات القرصنة (الاختراق) ويستخدمون هذه المهارات من اجل الأهداف الدفاعية, كما أنهم معروفين أيضا بقسم المحللين الأمنين (security analysts).

Gary Hats المخترق ذو القبعة الرمادية: هم أفراد لديهم مهارات الهاكر يستخدمونها في الهجوم والدفاع على حد سواء في أوقات مختلفة وهؤلاء يقعون بين Black Hats و White Hats هؤلاء يمكنهم أيضا مساعدة الهاكر في إيجاد الثغرات المختلفة في الأنظمة والشبكات وفي نفس الوقت يقومون بمساعدة المؤسسات في تحسين منتجاتهم (software and hardware) عن طريق جعلها أكثر أمانا وهكذا.

Suicide Hacker (الهاكر المنتحرون): ويطلق عليه أيضا الهاكر المنتحر لأنه يشبه إلى حد كبير الشخص الذي يقوم بتفجير نفسه غير مهتم بحياته من أجل هدف ما. وهم عباره عن أفراد يهدفون إلى إسقاط البنية التحتية الحيوية لسبب ما و لا يقلقون بشأن 30 عاما في في السجن ولا يخفون أفعالهم بعد القيام بالهجمة أي بمعنى أخر يسرقون علناً ولقد انتشر هذا النوع في السنوات الأخيرة.

3-Hacking Concepts (Hacker types)

Script Kiddies: هو هاكر ليس لديه مهارات الهاكر ولكن يتحايل على الأنظمة باستخدام بعض الأدوات والتطبيقات التي تم تطويرها بواسطة الهاكرز الحقيقين وهؤلاء من السهل لهم استخدام التطبيقات في اكتشاف الثغرات في الأنظمة المختلفة هذا النوع من الهاكر يركز في الأساس على كمية الهجمات أكثر من قوة وفاعلية الهجمة التي يقوم بإنشائها.

Spy Hackers: هم عباره عن افراد يتم تأجيرهم من قبل المنظمات المختلفة لاختراق والحصول على أسرار من المنظمات المنافسة لهم.

Cyber Terrorists ارهاب العالم الإلكتروني: هي هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية وتعتبر جرائم اتلاف للنظم والمعطيات أو جرائم تعطيل المواقع وعمل الأنظمة.

State Sponsored Hackers: هم عباره عن أفراد يتم تأجيرهم بواسطة الحكومات من اجل الاختراق والحصول على معلومات على درجة عالية من السرية و تدمير بعض انظمة المعلومات الأخرى للحكومات الأخرى.

4- Hack phases (A-Reconnaissance)

مراحل القرصنة تشمل: Hack phases

Reconnaissance-A الاستطلاع

Scanning-B المسح

Gaining Access-C الحصول على الوصول

Maintaining Access-D الحفاظ على الوصول

Clearing Tracks-E تنظيف الأثر

Reconnaissance-A الاستطلاع:

يطلق عليها أيضا preparatory phase أي المرحلة التحضيرية والتي فيها يقوم المهاجم بجمع أكبر قدر ممكن من المعلومات عن الهدف لتقييمه قبل تنفيذ هجمته.

أيضا في هذه المرحلة المهاجم يهتم بالاستخبارات التنافسية لمعرفة المزيد عن الهدف.

هذه المرحلة تشمل أيضا network scanning فحص الشبكة سواء من الداخل أو الخارج بدون دخول على النظام.

هذه المرحلة هي المرحلة التي فيها يضع المهاجم استراتيجيات الهجوم والتي من الممكن أن تأخذ بعض الوقت حتى يحصل على بعض المعلومات المهمة.

وينقسم Reconnaissance (الاستطلاع) إلى:

Passive Reconnaissance: التعامل مع الهدف ولكن بطريقه غير مباشره للحصول على معلومات مثل سجلات البحث العامة ونشرات الأخبار والهندسة الاجتماعية و dumpster diving وغيرها.

Active reconnaissance: ينطوي على التفاعل المباشر مع الهدف باستخدام أي وسيلة مثل استخدام الأدوات للكشف عن المنافذ المفتوحة مكان تواجد الموجه الراوتر وهكذا.....

4- Hack phases (B-Scanning, C- Gaining Access, D-Maintaining Access, E- Clearing Tracks)

Scanning-B المسح:

المسح هو ما يفعله المهاجم قبل تنفيذ الهجوم. ويشير المسح إلى فحص الشبكة للحصول على معلومات محددة على أساس المعلومات التي تم جمعها من خلال عملية الاستطلاع (Reconnaissance).

Gaining Access-C الحصول على الوصول:

هذه المرحلة تعتبر أهم مرحله ويطلق عليها أيضا potential damage.

وهذه المرحلة تشير إلى مرحلة الاختراق.

المخترق يستغل الضعف في النظام، حيث يمكن أن يحدث ذلك على مستوى شبكة محلية (LAN) أو الأنترنت أو على مستوى نظام التشغيل.

Maintaining Access-D الحفاظ على الوصول:

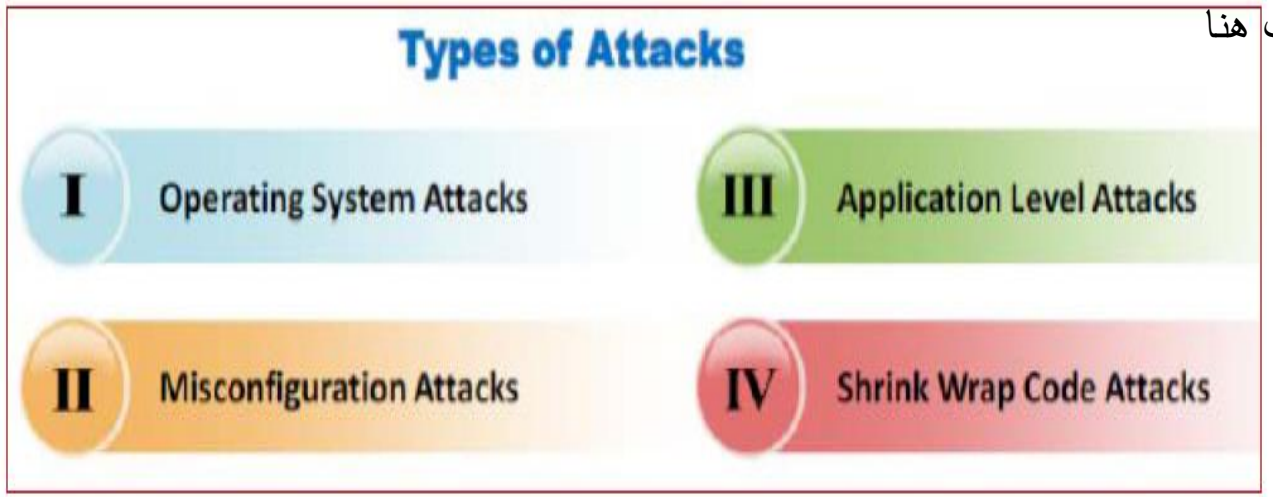
وتشير إلى المرحلة التي يحاول فيها المخترق حفظ ملكية الدخول مجددا إلى النظام.

من خلال وصول حصري باستخدام Backdoors,Rootkits,Trojans مما يسمح للمخترق بتحميل ورفع الملفات، والتعامل مع البيانات والتطبيقات على النظام المخترق .

Clearing Tracks-E تنظيف الأثر:

تشير إلى الأنشطة التي يقوم بها المخترق لإخفاء دخوله إلى النظام، بسبب الحاجة للبقاء لفترات طويلة، ومواصلة استخدام الموارد، وتشتمل إخفاء بيانات الدخول والتغيير في ملف Log

5- Types of Attacks



1- Operating System Attacks : ويستخدم OS vulnerabilities حيث هنا يبحث المهاجم عن ثغرات في نظام التشغيل هذه الثغرات للدخول إلى نظام الشبكة.

2- Application Level Attacks: إن معظم التطبيقات / البرامج تأتي مع وظائف وميزات لا تعد ولا تحصى. ولكن مع ندرة من الوقت لإجراء اختبار كامل قبل خروج المنتج إلى السوق.
يؤدى الى ان هذه التطبيقات يكون لديها بعض من نقاط الضعف المختلفة والتي قدتصبح مصدرا للهجوم من قبل الهاكر.

3- Misconfiguration Attacks: معظم مديري الأنظمة Admin لا يملكون المهارات الضرورية من اجل صيانة أو بعض المسائل / القضايا والتي من الممكن أن تؤدى إلى أخطاء في عمليات الإعداد بعض هذه الأخطاء من الممكن أن تكون مصدرا للمهاجم للدخول إلى الشبكة والنظام الذي يستهدفه.

4- Shrink Wrap Code Attacks: تطبيقات أنظمة التشغيل تأتى بالعديد من ملفات الاسكريبت المبسطة لكي تسهل العمل على مديري الأنظمة (Admin) ولكن مثل هذه الاسكربات تحتوي أيضا على العديد من الثغرات والتي من الممكن أن تؤدى إلى هذ النوع من الهجوم.

5- Types of Attacks: 1- Operating System Attacks

1- Operating System Attacks: أنظمة التشغيل، والتي يتم تحميلها اليوم مع الكثير من المميزات، أصبحت تزداد تعقيدا. ومع الاستفادة من الكثير من هذه المميزات التي توفرها هذه الأنظمة من قبل المستخدمين، تجعل النظام عرضة لمزيد من نقاط الضعف، وبالتالي عرضه للقراصنة. أنظمة التشغيل تعمل على تشغيل العديد من الخدمات مثل واجهات المستخدم الرسومية GUI. وهذه تدعم استخدام المنافذ ports وطريقة الوصول إلى شبكة الإنترنت، لذلك فهذه تتطلب الكثير من التغير والتبديل للتحكم في هذا. هنا يبحث المهاجم عن ثغرات في نظام التشغيل Os vulnerabilities ويستخدم هذه الثغرات للدخول إلى نظام الشبكة لإيقاف المهاجمين من الدخول إلى شبكة الاتصال الخاصة بك، فإن مسؤولي الشبكة أو النظام لابد لهم من مواكبة الاكتشافات والطرق الجديدة المختلف والمتبعة من قبل المهاجمين ومراقبة الشبكة بشكل مستمر. تطبيق التصحيحات والإصلاحات ليست سهلة في الوقت الحاضر لأنها شبكة معقده.

بعض من هذه الهجمات تشمل الآتي:

Buffer overflow vulnerabilities
Bugs in the operating system
Unpatched operating system
Exploiting specific network protocol implementation
Attacking built-in authentication systems
Breaking file system security
Cracking passwords and encryption mechanisms

5- Types of Attacks: 2- Application Level Attacks

يتم إصدار التطبيقات إلى سوق العمل مع العديد من المميزات والعديد من الأكواد المعقدة.

ومع الطلب المتزايد للتطبيقات لما تحمله من وظائف وميزات، أدى إلى إهمال مطوري التطبيقات الوضع الأمني للتطبيق، والذي أعطى الفرصة لوجود العديد من الثغرات الهاكر يعمل على اكتشاف هذه الثغرات الموجودة في التطبيقات باستخدام العديد من الأدوات والتقنيات.

التطبيقات لما بها من ثغرات تصبح عرضة للهجمات من قبل الهاكر نتيجة الأسباب الآتية:

1 - لمطوري البرامج الجداول الزمنية الضيقة لتسليم المنتجات في الوقت المحدد tight schedules to deliver والذي يؤدى إلى ظهور التطبيقات في سوق العمل بدون الاختبارات الكافية عليه.

2- تطبيقات البرامج تأتى مع العديد من الوظائف والمزايا.

3- ليس هناك ما يكفي من الوقت لأداء اختبار كامل قبل الإفراج عن المنتجات dearth of time .

4- الأمن في كثير من الأحيان تكون مرحلة لاحقة، ويتم تسليمها فيما بعد باعتبارها عناصر إضافية.

إن ضعف أو عدم وجود خطأ التدقيق في التطبيقات أمر يؤدى إلى الآتي:

الهجوم بإغراق ذاكرة التخزين المؤقت Buffer overflow attacks bots - Active content - Cross-site scripting

Malicious boots – SQL injection attacks - Denial-of service and SYN attacks

5- Types of Attacks: 2- Application Level Attacks

امثله على الهجمات على مستوى التطبيقات:

Session Hijacking-1

```
1:  <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:     <forms cookieless="UseUri">
5:   </system.web>
6:  </configuration>
```

TABLE 1.1: Session Hijacking Vulnerable Code

```
1:  <configuration>
2:   <system.web>
3:     <authentication mode="Forms">
4:     <forms cookieless="UseCookies">
5:   </system.web>
6:  </configuration>
```

TABLE 1.2: Session Hijacking Secure Code

denial of service-2

```
1:  Statement stmnt = conn.createStatement ();
2:  ResultSet rsltset = stmnt.executeQuery ();
3:  stmnt.close ();
```

TABLE 1.3: Denial-of-Service Vulnerable Code

```
1:  Statement stmnt;
2:  try {stmnt = conn.createStatement ();
3:  stmnt.executeQuery (); }
4:  finally {
5:  If (stmnt! = null) {
6:  try { stmnt.close ();
7:  } catch (SQLException sqlexp) { }
8:  } catch (SQLException sqlexp) { }
```

TABLE 1.4: Denial-of-Service Secure Code

بعض الهجمات الأخرى التي تكون على مستوى التطبيقات كالاتي:

1. Phishing
2. Session hijacking
3. Man-in-the middle attacks
4. Parameter/from tampering
5. Directory traversal attacks

5- Types of Attacks: 3-Misconfiguration Attacks, 4- Shrink Wrap Code attacks

3-Misconfiguration Attacks نقاط الضعف في الإعداد (misconfiguration) يؤثر على ملقمات / سيرفرات الويب، ومنصات التطبيق، وقواعد البيانات، والشبكات، أو الإطارات (framework) التي قد تؤدي إلى الدخول الغير المشروع illegal access أو احتمالية امتلاك النظام.

إذا تم إعداد النظام بشكل خاطئ، مثل عندما يتم تغيير في تصريحات / أذونات الملف، فيؤدى إلى جعله غير آمن.

4-Shrink Wrap Code Attacks عند تثبيت نظام التشغيل أو التطبيقات فانه يأتي مع العديد من الاسكربات والتي تسهل على Admin التعامل معها.

ولكن المشكلة هنا " ليست ضبط " أو تخصيص هذه الاسكربات التي من الممكن أن تؤدى إلى الرموز الافتراضية

أو هجوم shrink-wrap code.

6- Information Security Controls A- Introduction

لماذا الهاكر الأخلاقي ضروري ومهم؟

هناك نمو سريع في مجال التكنولوجيا، لذلك هناك نمو في المخاطر المرتبطة بالتكنولوجيا، والقرصنة الأخلاقية يساعد على التنبؤ بمختلف نقاط الضعف المحتملة في وقت مبكر وتصحيحها دون تكبد أي نوع من الهجمات القادمة من الخارج.

القرصنة الأخلاقية: ethical hacking تشمل التفكير الإبداعي، واختبار مواطن الضعف والتدقيق الأمني الذي لا يمكنه التأكد من أن الشبكة آمنة.

استراتيجية الدفاع من العمق: Defense-in-Depth Strategy لتحقيق ذلك، تحتاج المنظمات لتنفيذ استراتيجية "الدفاع من العمق" عن طريق اختراق شبكاتهم لتقدير مواطن الضعف وعرضهم لهذه.

الهجوم المضاد Counter the Attacks الهاكر الأخلاقي هو ضروري لأنه يسمح بمجابهة الهجمات التي يشنها القراصنة الخبثاء بطريقة التوقع anticipating methods والتي يمكن استخدامها لاقتحام النظام.

المخترق الأخلاقي يحاول أن يجاوب على الأسئلة التالية:

ماذا يمكن أن يرى الدخيل على نظام الهدف؟ reconnaissance and scanning مراحل الاستطلاع والمسح.

ما الذي يمكن أن يقوم به المتسلل بهذه المعلومات؟ Gaining Access and Maintaining Access مراحل الوصول والمحافظة على الوصول.

هل يوجد دخيل على النظام؟ reconnaissance and covering tracks مراحل الاستطلاع وتغطية الأثر .

هل جميع أجزاء نظام المعلومات يتم حمياته وتحديثه وتمكين الباتشات باستمرار ؟.

هل مقايس امن المعلومات ممتثله لمعاير الصناعة والقانون؟

6- Information Security Controls: B- Scope and limitations of the ethical hackers

Scope And Limitations Of The Ethical Hackers نطاق وحدود القراصنة الأخلاقيين:

Scope:

ما يلي نطاق القرصنة الأخلاقية:

- القرصنة الأخلاقية هو عنصر حاسم لتقييم المخاطر، ومراجعة الحسابات، ومكافحة الاحتيال، وأفضل الممارسات، والحكم الجيد.
- يتم استخدامه لتحديد المخاطر وتسليط الضوء على الإجراءات العلاجية، والحد من تكاليف تكنولوجيا المعلومات والاتصالات ICTعن طريق إيجاد حل لتلك الثغرات.

Limitations:

ما يلي حدود القرصنة الأخلاقية:

- ما لم تعرف الشركات أولا ما الذي يبحثون عنه، ولماذا يتعاقدون مع مورد خارجي لاختراق الأنظمة في المقام الأول؛ وهناك احتمالات بأن لن يكون هناك الكثير لتكسبه من خبرة.
- لذا القراصنة الأخلاقيين الوحيدين الذين يمكنهم أن يساعدوا المنظمات لفهم أفضل لأوضاعهم الأمنية، ولكن الأمر متروك للمنظمة لوضع الضمانات الأمنية على الشبكة.

6- Information Security Controls: C- Ethical Hacker Skills

Ethical Hacker Skills:مهارات الهاكر الأخلاقي

القرصنة الأخلاقية هي عملية قانونيه يتم تنفيذها بواسطة pen tester لإيجاد نقاط الضعف في بيئة تكنولوجيا المعلومات.

ولكي يتم هذا يجب أن يتمتع الهاكر الأخلاقي ببعض المهارات كالاتي:

1- خبير في مجال الحوسبة وبارع في مجالات التقنية

2- يملك معلومات قوية في علم البرمجة والشبكات

3- معرفته المتعمقة للأشياء المستهدفة، مثل ويندوز ويونكس ولينكس.

4- لدية معرفة مثالية لإقامة الشبكات والأجهزة ذات الصلة والبرمجيات

5- لدية معرفة مثالية في الأجهزة والتطبيقات التي قدمت عن طريق بائعي الكمبيوتر وأجهزة الشبكات ذات شعبية

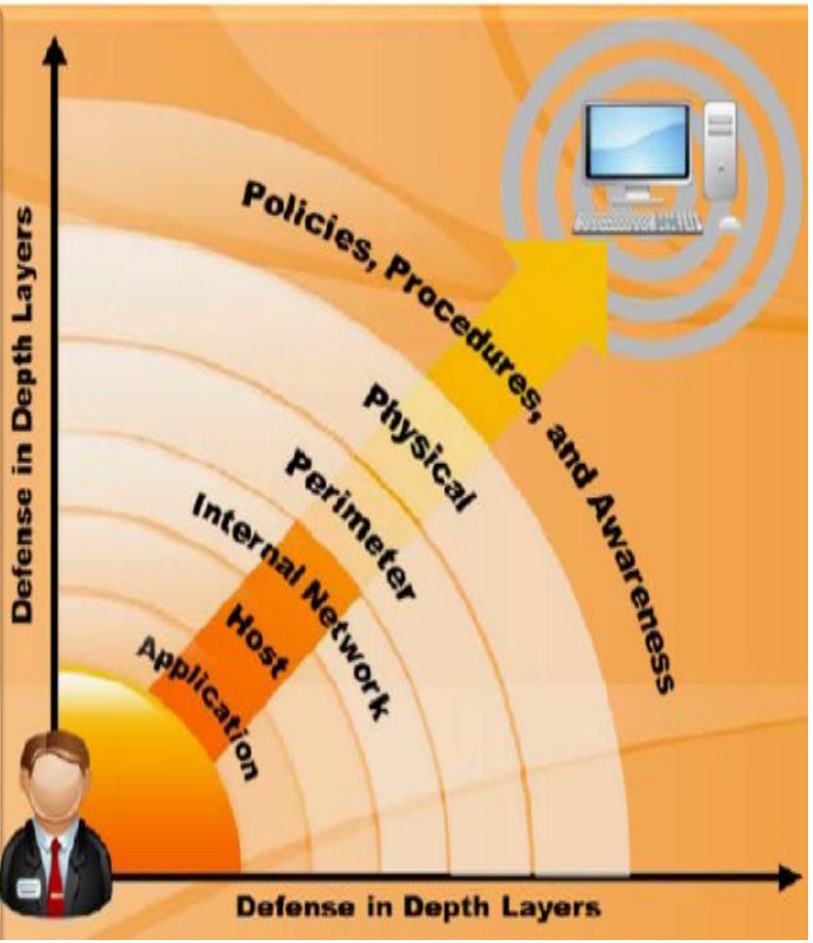
6- ليس من الضروري أن يحمل معرفه إضافية متخصصة في الوضع الأمني.

7- ينبغي أن يكون على دراية ببحوث الضعف

8- ينبغي أن يكون لديه السيادة في مختلف تقنيات الاختراق أو القرصنة.

9- ينبغي أن يكون على استعداد لاتباع سلوك صارم إذا احتاج الأمر لهذا.

6- Information Security Controls: D- Defence-in-Depth



الدفاع من العمق Defence-in-Depth :

- يتم اتخاذ العديد من التدابير المضادة للدفاع من العمق Defence-in-Depth لحماية أصول المعلومات في الشركة.
- تستند هذه الاستراتيجية على مبدأ عسكري أنه من الصعب على العدو هزيمة نظام دفاعي معقد ومتعدد الطبقات من اختراق حاجز واحد.
- إذا حدث واستطاع الهاكر الوصول إلى النظام، فإن الدفاع من العمق Defence-in-Depth يقلل التأثير السلبي ويعطي الإداريين والمهندسين الوقت لنشر مضادات جديدة أو محدثة لمنع تكرار هذا الاختراق مرة أخرى.
- الدفاع من العمق Defence-in-Depth هي استراتيجية الأمن التي توضع عدة طبقات واقية في جميع أنحاء نظام المعلومات.
- يساعد على منع وقوع هجمات مباشرة ضد نظام المعلومات والبيانات بسبب كسر طبقة واحدة لا يؤدي إلا انتقال المهاجم إلى الطبقة التالية.

6- Information Security Controls: E- Incident Management Process

Incident Management Process عملية الإدارة الطارئة:

هي مجموعة من العمليات المحددة لتحديد وتحليل، وتحديد الأولويات، وتسوية الحوادث الأمنية لاستعادة النظام إلى عمليات الخدمة العادية في أقرب وقت ممكن ومنع تكرار نفس الحادث.

الغرض من عملية إدارة الحوادث كالاتي:

- تحسين جودة الخدمة improves service quality
- حل المشاكل الاستباقية Proactive problem resolution
- يقلل من تأثير الحوادث على الأعمال التجارية المنظمات Reduces the impact of incidents on business/organization
- يلتقي متطلبات الخدمة المتوافرة Meets service availability requirements
- يزيد من كفاءة الموظفين وإنتاجيتهم Increases staff efficiency and productivity
- يحسن رضا المستخدم / العملاء Improves user/customer satisfaction
- يساعد في التعامل مع الحوادث في المستقبل Assists in handling future incidents

6- Information Security Controls: F- Information Security Policies

سياسات أمن المعلومات Information Security Policies

سياسة الأمن Security Policy هو وثيقة أو مجموعة من الوثائق التي تصف الضوابط الأمنية التي ينبغي تنفيذها في الشركة على مستوى عالي لحماية الشبكة التنظيمية من الهجمات سواء من الداخل أو الخارج.

- تحدد هذه الوثيقة الهيكل الأمني الكامل للمنظمة، وتشملالوثيقة أهداف واضحة، والأهداف والقواعد والأنظمة والإجراءات الرسمية، وهلم جرا. - - هذه السياسات من الواضح إنها تذكر الأصول التي ينبغي حمايتها والشخص الذي يمكنه تسجيل الدخول والوصول إليها، الذين يمكن عرض البيانات المحددة، فضلا عن الناس الذين يسمح لهم بتغيير البيانات، وما إلى ذلك من دون هذه السياسات، فإنه من المستحيل حماية الشركة من الدعاوى القضائية المحتملة، العائدات المفقودة، وهلم جرا.
- على وجه العموم سياسة الأمن هي الخطة التي تعرف الاستخدام المقبول أو المرضي لجميع الوسائط الإلكترونية في المنظمة.
- سياسات الأمن هي أساس البنية التحتية الأمنية Security infrastructure هذه السياسات تعمل على تأمين وحماية موارد المعلومات للمؤسسة وتوفير الحماية القانونية للمنظمة.
- هذه السياسات مفيدة في المساعدة في تحقيق الوعي للموظفين العاملين في المؤسسة على العمل معا لتأمين اتصالاتهم، وكذلك التقليل من مخاطر ضعف الأمن من خلال عامل الأخطاء البشرية مثل الكشف عن معلومات حساسة إلى مصادر غير مصرح بها أو غير معروفه الاستخدام الغير لائق للإنترنت، وما إلى ذلك.
- بالإضافة إلى ذلك، توفر هذه السياسات الحماية ضد الهجمات الإلكترونية والتهديدات الخبيثة، والاستخبارات الأجنبية، وهلم جرا.
- أنها تتناول أساسا الأمن المادي، وأمن الشبكات، أذون الدخول الحماية من الفيروسات، والتعافي من الكوارث.

نهاية المحاضرة

آمل أن تكونوا قد حققتم الفائدة

شكرا لحضوركم .....