Ethical Hacking

By Ahmad Elhoni

1

Chapter One

- What is hacking?
- Types of hackers
- What is cybercrime?
- Types of Cybercrime
- What is ethical hacking?
- Legality of ethical hacking

2

What is hacking?

- Hacking can be defined as identifying weakness in computer systems and/or networks and exploiting the weakness to gain access.
- An example of hacking is using login algorithm to gain access to a system.
- A hacker is that person who finds and exploits weakness in the system in general.
- Hackers are usually skilled computer programmers with knowledge of computer security.

3

ماهو القرصنة؟

- يمكنتعريف القرصنة على أنها تحديد نقاط الضعف في أنظمة الكمبيوتر و / أوالشبكات واستغلال الضعف للوصول إليها.
- مثالعلى القرصنة هو استخدام خوارزمية تسجيل الدخول للوصول إلى النظام.
- الهاكرهو ذلك الشخص الذي يجد ويستغل الضعف في النظام بشكل عام.
- عادةما يكون المتسللون من المبرمجين المهرة الذين لديهم معرفة بأمن الكمبيوتر.

3

Types of Hackers

- **White Hacker (Ethical Hackers):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments. اختبار الاختراق وتقييمات الضعف.
- **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

4

أنواعالهاكرز

- الهاكرالأبيض (الهاكر الأخلاقي):المتسلل الذي يمكنهالوصول إلى الأنظمة بهدف إصلاح نقاط الضعفالمحددة. يمكنهم أيضاً إجراء اختبار الاختراقوالضعف التقييمات.
- المفرقع(القبعة السوداء):متسلل يحصل على وصول غير مصرحبه إلى أنظمة الكمبيوتر لتحقيق مكاسب شخصية. عادةما يكون القصد هو سرقة بيانات الشركة وانتهاك حقوقالخصوصية وتحويل الأموال من الحسابات المصرفيةوما إلى ذلك.

4

Types of Hackers – cont.

- **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- **Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.

- قبعةرمادية:متسلل يقع بين قراصنة القبعة الأخلاقية والسوداء.يقوم باختراق أنظمة الكمبيوتر دون سلطة بهدفتحديد نقاط الضعف وكشفها لمالك النظام.
- السيناريوkiddies:شخص غير ماهر يمكنه الوصول إلىأنظمة الكمبيوتر باستخدام أدوات مصنوعة بالفعل.

5

5

Types of Hackers – cont.

- **Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- **Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

- هاكتيفيست:متسلل يستخدم القرصنة لإرسال رسائلاجتماعية ودينية وسياسية وما إلى ذلك. يتم ذلكعادةً عن طريق اختطاف مواقع الويب وترك الرسالةعلى موقع الويب الذي تم الاستيلاء عليه.

6

- Phreaker: مخترق يقوم بتحديد واستغلال نقاط الضعففي الهواتف بدلاً من أجهزة الكمبيوتر.

6

What is Cybercrime?

- Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc.
- Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications.

ماهي الجرائم الإلكترونية؟

- الجريمةالإلكترونية هي استخدام أجهزة الكمبيوتر والشبكات لأداء أنشطة غير قانونيةمثل نشر فيروسات الكمبيوتر ، والتنمر عبر الإنترنت ، وإجراء عمليات تحويلالأموال الإلكترونية غير المصرح بها ، وما إلى ذلك.
- ترُتكبمعظم الجرائم الإلكترونية عبر الإنترنت. يمكن أيضاً تنفيذ بعضالجرائم الإلكترونية باستخدام الهواتف المحمولة عبر الرسائل القصيرةوتطبيقات الدردشة عبر الإنترنت.

7

7

Type of Cybercrime

- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.

نوعالجريمة الإلكترونية

- الكمبيوترالاحتيال:الخداع المتعمد لتحقيق مكاسب شخصية من خلال استخدامأنظمة الكمبيوتر.
- انتهاكالخصوصية:الكشف عن المعلومات الشخصية مثل عناوين البريد الإلكتروني ورقم الهاتفوتفاصيل الحساب وما إلى ذلك على وسائل التواصل الاجتماعي والمواقع الإلكترونية ومإلى ذلك.
- سرقةالهوية:سرقة معلومات شخصية من شخص ما وانتحال صفة هذا الشخص.
- مشاركةالملفات / المعلومات المحمية بحقوق النشر:يتضمن ذلك توزيع الملفات المحميةبحقوق الطبع والنشر مثل الكتب الإلكترونية وبرامج الكمبيوتر وما إلى ذلك.

8

8

Type of Cybercrime – cont.

- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

9

- التحويلالإلكتروني للأموال:يتضمن ذلك الحصول على وصول غير مصرح به إلى شبكاتالكمبيوتر البنكية وإجراء تحويلات مالية غير قانونية.
- غسيلالأموال الإلكتروني:هذا ينطوي على استخدام الكمبيوتر لغسل الأموال.
- الاحتيالعلى أجهزة الصراف الآلي:يتضمن ذلك اعتراض تفاصيل بطاقة الصراف الآلي مثلرقم الحساب وأرقام التعريف الشخصي. ثم يتم استخدام هذه التفاصيل لسحب الأموالمن الحسابات المعترضة.
- هجماترفض الخدمة:يتضمن ذلك استخدام أجهزة الكمبيوتر في مواقع متعددة لمهاجمةالخوادم بهدف إيقاف تشغيلها.
- رسائلإلكترونية مزعجة:إرسال رسائل بريد إلكتروني غير مصرح بها. عادة ما تحتوي رسائل البريد الإلكترونيهذه على إعلانات.

9

What is Ethical Hacking?

- Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules:
  1. Get **written permission** from the owner of the computer system and/or computer network before hacking.
  2. **Protect the privacy** of the organization been hacked.
  3. **Transparently report** all the identified weaknesses in the computer system to the organization.
  4. Inform hardware and software vendors of the identified **weaknesses**.

10

ماهو القرصنة الأخلاقية؟

- القرصنةالأخلاقية هي تحديد نقاط الضعف في أنظمة الكمبيوتر و / أو شبكاتالكمبيوتر واتخاذ إجراءات مضادة تحمي نقاط الضعف. يجب على المتسللينالأخلاقيين الالتزام بالقواعد التالية:

1.احصل علىإذن كتابيمن مالك نظام الكمبيوتر و / أو شبكة الكمبيوتر قبل الاختراق.

2.حماية الخصوصيةالمنظمة تم اختراقها.

3.تقرير بشفافيةجميع نقاط الضعف التي تم تحديدها في نظام الكمبيوتر في المنظمة.

4.إبلاغ بائعي الأجهزة والبرامج عن الأشخاص الذين تم تحديدهمنقاط الضعف.

10

Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as **PayPal**. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

لماذاالقرصنة الأخلاقية؟

- المعلوماتهي واحدة من أكثر الأصول قيمة للمؤسسة. يمكن أن يؤدي الحفاظعلى أمان المعلومات إلى حماية صورة المؤسسة وتوفير الكثير منالمال للمؤسسة.
- يمكنأن يؤدي القرصنة إلى خسارة الأعمال للمؤسسات التي تتعامل في التمويلمثلباي بال.يضعهم القرصنة الأخلاقية في مرتبة متقدمة على مجرميالإنترنت الذين قد يؤديون بخلاف ذلك إلى خسارة الأعمال.

11

11

Legality of Ethical Hacking

- **Ethical Hacking is legal if the hacker abides by the rules stipulated in the previous section on the definition of ethical hacking.**
- The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

شرعيةالقرصنة الأخلاقية

- يعتبرالقرصنة الأخلاقية قانونية إذا التزم الهاكر بالقواعد المنصوص عليهافي القسم السابق حول تعريف القرصنة الأخلاقية.
- يقدمالمجلس الدولي لمستشاري التجارة الإلكترونية (EC-Council) برنامجشهادة يختبر مهارات الأفراد. أولئك الذين يجتازون الامتحان يتممنحهم شهادات. من المفترض أن يتم تجديد الشهادات بعد مرور بعضالوقت.

12

12

Summary

- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

- القرصنةهي تحديد واستغلال نقاط الضعف في أنظمة الكمبيوتر و / أو شبكاتالكمبيوتر.
- ترتكبالجرائم الإلكترونية جريمة بمساعدة أجهزة الكمبيوتر والبنية التحتيةلتكنولوجيا المعلومات.
- تدورأحداث القرصنة الأخلاقية حول تحسين أمان أنظمة الكمبيوتر و / أو شبكاتالكمبيوتر.
- القرصنةالأخلاقية قانونية.

13

Chapter two

- Potential Security Threats
- What is a Security Threat?
- What are Physical Threats?
- What are Non-physical threats?

14

Potential Security Threats

- **A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure.**
- Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

التهديداتالأمنية المحتملة

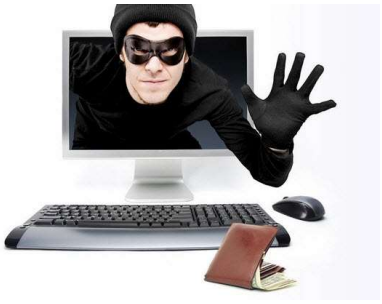
- تهديدنظام الكمبيوتر هو أي شيء يؤدي إلى فقدان البيانات أو تلفها أو تلفماديللأجهزة و / أو البنية التحتية.
- إنمعرفة كيفية التعرف على تهديدات أمان الكمبيوتر هي الخطوة الأولى في حمايةأنظمة الكمبيوتر. قد تكون التهديدات متعمدة أو عرضية أو ناجمة عن كوارثطبيعية.

15

15

What is a Security Threat?

- **Security Threat** is defined as a risk that which can potentially harm computer systems and organization. The cause could be **physical** such as someone stealing a computer that contains vital data. The cause could also be **non-physical** such as a virus attack.
- In this course chapter, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.



ماهو التهديد الأمني؟

- تهديدأمنييعُرفّ على أنه خطر يمكن أن يضر بأنظمةالكمبيوتر والمنظمة. يمكن أن يكون السبب بدني مثل قيام شخص ما بسرقة جهاز كمبيوتر يحتويعلى بيانات حيوية. يمكن أن يكون السبب أيضاً غير جسديةمثل هجوم الفيروس.
- فيهذا الفصل من الدورة التدريبية ، سوف نعرفّ التهديدعلى أنه هجوم محتمل من أحد المتطفلين يمكنأن يسمح لهم بالوصول غير المصرح به إلى نظامالكمبيوتر.

16

16

What are Physical Threats?

- A **physical threat** is a potential cause of an incident that may result in loss or physical damage to the computer systems.
- The following list classifies the physical threats into three (3) main categories:
  1. **Internal:** The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
  2. **External:** These threats include Lightning, floods, earthquakes, etc.
  3. **Human:** These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

ماهي التهديدات الجسدية؟

17

- أتهديد جسديهو سبب محتمل لحادث قد يؤدي إلى خسارة أو تلف مادي لأنظمةالكمبيوتر.
- تصنفالقائمة التالية التهديدات المادية إلى ثلاث (3) فئات رئيسية:

17

1.داخلي:تشمل التهديدات الحريق ، وإمدادات الطاقة غير المستقرة ، والرطوبة في الغرف التيتحتوي على الأجهزة ، وما إلى ذلك.
2.الخارجية:تشمل هذه التهديدات البرق والفيضانات والزلازل وما إلى ذلك.
3.الإنسان:تشمل هذه التهديدات السرقة والتخريب المتعمد للبنية التحتية و / أو الأجهزةأو التعطيل أو الأخطاء العرضية أو المتعمدة.

What are Physical Threats? – cont.

- To protect computer systems from the above mentioned **physical threats**, an organization must have physical security control measures. The following list shows some of the possible measures that can be taken:
  1. **Internal:** Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.
  2. **External:** Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
  3. **Humans:** Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

ماهي التهديدات الجسدية؟ - تابع

18

- لحمايةأنظمة الكمبيوتر مما سبق ذكرهالتهديدات الجسدية ،يجب أن يكون لدى المنظمة تدابيرمراقبة أمنية مادية. توضح القائمة التالية بعض الإجراءات الممكنة التي يمكن اتخاذها:

1.داخلي:يمكن منع تهديدات الحريق عن طريق استخدام أجهزة الكشف عن الحريق وطفايات الحريق الآليةالتي لا تستخدم الماء لإخماد الحريق. يمكن منع إمداد الطاقة غير المستقر باستخدام أجهزة التحكمفي الجهد. يمكن استخدام مكيف الهواء للتحكم في الرطوبة في غرفة الكمبيوتر.

2.الخارجية:يمكن استخدام أنظمة الحماية من الصواعق لحماية أنظمة الكمبيوتر من مثل هذه الهجمات. أنظمةالحماية من الصواعق ليست مثالية بنسبة 100٪ ، ولكنها تقلل إلى حد ما من فرص تسبب البرقفي حدوث أضرار. تعد أنظمة الكمبيوتر التي تسُكن في الأراضي المرتفعة إحدى الطرق الممكنة لحمايةالأنظمة من الفيضانات.

3.البشر:يمكن منع التهديدات مثل السرقة عن طريق استخدام الأبواب المقفلة والوصول المقيد إلى غرفالكمبيوتر.

What are Non-physical threats?

- **A non-physical threat is a potential cause of an incident that may result in;**
  1. Loss or corruption of system data
  2. Disrupt business operations that rely on computer systems
  3. Loss of sensitive information
  4. Illegal monitoring of activities on computer systems
  5. Cyber Security Breaches
  6. Others

ماهي التهديدات غير الجسدية؟

- التهديدغير المادي هو سبب محتمل لحادث قد يؤدي إلى ؛

1.فقدان أو تلف بيانات النظام
2.تعطيل العمليات التجارية التي تعتمد على أنظمة الكمبيوتر
3.فقدان المعلومات الحساسة
4.المراقبة غير القانونية للأنشطة على أنظمة الكمبيوتر
5.خروقات الأمن السيبراني
6.آخرون

19

19

What are Non-physical threats? – cont.

- The non-physical threats are also known as **logical threats**. The following list is the common types of non-physical threats;

1. Virus
2. Trojans
3. Worms
4. Spyware
5. Key loggers
6. Adware
7. Denial of Service Attacks
8. Distributed Denial of Service Attacks
9. Unauthorized access to computer systems resources such as data
10. Phishing
11. Other Computer Security Risks

ماهي التهديدات غير الجسدية؟ - تابع

- تعُرفالتهديدات غير الجسدية أيضاً باسمالتهديدات المنطقية.القائمة التالية هيالأنواع الشائعة من التهديدات غير المادية ؛

1.فيروس
2.أحصنة طروادة
3.الديدان
4.برامج التجسس
5.الحطابين المفاتيح
6.ادواري
7.هجمات الحرمان من الخدمة
8.هجمات رفض الخدمة الموزعة
9.الوصول غير المصرح به إلى موارد أنظمة الكمبيوتر مثل البيانات
10.التصيد
11.مخاطر أمن الكمبيوتر الأخرى

20

0

What are Non-physical threats? – cont.

- **To protect computer systems from the above-mentioned threats**, an organization must have **logical security measures** in place. The following list shows some of the possible measures that can be taken to protect cyber security threats
  - **To protect against viruses, Trojans, worms, etc.** an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.
  - **Unauthorized access to computer system resources can be prevented by the use of authentication methods.** The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.
  - **Intrusion-detection/prevention systems can be used to protect against denial of service attacks**. There are other measures too that can be put in place to avoid denial of service attacks.

21

- لحمايةأنظمة الكمبيوتر من التهديدات المذكورة أعلاه ،يجب أن تمتلك المنظمة تدابيرأمنية منطقيةفي المكان. توضح القائمة التالية بعض الإجراءات الممكنة التييمكن اتخاذها لحماية تهديدات الأمن السيبراني
  - للحمايةمن الفيروسات وأحصنة طروادة والديدان وما إلى ذلك.يمكن للمؤسسة استخدام برامجمكافحة الفيروسات. بالإضافة إلى برنامج مكافحة الفيروسات ، يمكن للمؤسسة أيضاً أنيكون لديها إجراءات تحكم في استخدام أجهزة التخزين الخارجية وزيارة موقع الويب الذي منالمرجح أن يقوم بتنزيل برامج غير مصرح بها على جهاز كمبيوتر المستخدم.
  - يمكنمنع الوصول غير المصرح به إلى موارد نظام الكمبيوتر باستخدام طرق المصادقة.يمكن أن تكونطرق المصادقة على شكل معرفات مستخدم وكلمات مرور قوية أو بطاقات ذكية أو مقاييسحيوية ، إلخ.
  - يمكناستخدام أنظمة الكشف عن التطفل / منعه للحماية من هجمات رفض الخدمة.هناك تدابيرأخرى أيضاً يمكن وضعها لتجنب هجمات رفض الخدمة.

21

Summary

- A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations.
- There are physical and non-physical threats
- Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.
- Non-physical threats target the software and data on the computer systems.

22

22