



1

الهاكر الأخلاقي

المقدمة (Introduction)

books

By

Dr.Mohammed Sobhy Teba

Introduction

<https://www.facebook.com/tibea2004>

CONTENTS

3Introduction to Ethical Hacker
3	ما هو الهاكرز؟
3	ما هو الهاكر الأخلاقي ethical hacking
3	ما الفرق بين الهاكرز الأخلاقي والهاكرز العشوائي؟
4	1.2 رؤية مبسطة عن امن المعلومات (Information security overview)
4	IC3
5Data Breach Investigations Report (Verizon business)
5	بعض المصطلحات المهمة:
5Hack Value
5Exploit
5Vulnerability
5Target of Evaluation
5Zero-day Attack
5Daisy chaining
6	بعض المصطلحات التعريفية الأخرى:
6	عناصر امن المعلومات (element of information security)
6	مستوى الأمان في أي من الأنظمة أو الشبكات الموجودة تتحدد بقوة الثلاثة أشياء التالية:
7Information security threats and attack vector
7Attack vector من أين يأتي هذا الهجوم؟
7Goal of attack الهدف من وراء هذا الهجوم
8Security Threat التهديدات الأمنية المحتملة
9Information Warfare (حرب المعلومات)
10IPv6 security threats (التهديدات الأمنية من استخدام IPv6)
10IPv6 التهديدات التي تكمن نتيجة استخدام IPv6
11Hack concept (مفهوم الهاكنج) 1.4
12	من هو الهاكرز؟
12	أنواع الهاكرز:
13Hacktivism
13Hack Phase (مراحل القرصنة) 1.5



14	(أنواع الهجمات) Type of Attacks 1.6
15	Operating System attacks-1
15	Application-level attacks-2
16	امثله على الهجمات على مستوى التطبيقات:
16	Misconfiguration attacks-3
16	Shrink wrap code attacks-4
17	(التحكم في امن المعلومات) Information security control 1.7
18	نطاق وحدود الفراصنة الأخلاقيين (scope and limitations of the ethical hackers)
18	Scope
18	Limitations
18	مهارات الهاكر الأخلاقي :Ethical Hacker Skills
18	(الدفاع من العمق) Defense-in-Depth
19	(عملية الإدارة الطارئة) Incident Management Process
20	سياسات أمن المعلومات Information Security Policies
20	أهداف السياسات الأمنية (security policies) :
20	(تصنيف السياسة الأمنية) Classification of security policy
21	هيكل ومحظوي السياسات الأمنية structure and contents of security policies
21	هيكل السياسات الأمنية (Structure of security policy)
21	محظوي السياسات الأمنية (Contents of security policy)
21	أنواع سياسات الأمن (Types of Security policy)
22	الخطوات لإنشاء وتطبيق السياسات الأمنية (Steps to Create and Implement Security Policies)
22	امثله على السياسات الأمنية كالاتي:
23	بحوث الثغرات الأمنية (Research Vulnerability security)
23	أدوات الوصول الى الأبحاث عن الضعف Vulnerability research website
25	ما هو اختبار الاختراق (what is penetration testing)
25	ما أهمية pen tester
25	منهج اختبار الاختراق penetration testing methodology



INTRODUCTION TO ETHICAL HACKER

"إذاً، إذا كنت تعرف العدو وتعرف نفسك – فلا حاجة بك للخوف من نتائج معركة. إذا عرفت نفسك لا العدو، وكل نصر تحرزه سيقابلها هزيمة تلقاها. إذا كنت لا تعرف نفسك أو العدو – ستنهزم في كل معركة"

كتاب فن الحروب للعبري والفيلسوف العسكري الصيني سون تزو

في عصرنا الحالي انقلب الموازين، أصبح الصغار كبارا بعقولهم في عالم الهاكر أعمارهم تتراوح ما بين الـ 16 سنة والـ 20 سنة. في هذا السن تجد كثيرون محترفون في عالم الهاكرز، منهم الطيب ومنهم الخبيث، المخترقون أجناس. وقد تجد فيهم من يساعد الناس في استرجاع بياناتهم وبريدهم الإلكتروني. ومنهم من يقوم بسرقة الناس مدعيا أنه شخص طيب وهو في الأصل متخصص يريد أن يخترق عبءا، كثرت عمليات الاختراقات في العالم العربي. ولاحظنا الاختراقات الكثيرة على الواقع العربي وبأيدي عربية للأسف. أصبح الهاكر وسيلة للتهديد ووسيلة للانتقام وأصبحت سلطة للاستفادة من الأشخاص إما من أجل المال أو شيء يريده ولم يجده إلا عند شخص ما، هذه الثلاثة من أغلب ما يحدث بين ما يسمون بالهاكر. لذلك فمن المهم جدا أن نضع في اعتباراتنا أن الهاكر يعمل على كسر الشبكة الخاصة بك والأنظمة التي تحتويها من أجل العديد من الأسباب والأهداف، لذلك فإنه من المهمفهم كيفية اختراق المهاجمين الهاكرز لأنظمة واستغلال الثغرات وأيضا معرفة الهدف من هذا الهجوم.

من الواجب على كل من مدير الأنظمة (**ADMIN**) ومحترفي الأمان في الشبكات (**network security prof.**) القيام بحماية البنية التحتية لأنظمتهم (**infrastructure**) من الثغرات وذلك بمعرفة العدو (الهاكرز) وما الذي يسعى إليه من استخدام أنظمتك (استغلالها في الأنشطة الغير قانونية والضارة) وهذا هو المغزى من المقوله السابقة من كتاب فن الحرب.

ما هو الهاكر؟

طلقت هذه الكلمة أول ما أطلق في السينما لتشير إلى المبرمجين المهرة القادرين على التعامل مع الكمبيوتر ومشاكله بخبرة ودرأية حيث أنهم كانوا يقومون حولاً لمشاكل البرمجة بشكل تطوعي في الغالب.

بالطبع لم يكن الوبندرز أو ما يعرف بالـ **GUI** أو **Graphical User Interface** قد ظهرت في ذلك الوقت ولكن البرمجة بلغة البسيك واللوغو والفور توران في ذلك الزمان كانت جديرة بالاهتمام. ومن هذا المبدأ غاليا العارفين بتلك اللغات والمقدمين العون للشركات والمؤسسات والبنوك يعرفون بالهاكرز وتعني الملمين بالبرمجة ومقدمي خدماتهم لآخرين في زمن كان عددهم لا يتجاوز بضع ألف على مستوى العالم أجمع. لذلك فإن هذا الوصف له مدلولات إيجابية ولا يجب خلطه خطأ مع الفئة الأخرى الذين يسطون عنده على البرامج ويكسرون رموزها بسبب امتلاكهم لمهارات فئة الهاكرز الشرفاء. ونظراً لما سببته الفئة الأخيرة من مشاكل وخسائر لا حصر لها فقد أطلق عليهم إسمًا مرادفاً للهاكرز ولكنه يتداول خطأ اليوم وهو **الكرياكرز Crackers** (كان الهاكرز في تلك الحقبة من الزمن يعتبرون عباقرة في البرمجة فالهاكر هو المبرمج الذي يقوم بتصميم أسرع البرامج والخالي في ذات الوقت من المشاكل والعيوب التي تعيق البرنامج عن القيام بدورة المطلوب منه. وأنهم كذلك فقد ظهر منهم إسمان نجحا في تصميم وإرساء قواعد أحد البرامج المستخدمة اليوم وهو دينيس ريتشي وكين تومسون اللذان نجحا في أواخر السينما في إخراج برنامج اليونيكس الشهير إلى حيز الوجود. لذلك فمن الأفضل عدم إطلاق لقب الهاكر على الأفراد الذين يدخلون عنده إلى الأنظمة بقصد التسلل أو التخريب بل علينا إطلاق لقب الكرياكرز عليهم وهي كلمة مأخوذة من الفعل **Crack** بالإنجليزية وتعني الكسر أو التحطيم وهي الصفة التي يتميزون بها).

ما هو الهاكر الأخلاقي؟ ETHICAL HACKING

هو عملية فحص واختبار الشبكة الخاصة بك من أجل إيجاد الثغرات و نقاط 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 الحق أي ضرر. وهذا من الطبيعي يؤدي إلى زيادة معدلات الأمان لدى النظام الخاص بك. أو بمعنى آخر 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 الهاكر الأخلاقي والهاكر العشوائي؟

- **الهاكر الأخلاقي (ethical hacker):** هو خريح هذه الشهادة أو ما يعادلها حيث يكتسب قوته من خلال خبرة أفضل هاكرز في العالم ويستخدمها في تحسين الوضع الأمني لأنظمة الشبكات المختلفة.
- **الهاكر العشوائي هو الهاكر المدمر.**

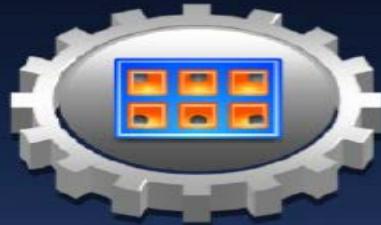
في هذا الفصل سوف نتحدث عن المواضيع التالية:



Information Security Overview



Information Security Threats and Attack Vectors



Hacking Concepts



Hacking Phases



Types of Attacks



Information Security Controls

1.2 رؤية مبسطة عن امن المعلومات (INFORMATION SECURITY OVERVIEW)

هذا المصطلح يشير إلى الطريقة المستخدمة لحماية أي نوع من المعلومات الحساسة أو بمعنى آخر وضع حائط أمن حول المعلومات المهمة وذلك لحمايتها من قبل الآتي:

- .1 **Unauthorized access** الوصول/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 أمنة، وذلك لأن وقوع هذه المعلومات في الأيدي الخطأ قد يسبب تهديداً كبيراً على البنية التي تخصها هذه المعلومات.

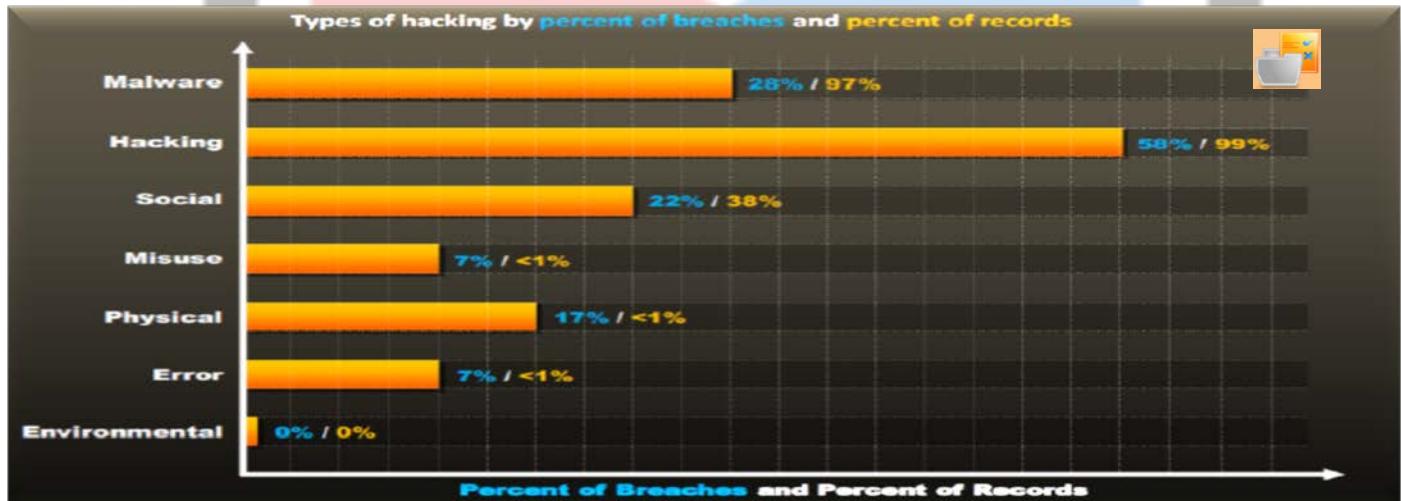
IC3

هو اختصار إلى **Internet Crime Complaint Center** وهي شركة تعمل على رصد الهمجات الإلكترونية ثم إعطاء تقرير عن هذا الموقع الإلكتروني لها هو www.ic3.gov



DATA BREACH INVESTIGATIONS REPORT (VERIZON BUSINESS)

شركة تعمل على رصد أنواع الهجمات وغيرها ثم تعطى تقرير عن هذا والموقع الإلكتروني الخاص بهم هو www.verizonbusiness.com



بعض المصطلحات المهمة:

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 هجوم من أي نوع على الأنظمة والشبكات ويمكن أن يكون أيضاً عباره عن تطبيقات أخرى أو أوامر (commands) والتي من الممكن أن تسبب سلوك غير متوقع لبرامجه قانونية أو أجهزه قانونية عن طريق اخذ ميزات نقاط الضعف التي تحتويها.

VULNERABILITY

هو مصطلح يعبر عن نقاط الضعف/الثغرات، وقد تكون نقاط الضعف هذه إما نقاط ضعف في التصميم (design code) أو أخطاء (error/bugs) والتي قد تسبب سلوك غير متوقع أو غير مرغوب فيه في نظام الأمان. وهو يعتبر المصدر الذي يهتم به الهاكر لكي يعمل عليه.

TARGET OF EVALUATION

هو نظام المعلومات أو الشبكات (IT system) أو برنامج أو محتوى يستخدم للوصول إلى درجة معينة من الأمان. 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 مسبقاً للمبرمجين في تطبيق كمبيوتر وهذا يعني أن المبرمجين لديهم صفر يوم لمعالجة هذا الضعف.

DAISY CHAINING

تعنى أن الهاكر الذي استطاع الوصول إلى قاعدة المعلومات فانه يعمل على تكملة أهدافه عن طريق تغطية أثار ما فعله ويتم ذلك بتدمير ملفات السجل (destroy log file) وذلك لإخفاء الهوية الخاصة به.

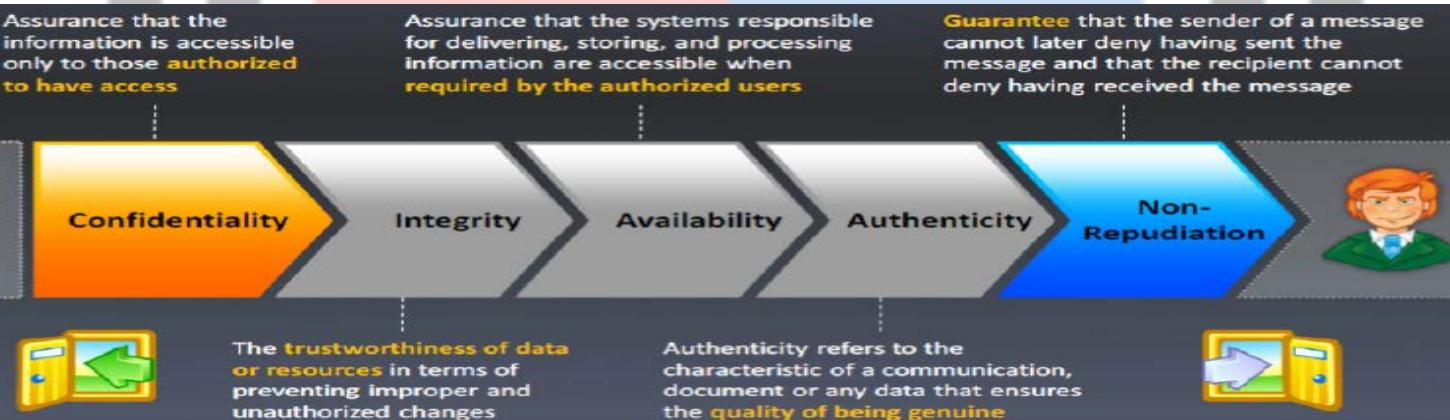


بعض المصطلحات التعريفية الأخرى:

- **Attack:** هو عباره عن أي هجوم على نظام امن.
- **Security:** عملية حماية البيانات من السرقة والعبث.
- **Threat:** الفعل أو الحدث الذى يمكن أن يضر بالأمن ، التهديد هو انتهاك محتمل للأمن.

عناصر امن المعلومات (ELEMENT OF INFORMATION SECURITY)

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



- **Confidentiality (الخصوصية):** هي الإجابة على السؤال (من له الحق في الأطلاع/الدخول على هذه المعلومات؟) أو بمعنى اصح هي صلاحيات الدخول.
- **Integrity (الكاملية):** شكل البيانات (منع أي تغير على البيانات).
- **Availability (الاتاحة):** البيانات تكون متاحة لمن له الحق في الدخول عليها أو بمعنى آخر أن النظام المسئول عن نقل وتخزين ومعالجة البيانات يكون متاحاً لمن له الحق في الدخول عليها.
- **Authenticity:** هذا يشير إلى سمة (الاتصالات، أو الوثيقة، أو أي بيانات) والتي تضمن نوعية كونها حقيقة أم لا (**genuine**) غير مقلدة من الأصل. والأدوار الرئيسية من عملية المصادقة **authentication** تشمل الآتي:
 1. التأكيد من هوية المستخدم هل هو هذا المستخدم المعرف لديه أم لا.
 2. ضمان أن الرسالة القادمة منه أصلية ولم يتم التغير في محتواها أو ليست مزورة.
 3. تستخدم كل من **smart cards** و **biometric** و الشهادة الرقمية **digital certificate** في التأكيد من مصداقية البيانات أو الاتصال أو حتى المستندات.

Non-repudiation

هذا يشير إلى القدرة على التأكيد من أن طرفي العقد أو الاتصالات لا يستطيعوا أن ينكروا صحة التوقيع على الوثيقة أو الرسالة المرسلة بينهم من الأمثلة على ذلك بروتوكول **Kerberos** و **HTTPS**.

مستوى الأمان في أي من الأنظمة أو الشبكات الموجودة تتحدد بقوة الثلاثة أشياء التالية:



حيث نلاحظ وجود دائرة صفراء والتي من الممكن أن تتحرك في أي زاوية من زوايا المثلث والتي تدل على معنى. حيث مكانها الحالي يدل انه مع زيادة الأمان (**security**) فإنه سوف يقل الأداء (**Usability – Functionality**)

INFORMATION SECURITY THREATS AND ATTACK VECTOR 1.3

إن هذا الجزء يقدم لك الآتي:

1. من أين تأتي الهجمات؟ **Attack Vector**
2. التهديدات الأمنية المحتملة. **Security Threat**
3. الهدف من وراء هذا الهجوم. **Goal of attack**

من أين يأتي هذا الهجوم؟ **ATTACK VECTOR**

هذا يشير إلى المسار الذي يتبعه المهاجم للوصول إلى مركز المعلومات على أنظمة الشبكة لأداء بعض الأنشطة المختلفة. **Attack Vector**: تتمكن المهاجم من الاستفادة من الثغرات الموجودة في نظام المعلومات لحمل الهجوم الخاص به. المسارات المتاحة التي من الممكن أن يستخدمها المهاجم في عملية القرصنة كالتالي:



الهدف من وراء هذا الهجوم. **GOAL OF ATTACK**

حيث نلاحظ من هذا أن أي هجوم **attack** يتكون من ثلاثة عناصر

$$\text{Attacks} \quad \Delta \quad \text{Attacks} = \text{Motive (Goal)} + \text{Method} + \text{Vulnerability}$$

(الهدف من الهجوم **Motive** + (الطريقة **method** + نقاط الضعف **Vulnerability**)

العنصر الأول هو **motive** وذلك لأن أي هجوم إما أن يكون لهدف أو لدافع معين (**motive , goal or objective**) مثل لهذه الأهداف تعطيل استمرارية العمل (**disrupting business continuity**), سرقة المعلومات، تنفيذ انتقام من مؤسسه معينه أو سرقة شيء ذات قيمة من مؤسسه ما. هذه الأهداف تختلف من شخص إلى آخر على حسب الحالة العقلية للمهاجم الذي حمله على القيام بهذا العمل. بمجرد امتلاك المهاجم للهدف فإنه يستخدم العديد من الطرق والأساليب لاستغلال نقاط الضعف (**exploit vulnerability**) في نظام المعلومات أو في **security policy** أو في **information system** في عملية الهجوم حتى يصل إلى تحقيق هدفه.

التهديدات الأمنية المحتملة SECURITY THREAT

التهديدات الأمنية المحتملة تنقسم هنا إلى ثلاثة أقسام كالتالي:



• التهديدات الطبيعية Natural Threats

التهديدات الطبيعية تشمل الكوارث الطبيعية مثل الزلازل **earthquake** او الفيضانات **floods** او الأعاصير **hurricanes** أو أي كارثة طبيعية أخرى التي لا يمكن ليفافها أو التحكم فيها. المعلومات التي يتم تدميرها أو فقدانها نتيجة التهديدات الطبيعية لا يمكن توقع وقت حدوثها واقصى ما يمكن فعله هو وضع بعض الخطط الأمنية التي تمكّن من عدم فقد هذه المعلومات مثل خطط الطوارئ واسترجاع البيانات عند الفقدان أو التدمير.

• التهديدات الفيزيائية Physical Threats

هذا النوع من التهديد ينتج نتيجة تلف أي جزء من الأجهزة المستخدمة سواء بواسطة الحريق أو الماء أو السرقة أو التدخلات الفيزيائية (hardware damage) وأيضاً مصادر الطاقة التي من الممكن أن تؤدي إلى تلف بعض الأجهزة (physical impact).

• التهديدات البشرية Human Threat

- هذا النوع من التهديدات ينتج نتيجة الهجمات سواء من داخل المنظمة (Insider) أو من الخارج (Outsider).
- **Insider Attack** (الهجمات من الداخل): تعتبر الأخطر والتي تتم بواسطة الموظفين من داخل المنظمة او من قبل شخص ساخط. وتعتبر الأخطر لأن المهاجم يعرف الكثير مثل الوضع الأمني (security posture) الخاص بانظمة المعلومات.
- **Outsider Attack** (الهجمات من الخارج): تتم بواسطة أشخاص آخرين من الخارج الذين يملكون بعض من الخبرة التي تمكّنهم من معرفة الوضع الأمني لنظام المعلومات.

هذا النوع من التهديد ينقسم هو الآخر إلى ثلاثة أنواع أخرى كالتالي:



:Network Threats .A

الشبكة Network هي عبارة عن ربط جهازين حاسوب فأكثر (مجموعة من الأجهزة) مع بعضهما البعض من خلال قنوات اتصال وذلك لتبادل البيانات والموارد **communication channel** مثل (الطابعات، الملفات ... وغيرها). ومع مرور هذه البيانات من خلال قنوات الاتصال **communication channel** فإنه من الممكن دخول شخص ما عنوةً إلى هذه القنوات وسرقة ما بها من معلومات.

لذلك فإن المهاجم الهاكر يعرض العديد من التهديدات من خلال الشبكة ومن هذه التهديدات كالتالي:

Information gathering	.1
sniffing and eavesdropping	.2
(التنصت والتتجسس)	
(spoofing)	.3
session hijacking and man-in-middle attack	.4
sql injection	.5
ARP Poisoning	.6
Denial of service attack	.7
comprised key attack	.8

:Host Threats .B

هذا النوع من التهديد يتم توجيهه إلى النظام الحالي الذي يحمل المعلومات القيمة التي يريد المهاجم مباشرة (عن طريق الاتصال المباشر). حيث يحاول المهاجم من كسر الوضع الأمني للنظام الذي يحمل هذه المعلومات ومن هذه التهديدات كالتالي:

Malware attacks	.1
Target Footprinting	.2
Password attacks	.3
Denial of service attacks	.4
Arbitrary code execution	.5
Unauthorized access	.6
Privilege escalation	.7
Back door attacks	.8
Physical security threats	.9

:Application Threats.C

تطوير أي تطبيق أو إنشائه مع عدم الاهتمام بالأوضاع الأمنية الخاصة به. قد يؤدي إلى وجود بعض الثغرات الأمنية في هذا التطبيق وقد ينتج عن هذه الثغرات ثغرات أخرى في تطبيقات أخرى. حيث أن المهاجم يستفيد من هذه الثغرات في تنفيذ هجماته لسرقة المعلومات أو تدميرها ومن هذه التهديدات كالتالي:

Data/Input validation	.1
Authentication and Authorization attacks	.2
Configuration management	.3
Information disclosure	.4
Session management issues	.5
Cryptography attacks	.6
Parameter manipulation	.7
Improper error handling and exception management	.8
Auditing and logging issues	.9

INFORMATION WARFARE (حرب المعلومات)

المصطلح (Information Warfare/InfoWar) يشير إلى استخدام تكنولوجيا المعلومات والاتصالات **ICT** في الحصول على بعض المزايا التنافسية من الشركات المنافسة أو بمعنى آخر هو سرقة المعلومات من الشركات المنافسة.

أو بمعنى آخر هو اصطلاح ظهر في بيئه الإنترن特 للتعبير عن اعتداءات تعطيل الواقع وإنكار الخدمة والاستيلاء على المعلومات، وكما يشير الاصطلاح فإن الهجمات والهجمات المقابلة هي التي تدل على وجود حرب حقيقة، وبما إنها حرب فهي حرب بين جهات تتناقض مصالحها وتتعارض مواقفها، لهذا تكون في الغالب هجمات ذات بعد سياسي، أو هجمات منافسين في قطاع الأعمال. ولذا وصفت حملات الهاكرز اليوغسلافيين على موقع الناتو أبان ضربات الناتو بانها حرب معلومات ، ووصفت كذلك هجمات المخترقين الأمريكيان على موقع صينية في إطار حملة أمريكية على الصين تحت ذريعة حقوق الإنسان والتي تمت بدعم حكومي أمريكي بانها حرب معلومات ، وأشهر

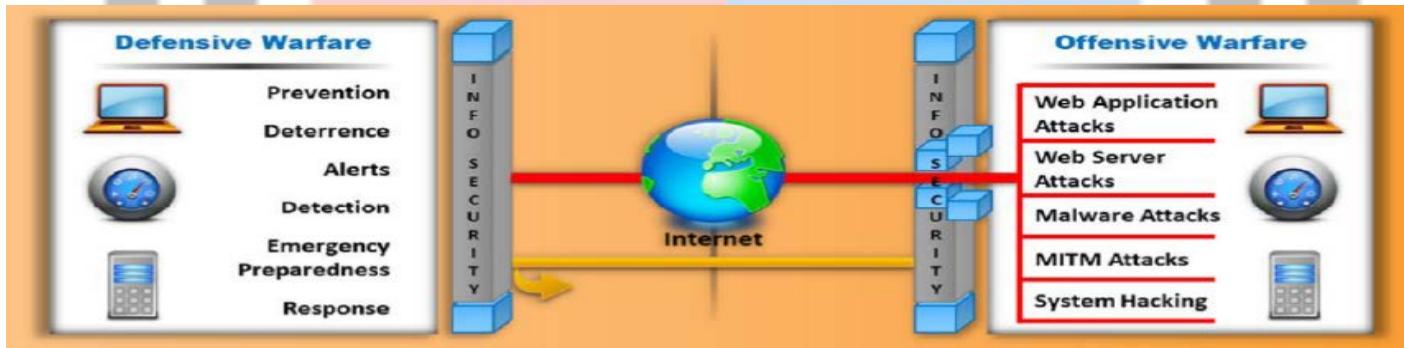
حروب المعلومات القائمة حتى الأن المعركة المستمرة بين الشباب العرب والمسلم وتحديا شباب المقاومة اللبنانية والمدعومين من خبراء اختراق عرب ومسلمين ، وبين جهات تقنية صهيونية في اطار حرب تستهدف إثبات المقدرات في اختراق الموقع وتعطيلها أو الاستيلاء على بيانات من هذه المواقع . وهذا الاصطلاح في حقيقته اصطلاح إعلامي أكثر منه أكاديمي، ويستخدم مرادفا في غالبية القارier لاصطلاح الهجمات الإلكترونية ونجد له لدى الكثرين اصطلاح واسع الدلالة لشمول كل أنماط مخاطر وتهديدات واعتداءات وجرائم البيئة الإلكترونية، ونرى قصر استخدامه على الهجمات والهجمات المضادة في ضوء حروب الرأي والمعتقد لتمييزه عن بقية أنشطة تعطيل المواقع التي لا تنطبق من مثل هذه الأغراض.

Defensive InfoWar

يشير إلى جميع الاستراتيجيات والمبادرات التي تستخدم الدفاع ضد هذا النوع من الهجمات (ICT assets).

Offensive InfoWar

يشير إلى InfoWar التي تستخدم للهجوم على المؤسسات (ICT assets) في الشركات المنافسة.



IPV6 (التهديدات الأمنية من استخدام IPV6 SECURITY THREATS)

مقارنة بـ IPv4 فإنه يملك تحسينات أمنية أفضل منه والتي تصل بك إلى مستوى أعلى من الأمان والخصوصية للمعلومات التي تمر عبر الشبكة ولكن مع ذلك فإنه يحمل بعض التهديدات كالتالي:

Auto-Configuration threat-1

IPv6 يدعم الإعداد الآلي (Authconfig) لعناوين الشبكة (IP)، والتي تترك المستخدم عرضه للهجوم عبر بعض الثغرات إذا لم يتم الإعداد الصحيح والأمن من البداية.

Unavailability Reputation-based Protection-2

بعض الحلول الأمنية الحالية تعتمد على استخدام reputation of IP address (عناوين IP مشهوره أو معروفة) في تصفية بعض المصادر المعروفة لا malware. والتي تحتاج إلى وقت حتى يتم تطويرها لكي تشمل عناوين IPv6.

Incompatibility of Logging Systems-3

IPv6 يستخدم عناوين ذات حجم bit 128 والتي يتم تخزينها على هيئة 39 حرفاً ورقم، ولكن IPv4 يستخدم عناوين ذات أحجام 32 bit وتختزن على هيئة 15 رمزاً. لذلك فإن عمليات التسجيل logging solutions في الأنظمة المعتمدة على IPv4 من الممكن إنها لن تعمل مع الشبكات القائمة على IPv6.

Rate Limiting Problem-4

يستخدم مدير الأنظمة Admin استراتيجيات الحد (rate limiting strategy) لإبطاء أدوات المهاجم ألياً (Automated attack tool) لكن هذا سوف يكون صعباً عند استخدامه مع عناوين ذات أحجام bit 128.

التهديدات التي تتمكن نتيجة استخدام IPV6

Default IPv6 Activation-1

من الممكن أن يفعل ألياً بدون علم مدير النظام ADMIN، والتي يؤدي إلى عدم فاعلية الأوضاع الأمنية القائمة على IPv4.

Complexity of Network Management Tasks-2

مدير النظام admin دائماً ما يختاروا عناوين IPv6 سهلة الحفظ مثل (::FOOD, ::C5C0, ::20, ::10) وغيرها والتي من السهل توقعها بالنسبة للمهاجم.



Complexity in Vulnerability Assessment-3

IPv6 ذات أحجام 128 bit يجعل فحص بنية الأنظمة (**infrastructure**) من أجل كشف المتسللين والثغرات عملية معقدة.

Overloading of Perimeter Security Controls-4

IPv6 يحمل عنوان ثابت في **header** ذات حجم **add-on** مع 40 byte قد تكون مقيدة والتي تحتاجها في بعض العمليات المعقدة بواسطة بعض أدوات التحكم الأمن (security control) للشبكة مثل routers , security gateways و firewalls .

IPv4 to IPv6 Translation Issues-5

ترجمة الحزم من **IPv4** إلى **IPv6** من الممكن أن يؤدى تدمير الحزم أو ينتج عن سوء تنفيذ هذه الترجمة (poor implementation).

Security Information and Event Management (SIEM) Problems-6

كل عميل يستخدم **IPv6** يحمل عناوين عده من **IPv6** وليس عنوان واحد مما يؤدى إلى التعقيد في ملفات **log** والأحداث **event**.

Denial-of-service (DOS)-7

زيادة التحميل على امن الشبكة وأجهزة التحكم يؤدى إلى تقليل إتاحة موارد الشبكة، والتي تؤدى إلى الهجمات من النوع **DOS**.

Trespassing-8

الميزات المستقبلية لعناوين **IPv6** التي يتم استكشافها من الممكن أن تستغل من قبل المهاجمين في احتياز الشبكة الخاصة بك من أجل الوصول إلى موارد الشبكة المقيدة (restricted resources).

HACK CONCEPT 1.4 (مفهوم الهاكنج)

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



التهكير المدمر hacking

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



التهكير الأخلاقي Ethical hacking

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

• ما هو تأثير الهاكر المدمر؟

1. تلف وسرقة المعلومات.

2. استخدام أجهزة كمبيوتر في التهكير على آخر.

3. استخدام back door

4. سرقة البريد الإلكتروني من أجل الأرقام السرية.

5. سرقة وتدمير الأجهزة.

• تأثير الهاكر المدمر على الأعمال:



من هو الهاكرز؟

هو عباره عن شخص محترف يمكنه اختراق الأنظمة والشبكات بطريقه غير قانونيه أو بدون تصريح من أجل تدمير أو سرقة المعلومات الحساسة أو أداء بعض الهجمات الأخرى على الأجهزة الأخرى. وهذا الشخص يتميز بأنه يملك ذكاء مع مهارات جيده في علم الكمبيوتر مع المقدرة على إنشاء وفحص برامج وأجهزة الكمبيوتر.

بعض المهاجمين لديهم هواية في رؤية كم العدد من الأجهزة والشبكات الذي اختراقها. البعض الآخر يستخدم هذا لkses المعلومات أو لفعل شيء غير قانوني مثل سرقة معلومات الاستثمارية أو معلومات كارت الائتمان (ATIM) أو الرقم السري للبريد الإلكتروني وغيرها.

أنواع الهاكرز:

Black Hats (المخترق ذو القبعة السوداء)



هم أفراد لديهم مهارات استثنائية في علم الحوسبة (computer science)، اللجوء إلى أنشطة ضارة أو مدمرة، كما أنهم معروفين أيضاً باسم **كراكرز (crackers)**.

هؤلاء الأفراد دائم ما يستخدمون مهاراتهم في الأنشطة التدميرية والتي تسبب ضرر كبير للشركات والمؤسسات والأفراد. هؤلاء يستخدمون مهاراتهم في إيجاد الثغرات في الشبكات المختلفة والتي تشمل أيضاً المواقع الحكومية ومواقع الدفاع والبنوك وهكذا. بعضهم يفعل ذلك من أجل أحداث ضرر أو سرقة معلومات أو تدمير بيانات أو كسب المال بطريقه سهل عن طريق فرصله الرقم التعريقي لعملاء البنوك.

White Hats (المخترق ذو القبعة البيضاء)



هم أفراد يعتقدون بمهارات القرصنة (الاختراق) ويستخدمون هذه المهارات من أجل الأهداف الدفاعية، كما أنهم معروفين أيضاً باسم **المحللين الآمنين (security analysts)**. في هذه الأيام فإن معظم الشركات يملكون محللين آمنين من أجل حماية أنظمتهم ضد الهجمات المختلفة. هؤلاء يساعدون الشركات لتامين الشبكات الخاصة بهم.

Gray Hats (المخترق ذو القبعة الرمادية)



هم أفراد لديهم مهارات الهاكر يستخدمونها في الهجوم والدفاع على حد سواء في أوقات مختلفة. هؤلاء يقعون بين **White Hats** و **Black Hats**. هؤلاء يمكنهم أيضاً 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 أماناً وهكذا.

Suicide Hackers (الهاكر المنتحرون)



ويطلق عليه أيضاً الهاكر المنتحر لأنه يشبه إلى حد كبير الشخص الذي يقوم بتغيير نفسه غير مهم بحياته من أجل هدف ما. وهو عباره عن أفراد يهددون إلى إسقاط البنية التحتية الحيوية بسبب ما سبب لا يقلون بشأن 30 عاماً في السجن نتيجةً لأفعالهم ولا يخفون أنفسهم بعد القيام بالهجوم أي بمعنى آخر يسرقون علانيتاً. وقد انتشر هذا النوع في السنوات الأخيرة.

Script Kiddies



هو هاكر ليس لديه مهارات الهاكر ولكن يتحايل على الأنظمة باستخدام بعض الاسكريبات والأدوات والتطبيقات التي تم تطويرها بواسطة الهاكرز الحقيقيين. هؤلاء من السهل لهم استخدام التطبيقات والاسكريبات 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 أفراد يتم تأجيرهم من قبل المنظمات المختلفة لاختراق والحصول على أسرار من المنظمات المنافسة لهم.

Cyber Terrorists (إرهاب العالم الإلكتروني)



هي هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية. وتعتبر جرائم إتلاف للنظم والمعطيات أو جرائم تعطيل للموقع وعمل الأنظمة. وهي ممارسات لذات مفهوم الأفعال الإرهابية لكن في بيئه الكمبيوتر والإنترنت وعبر الإفادة من خبرات الكراكرز وهذا النوع من الهاكر يعتبر الأكثر خطورة لأنه لن يخترق الواقع الإلكتروني فحسب بل من الممكن منطقه بأكملها.

State Sponsored Hackers



هم عباره عن أفراد يتم تأجيرهم بواسطة الحكومات من أجل الاختراق والحصول على معلومات على درجه عالية من السرية وتدمير بعض أنظمة المعلومات الأخرى للحكومات الأخرى.

THE CHOICE IS YOURS



:HACKTIVISM

هو عمل لتعزيز أجندات سياسية عن طريق القرصنة، خاصة عن طريق تشويه أو تعطيل بعض الواقع. والشخص الذي يقوم بهذه الأشياء يسمى **hacktivist**. أو بمعنى آخر (هذا يشير إلى فكرة القرصنة لأسباب) هؤلاء الأشخاص يزدھرون في البيئة حيث توجد المعلومات التي يمكن الوصول إليها بسهولة. وهذا يهدف إلى إرسال رسالة من خلال أنشطة القرصنة واكتساب الرؤية من أجل قضية معينة. ومعظم الأهداف إما أن تكون الوكالات الحكومية، والشركات متعددة الجنسيات، أو أي كيان آخر ينظر إليها على أنها كيان سيء (**bad or wrong**) من وجهة نظر هؤلاء الأشخاص. ولكن يبقى الواقع، أن اكتساب الوصول الغير مصرح به هو جريمة، مهما كان القصد من ذلك. أو بمعنى آخر هم يقومون بعملية القرصنة بسبب معين قد يكوندافع الانتقام، أو أسباب سياسية أو اجتماعية أو إيديولوجية، أو للتخييب، والاحتجاج والرغبة في إذلال الضحايا.

(مراحل القرصنة) HACK PHASE 1.5

هذا يشمل الآتي:

Reconnaissance-1	عملية جمع المعلومات (الاستطلاع)
Scanning-2	فحص
Gaining Access-3	الدخول إلى الهدف
Maintaining Access-4	يحافظ على الدخول
Clearing Tracks-5	ينظف أي إشارة له

• Reconnaissance •

يطلق عليها أيضا **preparatory phase** أي المرحلة التحضيرية والتي فيها يقوم المهاجم بجمع أكبر قدر ممكن من المعلومات عن الهدف لتقييمه قبل تنفيذ هجنته. 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 عن طريقها يضع المهاجم استراتيجيات الهجوم والتي من الممكن أن تأخذ بعض الوقت حتى يحصل على المعلومات المهمة.

جزء من هذه المرحلة يشمل **الهندسة الاجتماعية** (**social engineering**). الهندسة الاجتماعية أو ما يعرف بفن اختراق العقول هي عباره عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفصحون عن معلومات سريه. وتستخدم في عمليات القرصنة في المرحلة الأولى (مرحلة جمع المعلومات) حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة بسيطة أو تافهة (عن طريق الهاتف أو البريد الإلكتروني مع انتقال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هذه الأسئلة دون إثارة الشبهات).

بعض تقنيات الفحص الأخرى هي **Dumpster diving** (الغوص في سلة المهملات) وهي عباره عن عملية النظر في سلة مهملات بعض المنظمات من أجل الوصول إلى بعض المعلومات الحساسة المستبعدة.

المهاجم أيضا يمكنه استخدام شبكة المعلومات الأنترنت للحصول على بعض المعلومات مثل معلومات الاتصال والشركاء في العمل والتكنولوجيا المستخدمة وبعض المعلومات الحساسة الأخرى ولكن **dumpster diving** تدعوك بمعلومات أكثر حساسية مثل اسم المستخدم والرقم السري وأرقام кредит كارد والحالة المالية ورقم الائتمان الاجتماعي وغيرها من المعلومات الحساسة.

وينقسم Reconnaissance (الاستطلاع) إلى:

- Passive Reconnaissance**: التعامل مع الهدف ولكن بطريقه غير مباشره للحصول على معلومات؛ مثل سجلات البحث العامة ونشرات الأخبار و الهندسة 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/راوتر وهكذا.

Scanning •

المسح هو ما يفعله المهاجم قبل تنفيذ الهجوم. ويشير المسح إلى فحص الشبكة للحصول على أساس المعلومات التي تم جمعها من خلال عملية الاستطلاع (**Reconnaissance**)، يستخدم القراءة المسح للحصول على نقطة دخول (الثغرة) للبدء في الهجوم، وتتضمن عملية المسح مسح المنافذ، خرائط الشبكة الضعف الأمني، وما إلى ذلك.

المهاجم دائماً ما يستخدم الأدوات الجاهزة مثل **war dialers** و **network/host scanner** لإيجاد النظام واكتشاف الثغرات الذي يحتويها.

Gaining Access •

هذه المرحلة تعتبر اهم مرحلة ويطلق عليها أيضاً **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 أو على مستوى التطبيقات، ومن الأمثلة على ذلك: **password cracking**, **session hijacking**, **denial of service**, **buffer overflows**.

Maintaining Access •

وتشير إلى المرحلة التي يحاول فيها المخترق حفظ ملكية الدخول مجدداً إلى النظام، من خلال وصول حصري باستخدام **Backdoors**، مما يسمح للمخترق بتحميل ورفع الملفات، والتعامل مع البيانات والتطبيقات على النظام المخترق، أو **Trojans**، أو **Rootkits**.

Clearing Tracks •

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**.

(أنواع الهجمات) TYPE OF ATTACKS 1.6

هناك العديد من الطرق التي تمكن المهاجم من الدخول إلى النظام. ويجب أن يكون الهاكر قادراً على اكتشاف نقاط الضعف والثغرات في النظام حتى يتمكن من الدخول. ومن هذه الطرق كالتالي:

Types of Attacks

I Operating System Attacks

III Application Level Attacks

II Misconfiguration Attacks

IV Shrink Wrap Code Attacks

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

Application-level attacks-2: 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. يؤدي إلى أن هذه التطبيقات يكون لديها بعض من نقاط الضعف المختلفة والتي قد تصبح مصدراً للهجوم من قبل الهاكر.

Misconfiguration attacks-3: معظم مدير الأنظمة (**Admin**) لا يملكون المهارات الضرورية من أجل صيانة أو إصلاح بعض المسائل/القضايا، والتي من الممكن أن تؤدي إلى أخطاء في عمليات الإعداد. بعض هذه الأخطاء من الممكن أن تكون مصدراً للمهاجم للدخول إلى الشبكة هو النظام الذي يستهدفه.

Shrink wrap code attacks-4: تطبيقات أنظمة التشغيل تأتي بالعديد من ملفات الاسكريبت المبسطة لكي تسهل العمل على مدير الأنظمة (**Admin**)، ولكن مثل هذه الاسكريبتات تحتوي أيضاً على العديد من الثغرات والتي من الممكن أن تؤدي إلى هذا النوع من الهجوم.

OPERATING SYSTEM ATTACKS-1

أنظمة التشغيل، والتي يتم تحميلها اليوم مع الكثير من المميزات، أصبحت تزداد تعقيداً. ومع الاستفادة من الكثير من هذه المميزات التي توفرها هذه الأنظمة من قبل المستخدمين، تجعل النظام عرضة لمزيد من نقاط الضعف، وبالتالي عرضه للقرصنة. 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 التغيير 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 المختلفة والمتبعة من قبل المهاجمين ومراقبة الشبكة بشكل مستمر. تطبيق التصحيحات والإصلاحات ليست سهلة في الوقت الحاضر لأنها شبكة معقدة.

معظم مستخدمي أنظمة التشغيل يقومون بتنبيث العديد من التطبيقات والتي تقوم بعضها بفتح بعض المنافذ **ports** افتراضياً. والتي تسهل على المهاجمين من اكتشاف العديد من الثغرات. تنبيث البالشات **patches** وملفت الإصلاح **fix-file** لم يعد سهلاً مع تعقيدات الشبكة الموجودة في هذه الأيام. وأيضاً معظم البالشات تعمل على حل المشاكل والثغرات الحالية ولكن لا يمكن اعتباره الحل الدائم.

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

APPLICATION-LEVEL ATTACKS-2

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. المهاكر يعمل على اكتشاف هذه الثغرات الموجودة في التطبيقات باستخدام العديد من الأدوات والتقنيات.

التطبيقات لما بها من ثغرات تصبح عرض للهجمات من قبل المهاكر نتيجة الأسباب الآتية:

1. لمطوري البرامج الجداول الزمنية الضيقة لتسليم المنتجات في الوقت المحدد (**tight schedules to deliver**) والذي يؤدي إلى ظهور التطبيقات في سوق العمل بدون الاختبارات الكافية عليه.
2. تطبيقات البرامج تتأثر مع العديد من الوظائف والمزايا.
3. ليس هناك ما يكفي من الوقت لأداء اختبار كامل قبل الإفراج عن المنتجات (**dearth of time**).
4. الأمان في كثير من الأحيان تكون مرحلة لاحقة، ويتم تسليمها فيما بعد باعتبارها عناصر إضافية (**add-on component**).

ضعف أو عدم وجود خطأ التدقيق (**poor or nonexistent error checking**) في التطبيقات أمر يؤدي إلى الآتي:

Buffer overflow attacks	.1
Active content	.2
Cross-site scripting	.3
Denial-of service and SYN attacks	.4
SQL injection attacks	.5
Malicious bots	.6

بعض الهجمات الأخرى التي تكون على مستوى التطبيقات كالتالي:

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

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

```

TABLE 1.4: Denial-of-Service Secure Code

MISCONFIGURATION ATTACKS-3

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/أنواع الملف، فيؤدي إلى جعله غير آمن.

SHRINK WRAP CODE ATTACKS-4

عند تثبيت نظام التشغيل أو التطبيقات فإنه يأتي مع العديد من الاسكريبات والتي تسهل على **Admin** التعامل معها. ولكن المشكلة هنا " ليست ضبط " أو تخصيص هذه الاسكريبات التي من الممكن أن تؤدي إلى الرموز الافتراضية أو هجوم **.shrink-wrap code**



```

01522 Private Function CleanUpLine(ByName sLine As String) As String
01523     Dim lQuoteCount As Long
01524     Dim lCount As Long
01525     Dim sChar As String
01526     Dim sPrevChar As String
01527
01528     ' Starts with Rem it is a comment
01529     sLine = Trim(sLine)
01530     If Left(sLine, 3) = "Rem" Then
01531         CleanUpLine = ""
01532         Exit Function
01533     End If
01534
01535     ' Starts with ' it is a comment
01536     If Left(sLine, 1) = "'" Then
01537         CleanUpLine = ""
01538         Exit Function
01539     End If
01540
01541     ' Contains ' may end in a comment, so test if it is a comment or in the
01542     ' body of a string
01543     If Instr(sLine, "'") > 0 Then
01544         sPrevChar = ""
01545         lQuoteCount = 0
01546
01547     For lCount = 1 To Len(sLine)
01548         sChar = Mid(sLine, lCount, 1)
01549
01550         ' If we found " " then an even number of " characters in front
01551         ' means it is the start of a comment, and odd number means it is
01552         ' part of a string
01553         If sChar = " " And sPrevChar = " " Then
01554             If lQuoteCount Mod 2 = 0 Then
01555                 sLine = Trim(Left(sLine, lCount - 1))
01556             Exit For
01557         End If
01558         ElseIf sChar = "'" Then
01559             lQuoteCount = lQuoteCount + 1
01560         End If
01561         sPrevChar = sChar
01562
01563     Next lCount
01564
01565     CleanUpLine = sLine
01566 End Function

```

إذا كان المتسلل هو أو هي يريد الدخول على النظام الخاص بك فانت لن تستطيع أن تفعل شيء أمام هذا ولكن الشيء الوحيد الذي يمكنك القيام به هو جعل الأمر أكثر صعوبة عليه للحصول على نظامك.

INFORMATION SECURITY CONTROL 1.7 (التحكم في امن المعلومات)

- لماذا الهاكر الأخلاقي ضروري ومهم؟

هناك نمو سريع في مجال التكنولوجيا، لذلك هناك نمو في المخاطر المرتبطة بالเทคโนโลยيا، والفرصنة الأخلاقية يساعد على الت碧ؤ بمختلف نقاط الضعف المحتملة في وقت مبكر وتصحيحها دون تكبدي أي نوع من الهجمات القادمة من الخارج.

الفرصنة الأخلاقية (ethical hacking) : مثل الفرصنة يشمل التفكير الإبداعي، واختبار مواطن الضعف والتدقق الأممي 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 الفراصنة الخبيثة بطريقة التوقع (anticipating methods) والتي يمكن استخدامها لاقتحام نظام.

- المخترق الأخلاقي يحاول أن يجاوب على الأسئلة التالية:

- ماذا يمكن أن يرى الدخيل على نظام الهدف؟

مراحل الاستطلاع والمسح (reconnaissance and scanning)

- ما الذي يمكن أن يقوم به المتسلل بهذه المعلومات؟

مراحل الوصول والمحافظة على الوصول (Gaining Access and Maintaining Access)

- هل يوجد دخيل على النظام؟

مراحل الاستطلاع وتغطية الأثر (reconnaissance and covering tracks)

- هل جميع أجزاء نظام المعلومات يتم حمياته وتحديثه وتمكين الباشات باستمرار؟

- هل مقاييس امن المعلومات مماثلة لمعايير الصناعة والقانون؟

• لماذا تقوم المؤسسات بتعيين المخترقين الأخلاقين؟

1. لمنع القرصنة من الدخول إلى قسم المعلومات.
2. لمكافحة الإرهاب ومخالفات الأمن القومي.
3. لبناء نظام يكون قادر على تفادي هجمات القرصنة.
4. لاختبار الوضع الأمني للمؤسسات والمنظمات.

نطاق وحدود القرصنة الأخلاقية (SCOPE AND LIMITATIONS OF THE ETHICAL HACKERS)

SCOPE

ما يلي نطاق القرصنة الأخلاقية:

- القرصنة الأخلاقية هو عنصر حاسم لتقدير المخاطر، ومراجعة الحسابات، ومكافحة الاحتيال، وأفضل الممارسات، والحكم الجيد.
- يتم استخدامه لتحديد المخاطر وتسلیط الضوء على الإجراءات العلاجية، والحد من تكاليف تكنولوجيا المعلومات والاتصالات (ICT) عن طريق إيجاد حل لتلك التغرات.

LIMITATIONS

ما يلي حدود القرصنة الأخلاقية:

- ما لم تعرف الشركات أولاً ما الذي يبحثون عنه، ولماذا يتعاقدون مع مورد خارجي لاختراق الأنظمة في المقام الأول؛ وهناك احتمالات بأن لن يكون هناك الكثير لكتسيه من خبرة.
- لذا القرصنة الأخلاقية الوحيدة الذين يمكنهم أن يساعدوا المنظمات لفهم أفضل لأوضاعهم الأمنية، ولكن الأمر متترك للمنظمة لوضع الضمانات الأمنية على الشبكة.

مهارات الهاكر الأخلاقي :ETHICAL HACKER SKILLS

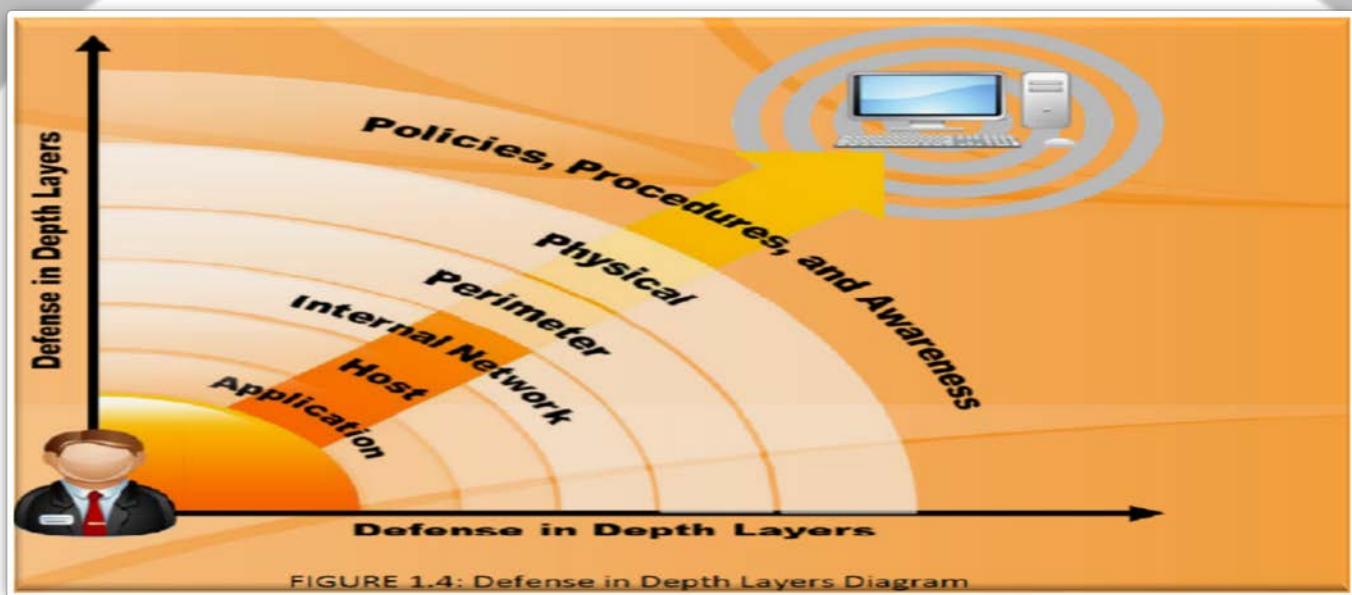
القرصنة الأخلاقية هي عملية قانونية يتم تنفيذها بواسطة **pen tester** لإيجاد نقاط الضعف في بيئه تكنولوجيا المعلومات. ولكي يتم هذا يجب أن يتمتع الهاكر الأخلاقي ببعض المهارات كالتالي:

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. لديه معرفة مثالية لإقامة الشبكات والأجهزة ذات الصلة والبرمجيات.
5. لديه معرفة مثالية في الأجهزة والتطبيقات التي قدمت عن طريق بائع الكمبيوتر وأجهزة الشبكات ذات شعبية.
6. ليس من الضروري أن يحمل معرفة 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.

(الدفاع من العمق) DEFENSE-IN-DEPTH

يتم اتخاذ العديد من التدابير المضادة للدفاع من العمق (**Defense-in-Depth**) لحماية أصول المعلومات في الشركة. وتستند 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 (**Defense-in-Depth**) يقلل التأثير السلبي ويعطي الإداريين والمهندسين الوقت لنشر مضادات جديدة أو محدثة لمنع تكرار هذا الاختراق مرة أخرى.

- الدفاع من العمق (**Defense-in-Depth**) هي استراتيجية الأمان 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.



INCIDENT MANAGEMENT PROCESS (عملية الإدارة الطارئة)

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

الغرض من عملية إدارة الحوادث كالتالي:

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



يتم التعامل مع أي حادث وقع في مؤسسة ما وحلها باتباع الخطوات التالية من قبل إدارة الحوادث



INFORMATION SECURITY POLICIES سياسات أمن المعلومات

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، وتشمل الوثيقة 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، فضلاً 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 تُعرف الاستخدام المقبول أو المرضى لجميع الوسائل الإلكترونية في المنظمة.

سياسات الأمان 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 معًا لتأمين اتصالاتهم، وكذلك التقليل من مخاطر ضعف الأمان من خلال عامل الأخطاء البشرية مثل الكشف عن معلومات حساسة إلى مصادر غير مصرح بها أو غير معروفة، الاستخدام الغير لائق للإنترنت، وما إلى ذلك. بالإضافة إلى ذلك، توفر هذه السياسات الحماية ضد الخدمات الإلكترونية والتهديدات الخبيثة، والاختبارات الأجنبية، وهلم جرا. أنها تتناول أساساً الأمان المادي، وأمن الشبكات، وأمن الدخول، الحماية من الفيروسات، والتعافي من الكوارث.

أهداف السياسات الأمنية : (SECURITY POLICIES)

- الحفاظ على الخطوط العريضة لتنظيم وإدارة أمن الشبكات.
- حماية موارد الحوسبة للمنظمة.
- القضاء على المسئولية القانونية من الموظفين أو أي طرف ثالث.
- ضمان سلامة العملاء ومنع إهانة موارد الحوسبة الخاصة بالشركة.
- منع التعديلات الغير المصرح به على البيانات.
- الحد من المخاطر الناجمة عن الاستخدام الغير مشروع لموارد النظام وفقدان البيانات السرية والحساسة والممتلكات المحتملة.
- التفريق في حقوق الوصول بالنسبة للمستخدم.
- حماية سرية المعلومات الشخصية من السرقة أو سوء الاستخدام، أو الكشف الغير المصرح به.

(تصنيف السياسة الأمنية) CLASSIFICATION OF SECURITY POLICY

إن استراتيجية أمن المعلومات، أو سياسة أمن المعلومات هي مجموعة من القواعد التي يطبقها الأشخاص عند التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها. لإدارة أمنية فعالة، فإن السياسات الأمنية يتم تصنيفها إلى خمسة مجالات مختلفة كالتالي:

• (السياسات الأمنية للمستخدم) User Policy

هي تتعلق بالموظفين العاملين على النظام التقني. المعنى من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمان إلى جانب الوعي بمسائل الأمان ومخاطر الاعتداء على المعلومات. مثال على ذلك: **password management policy**.

• IT Policy

هذا الجزء مصمم لقسم تكنولوجيا المعلومات للحفاظ على الشبكة آمنة ومستقرة. مثال على ذلك: **modification policy, patch updates, server configuration, backup policies**.

• General policies

تحديد المسئولية للأغراض التجارية العامة. مثال على ذلك: **crisis management, business continuity plans, high-level program policy**.

• Partner policy

السياسة التي يتم تعريفها ضمن مجموعة من الشركاء.

• Issue-specific policies

يتم تعريف مجالات محددة للقلق ووصف وضع المنظمة من أجل الإدارة على مستوى عالي.



- مثال على ذلك: personnel security policy ‘Physical security policy’

هيكل ومحفوظة السياسات الأمنية STRUCTURE AND CONTENTS OF SECURITY POLICIES

هيكل السياسات الأمنية (STRUCTURE OF SECURITY POLICY)

سياسة الأمان هو المستند الذي يوفر الوسيلة لتأمين الأجزاء المادية للشركة، الخاصة بالموظفين والبيانات من التهديدات أو الاختراقات الأمنية. ينبغي تنظيم السياسات الأمنية بعناية فائقة وينبغي إعادة النظر بشكل صحيح للتأكد من أنه لا توجد صيغة يمكن لشخص ما الاستفادة منها. وينبغي أن يتضمن الهيكل الأساسي للسياسات الأمنية العناصر التالية:

- وصف تفصيلي لقضايا السياسات الأمنية.
- وصف حالة السياسة الأمنية.
- تطبيق السياسة الأمنية.
- تحديد وظائف المتضررين من السياسة.
- عواقب محددة من شأنها أن تحدث إذا كانت السياسة غير متوافقة مع المعايير التنظيمية.

محفوظة السياسات الأمنية (CONTENTS OF SECURITY POLICY)

- المتطلبات لوضع مستوى عالي من سياسات الأمان **high-level security requirements** : هذا يوضح متطلبات النظام لوضع سياسات الأمنية التي سيتم تطبيقها. وهذا يشمل أربعة متطلبات كالتالي:
 - المتطلبات لأنضباط الأمان **Discipline security requirements** : هذه المتطلبات تشمل السياسات الأمنية المختلفة مثل أمن الاتصالات، وأمن الحاسوب، وأمن العملية، الانتلاق الأمن، وأمن الشبكات، وأمن الأفراد، وأمن المعلومات والأمن المادي.
 - المتطلبات للحفاظ على الأمان **safeguard security requirement** : هذه المتطلبات تحتوي أساسياً على التحكم في الوصول، الأرشيف، والتدقيق **audit**، المصداقية **authenticity** ، التوافر، السرية، التشفير، التحديد والتوثيق، التزاهة **integrity** ، الواجهات، وضع العلامات، عدم الأنكار **non-repudiation** ، إعادة استخدام كائن **object reuse** ، الاسترجاع **recovery** ، والحماية من الفيروسات.
 - المتطلبات لإجراء سياسات الأمان **procedural security requirement** : هذه المتطلبات تحتوي أساسياً على سياسات الدخول/الوصول، وقواعد المساعدة، وخطط وثائق استمرارية العمليات **(continuity-of-operations)**
 - ضمان الأمان **assurance security** : وهذا يشمل عرض شهادات التصديق والاعتماد ووثائق التخطيط المستخدمة في عملية الضمان.
- الوصف لهذه السياسات **Policy Description**: يركز على التخصصات الأمنية، والضمانات والإجراءات واستمرارية العمليات، والوثائق. حيث يصف كل جزء من هذا الجزء من السياسة كيفية قيام معمارية النظام في فرض الأمان.
- المفهوم الأمني للعمليات **security concept of operation**: يعرف أساساً الأدوار والمسؤوليات ومهام سياسة الأمان. لأنها تركز على المهمة، والاتصالات، والتشفير، وقواعد المستخدم والصيانة، وإدارة الوقت الضائع، واستخدام البرمجيات المملوكة للقطاع الخاص مقابل برمجيات الدومين العام، وقواعد إدارة البرامج التجريبية، وسياسة الحماية من الفيروسات.
- تخصيص الأمان لتطبيقه على عناصر المعمارية **allocation of security enforcement to architecture elements**: يوفر تخصيص بنية نظام الكمبيوتر إلى كل نظام من البرنامج.

أنواع سياسات الأمان (TYPES OF SECURITY POLICY)

سياسة الأمان هو عبارة عن مستند يحتوي على معلومات عن طريقة وتحrott الشركة لحماية أصول المعلومات الخاصة بها من التهديدات المعروفة وغير معروفة. هذه السياسات تساعد على الحفاظ على سرية، وتوافر، وسلامة المعلومات. يوجد أربعة أنواع رئيسية من السياسات الأمنية هي كما يلي:

- (1) **Promiscuous Policy** **سياسة خفيفة**: تتميز هذه السياسة بعدم وجود أي قيود على الوصول إلى الإنترنت. يمكن للمستخدم الوصول إلى أي موقع، وتحميل أي تطبيق، والوصول إلى كمبيوتر أو شبكة من موقع بعيد. في حين أن هذا يمكن أن يكون مفيداً في الأعمال التجارية للشركات حيث كان الناس الذين يسافرون أو العمل في المكاتب الفرعية تحتاج إلى الوصول إلى شبكات تنظيمية، العديد من التهديدات مثل البرمجيات الخبيثة **(malware)**، والفيروسات، وترواده موجودة على شبكة الانترنت. بسبب

حرية الوصول إلى الإنترنت، وهذه البرمجيات الخبيثة (**malware**) من الممكن أن تأتي كمرفقات دون علم المستخدم. يجب أن يكون مسؤولي الشبكة في حالة تأهب للغاية إذا ما تم اختيار هذا النوع من السياسة.

- (2) **سياسة متساهلة Permissive Policy:** يتم قبول أغلبية حركة المرور (**internet traffic**) على الإنترنت، ولكن يتم حظر العديد من الخدمات والهجمات الخطيرة المعروفة. وأنه يعمل على حظر الهجمات المعروفة فقط، فإنه من المستحب لمسؤولي النظام مواكبة التطور الحالي في الهجمات. الإداريين يحاولون دائماً اللحاق بالركب بمعرفة الهجمات والاختراقات الجديدة.
- (3) **سياسة حكيم Prudent Policy:** تبدأ هذه السياسة بحظر كافة الخدمات. مسؤولي النظام (**administrator**) يمكنوا فقط الخدمات الأمنة والضرورية بشكل فردي. وهذا يوفر أقصى قدر من الأمان. كل شيء مثل أنشطة النظام والشبكة يتم تسجيله.
- (4) **سياسة مراهقة Paranoid Policy:** تبدأ هذه السياسة بمنع كل شيء. هناك قيود صارمة على استخدام أجهزة الكمبيوتر الخاصة بالشركة، سواء كان استخدام النظام أو استخدام الشبكة. بسبب هذه القيود على الملقن **server** بشكل مفرط، فإن المستخدمين غالباً ما يحاولون إيجاد السبل حول هذه السياسة.

الخطوات لإنشاء وتطبيق السياسات الأمنية (STEPS TO CREATE AND IMPLEMENT SECURITY POLICIES)



تنفيذ السياسات الأمنية يقلل من خطر التعرض لهجوم. وبالتالي، يجب أن يكون كل شركة السياسات الأمنية الخاصة التي تقوم على أعمالها. وفيما يلي الخطوات التي يجب أن تتبعها كل مؤسسة من أجل وضع وتنفيذ السياسات الأمنية:

1. تنفيذ عملية تقييم المخاطر لتحديد المخاطر إلى أصول معلومات المنظمة.
2. التعلم من المبادئ التوجيهية الفياسية وغيرها من المنظمات.
3. في وضع السياسات فإنها تشمل الإدارة العليا وجميع الموظفين الآخرين.
4. تعين عقوبات واضحة وتحفظها وأيضاً من راجعة وتحديث السياسة الأمنية.
5. جعل النسخة النهائية متاحة لجميع الموظفين في المنظمة.
6. ضمان كل فرد من الموظفين أن يقوم بقراءته، وفهم السياسة.
7. تثبيت الأدوات التي تحتاجها لتطبيق سياسة.
8. تدريب موظفيه وتقديرهم حول السياسة.

أمثلة على السياسات الأمنية كالتالي:

وفيما يلي بعض الأمثلة على السياسات الأمنية التي تم إنشاؤها، وتم قبولها، واستخدامها من قبل المنظمات في جميع أنحاء العالم لتأمين أصولها ومواردها الهامة.

- **Acceptable-Use Policy**
يحدد الاستخدام المقبول لموارد النظام.
- **User-Account policy**
يحدد عمليات إنشاء الحساب (**account**). يحدد السلطة، والحقوق، والمسؤوليات الخاصة بحسابات المستخدمين.

Remote-Access Policy •

يحدد من له الصلاحية في استخدام الاتصال عن بعد، ويحدد الضوابط الأمنية لهذا الاتصال عن بعد.

Information-Protection Policy •

يحدد مستويات حساسية المعلومات، ومن الذي يتاح له الوصول لهذه المعلومات؟ وكيف يتم تخزينها ونقلها؟ وكيف ينبغي حذفها من وسائل التخزين؟

Firewall-Management Policy •

يحدد وصول، وإدارة، ورصد الجدران الناريه في المنظمات.

Special-access Policy •

تحدد هذه السياسة أحكام وشروط منح وصول خاص إلى موارد النظام.

Network-Connection Policy •

يحدد الذين يمكنهم تثبيت موارد جديدة على الشبكة، والموافقة على تركيب الأجهزة الجديدة، وتوثيق تغيرات الشبكة، الخ.

Email Security Policy •

أنشأت لتحكم الاستخدام السليم للبريد الإلكتروني للشركات.

Password Policy •

يوفر مبادئ توجيهية لاستخدام كلمة مرور قوية على موارد المنظمة لحمايتها.

(RESEARCH VULNERABILITY SECURITY)

Research Vulnerability هي تقنيات يستخدمها مختبرى الاختراق لاكتشاف الثغرات وضعف التصميم التي يمكن من خلالها الهجوم على التطبيقات وأنظمه التشغيل، وتشمل الدراسة الديناميكية للمنتجات والتقييم المستمر لإمكانية الاختراق. هذه البحث تساعد كل من مسئولي الأمان والمهاجمين. ويمكن تصنيفها على أساس:

- مستوى الخطورة (منخفضة، متوسطة، أو عالية)
- استغلال النطاق (محلي(local)، عن بعد(remotely)).

وتسخدم هذه التقنية:

- لتحديد وتصحيح نقاط ضعف الشبكة.
- لحماية الشبكة من التعرض للهجوم من قبل الدخلاء.
- للحصول على المعلومات التي تساعد على منع المشاكل الأمنية.
- لجمع المعلومات حول الفيروسات.
- للعثور على نقاط الضعف في الشبكة وتتبیه مدير الشبكة قبل حصول الهجوم.
- لمعرفة كيفية التعافي من الهجوم.

VULNERABILITY RESEARCH WEBSITE**1. CodeRed Center**

المصدر: <http://www.eccouncil.org>

هو مصدر امني شامل لمسؤولي النظام (**admin**) والتي يمكنها أن تعطيك تقرير يومي ودقيق وأحدث المعلومات عن أحدث الفيروسات، وأحصنة طروادة، والبرمجيات الخبيثة، والتهديدات، وأدوات الأمان والمخاطر ونقاط الضعف.

2. TechNet

المصدر: <http://blogs.technet.com>

موقع تم إنشائه من قبل فريق سيرفرات مايكروسوفت (**Microsoft Lync server teams**). يتم قيادتهم من قبل **Lync Server documentation** الكتاب والمعلقين التقين يأتون من جميع التخصصات والتي تشمل مهندسي الإنتاج ومهندسي الحقول ومهندسي الدعم ومهندسي التوثيق والعديد من التخصصات الأخرى.

Security Magazine .3

[المصدر:](http://www.securitymagazine.com)

هذا الموقع يركز على الحلول الفريدة لقادة المؤسسة الأمنية. لقد تم تصميمه وكتابته للمديرين التنفيذيين لرجال الأعمال الذين يقومون بإدارة المخاطر والمؤسسة الأمنية.

SecurityFocus .4

[المصدر:](http://www.securityfocus.com)

هذا الموقع يركز على عدد قليل من المجالات الرئيسية التي هي من أعظمها أهمية للمجتمع الأمني. وعند تصفح الموقع سوف ترى بعض التصنيفات منها كالاتى:

BugTraq يحتوى على قائمه بريديه كبيرة الحجم والإفصاح الكامل لمناقشة تفصيلية والإعلان عن الثغرات الأمنية للكمبيوتر. وهو يعتبر حجر الأساس بالنسبة لمجتمع الانترنت الأمني.

The SecurityFocus Vulnerability Database يوفر للمتخصصين في مجال الأمن معلومات محدثة عن نقاط الضعف لجميع المنصات والخدمات.

Help Net Security .5

[المصدر:](http://www.net-security.org)

هو موقع إخباري يومي عن الأمان والذي يغطي أحدث الأخبار عن أجهزة الكمبيوتر وأمن الشبكات منذ تأسيسها عام 1998. بجانب تعطية الأخبار في جميع أنحاء العالم، فإنه يركز أيضاً على جودة المواد الفنية والورقات، ونقاط الضعف، تحذيرات البائعين، والبرمجيات الخبيثة، وتستضيف أكبر مساحة تحميل للبرمجيات الآمنة مع برامج ويندوز، لينكس، ونظام التشغيل **Mac OS X**.

HackerStorm .6

[المصدر:](http://www.hackerstorm.com.uk)

هو مورد أمني للفراغنة الأخلاقيين ومخبرى الاختراق لوضع خطط اختراق الأختراق أفضل ونطاقات أفضل، وإجراء بحث عن الضعف.

SC Magazine .7

[المصدر:](http://www.scmagazine.com)

هو موقع يتم نشره من قبل **Haymarket Media Inc.** وهو جزء من العلامة التجارية العالمية. ويوجد ثلاثة إصدارات من هذه المجلة.

North America –U.S. and Canada إصدار لأمريكا الشمالية مخصص لأمريكا وكندا

International – U.K and mainland Europe إصدار عالمي مخصص لإنجلترا وبعض البلدان الأوروبية.

Asia Pacific online إصدار يتم قراءته بواسطة صانعي القرار لأكثر من 20 دولة موجود في منطقة المحيط الهادئ.

المجلة يتم إصدارها شهرياً في أول أسبوع في الشهر. وهي أكبر مجلة لأمن المعلومات في العالم مع أكبر توزيع في العالم. بدأت العمل سنة 1989.

Computerworld .8

[المصدر:](http://www.computerworld.com)

لأكثر من 40 سنة أصبحت computer world المصدر الرئيسي للأخبار التكنولوجيا والمعلومات على مستوى العالم.

HackerJournals .9

[المصدر:](http://www.hackerjournals.com)

هو مجتمع أمن المعلومات على الانترنت. إنها تنشر الأخبار المتعلقة على وجه التحديد لتهديدات أمن المعلومات والقضايا من جميع أنحاء العالم. وهم عبارة عن فريق بحثي يعمل على بحث وتجميع الأخبار من عشرات الآلاف من المواقع لتجلب لك عناوين الأمان الأكثر ملاءمة في مكان واحد. بالإضافة إلى الأخبار، فإنها تستضيف **blogs** والمناقشات، وأشرطة الفيديو التعليمية، ولقد أصبح من أفضل مواقع الإختراق الأكثر شهرة في العالم.

WindowsSecurity Blogs .10

[المصدر:](http://blogs.windowsecurity.com)

كتب بواسطة المؤلفين المشهورين الذين يقودون خبراء الصناعة.

ما هو اختبار الاختراق (WHAT IS PENETRATION TESTING)?

اختبار الاختراق (**penetration test**): هو وسيلة لتقدير مستويات الأمان لنظام أو لشبكة معينة. تساعد على حماية الشبكة حيث إذا لم يتم اكتشاف نقاط الضعف في أسرع وقت ممكن فإنك سوف تكون مصدر سهل للهاكر. خلال اختبار الاختراق، فإن الشخص الذي يقوم بهذا الاختبار يحل كل الإجراءات الأمنية التي تستخدمنا لتشخيص ضعف التصميم، والعيوب الفنية، ونقاط الضعف. هناك نوعان من الاختبار كالتالي:

- **الصندوق الأسود (black box)**

هو إنشاء هجوم من قبل أشخاص ليس لديهم معرفة مسبقة عن البنية التحتية لفحصها.

- **الصندوق الأبيض (white box)**

هو إنشاء هجوم من قبل أشخاص لديهم معرفة كاملة عن البنية التحتية لشبكة.

بمجرد الانتهاء من الاختبارات فإن الشخص المسؤول عن الاختبارات (**pen tester**) يبدأ في إعداد تقارير والتي تشمل جميع نتائج الاختبار والتي تبين مناطق الضعف التي تم إيجادها.

وتشمل هذه التقارير تفاصيل عن نشاط الاختراق، ونقاط الضعف مفصلة وإجراءات الوقاية والإقتراحات وعادة ما يكون تسليمها في شكل نسخة مطبوعة لأسباب أمنية.

ما أهمية PEN TESTER؟

- تحديد التهديدات التي تواجه أصول المعلومات في المؤسسة
- تخفيض تكاليف أمن تكنولوجيا المعلومات للمؤسسة وتوفير أفضل عائد من الاستثمار الأمن (**ROSI**) حسب تحديد وحل نقاط الضعف. (**ROSI = Return On Security Investment**)
- توفير المنظومة مع الضمان: من خلال تقييم شامل للمنظومة الأمنية والتي تغطي السياسة(**policy**)، والإجراءات، والتصميم، والتنفيذ.
- الكسب والحفاظ على شهادة لتنظيم الصناعة(**BS7799,HIPAA etc.**).
- تبني أفضل الممارسات من خلال مطابقة اللوائح القانونية والصناعة.
- الاختبار والتحقق من صحة وكفاءة الحماية الأمنية والضوابط.
- تغيير أو ترقية البنية التحتية القائمة من البرمجيات أو الأجهزة أو تصميم الشبكات.
- التركيز على نقاط الضعف الأكثر شدة والتأكيد من الأمان على مستوى التطبيق.
- توفير نهج شامل لخطوات إعداد التي يمكن اتخاذها لمنع الاستغلال.
- تقييم كفاءة أجهزة أمن الشبكات مثل الجدران الناريه والموجهات/الراوتر وخوادم ويب.

PENETRATION TESTING METHODOLOGY

بمثابة إنك **pen tester**، فيجب عليك ألا تغفل عن أي مورد للمعلومات. يجب أن يتم اختبار جميع مصادر المعلومات الممكنة للبحث عن نقاط الضعف، ليس فقط مصادر المعلومات، ولكن يجب أن يتم اختبار كل آلية وبرنامجه المستخدمون في عملك لأنه إذا كان المهاجم ليس قادرًا على خرق نظام المعلومات، فإنه أو إنها قد تحاول الوصول إلى النظام ومن ثم إلى المعلومات الحساسة. هناك عدد قليل من الهجمات، مثل هجمات الحرمان من الخدمات (**denial-of-services**، والتي لا تحتاج إلى الدخول إلى النظام. وبالتالي لضمان أن تحقق فحص لجميع السبل الممكنة لاختراق النظام أو الشبكة، يجب عليك اتباع منهجية اختبار الاختراق. وهذا يضمن النطاق الكامل للاختبار.



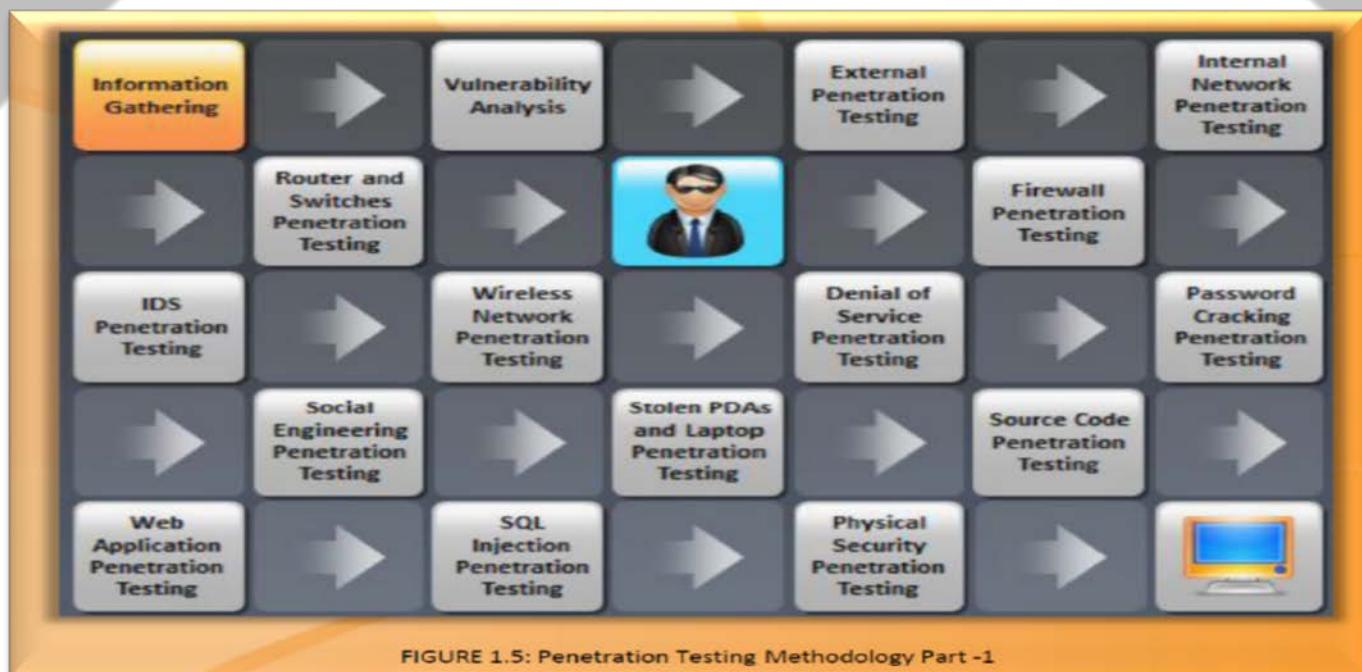


FIGURE 1.5: Penetration Testing Methodology Part -1

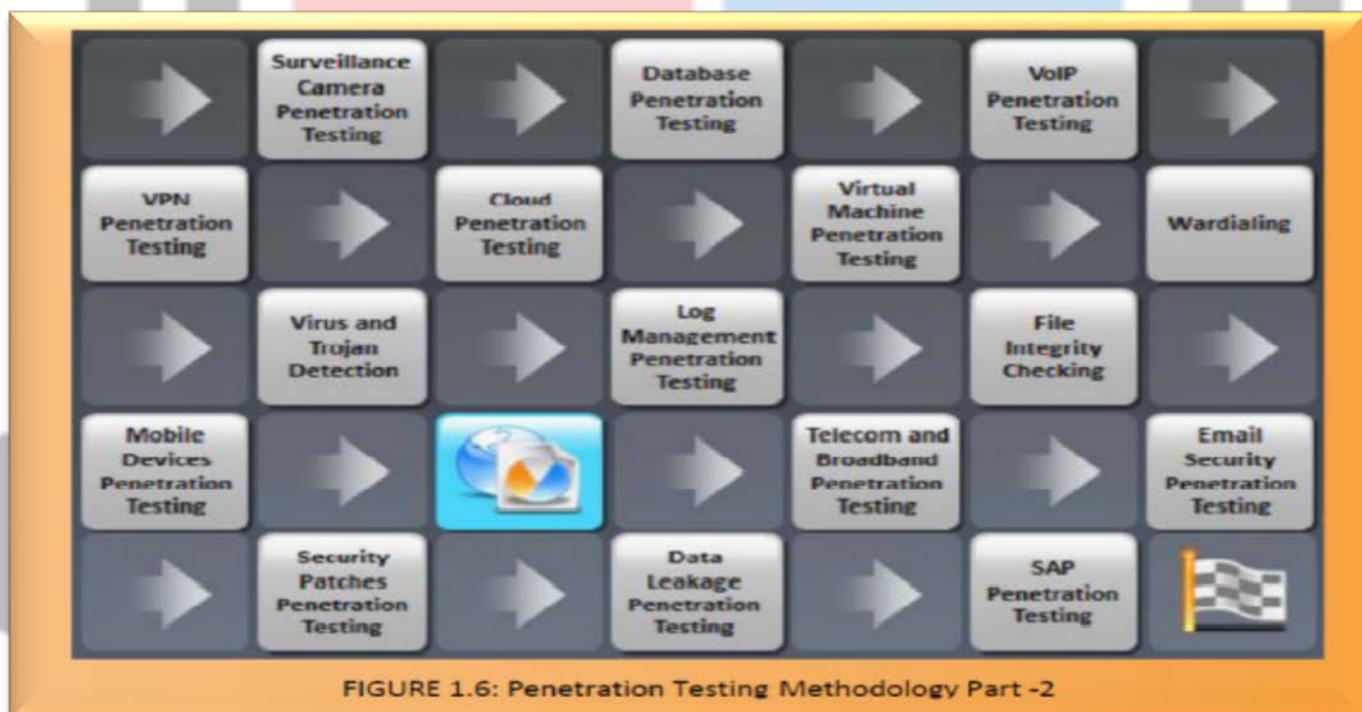


FIGURE 1.6: Penetration Testing Methodology Part -2

لا تنسونا بالدعاء

د. محمد صبحي طيبة

