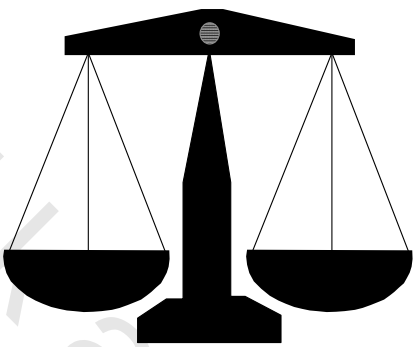

الفصل السادس

القرصنة والاختراق

القرصنة أو الاختراق

(الهاكرز والكراكرز)

س١٠١: ماذا يقصد بالقرصنة أو الاختراق؟

ج: يتم اختراق الأجهزة الكمبيوترية عن طريق القرصنة الرقمية بواسطة القراصنة لتحقيق أهداف لهم تختلف من صنف إلى الآخر ومنهم:

١ـ مَن يقف عند حد السرقة البسيطة.

٢ـ مَن يصل لأقصى درجات القسوة من التدمير والجاسوسية والنصب وإباحة الخصوصية.

س١٠٢: ما أنواع القراصنة أو المخترقين؟

ج: القراصنة أو المخترقون للسرية نوعان:

١ـ الهاكرز **Hackers**.

٢ـ الكراكرز **Crackers**.

س١٠٣: ما هي صفات القراصنة وتخصصاتهم؟

ج: الهاكرز **Hackers** كلمة كانت تطلق على المبرمجين الصانعين للبرمجة؛ أي الذين لهم مستويات عالية في البرمجة ولهم خبرة ودراية واسعة بالبرامج وخباياها وكانوا المبرمجين الشرفاء.

ومع بداية استخدام نظام ويندوز للتشغيل **Windows** اتضح أنه يحتوى على ثغرات أمنية كثيرة، ومع استخدام الإنترنت حدث تحول لدى الهاكرز فاتجهوا نحو الاختراق والتجسس على أجهزة الحاسب الآلي فتحولوا إلى لصوص.

أما الكراكرز Crackers فهم الذين تخصصوا في كسر Crack كلمات السر Passwords وكسر حماية البرامج ـ والتي يقال إنها محمية ـ ليس هذا فقط بل وتداولها .

س١٠٤: ما هي أنواع الاختراق؟

ج : يصنف الاختراق إلى ثلاثة أنواع هي :

١ـ اختراق للأجهزة الخادمة .

٢ـ اختراق للمواقع .

٣ـ اختراق للبريد .

س١٠٥: كيف تتم عملية الاختراق؟

ج : عن طريق برنامج يتم تصميمه ليتيح للمخترق أو القرصان اختراق جهاز شخص آخر بسهولة .

وبرامج الاختراق بها نقطة ضعف إذ إنه يمكن لصاحب الجهاز أن يتعرف على أن جهازه تم اختراقه من خلال رسالة أو تحذير وبالتالي يمكن القضاء عليه بسهولة مثلما يتم الاختراق بسهولة ، لكن البرنامج المسمى حصان طروادة Trojans Horse فهو الذي لا يشعر به صاحب الجهاز المختَرق ، وإن كانت البرامج الحديثة المضادة للفيروسات تتنبه إليه وتحذر من وجوده بل وتتخلص منه .

س١٠٦: ما الأسس التي يقوم عليها الاختراق؟

ج : تعتمد عملية الاختراق على ثلاثة أسس مترابطة مع بعضها وهى :

أـ تتبع الأثر Tracing :

هي مرحلة يتم فيها جمع معلومات عن الهدف واكتشافها وعن بناء النظام وأسماء البطاقات وعناوين الإنترنت Internet Address Protocol (IP) وذلك بوسائل تكنولوجية مختلفة عن طريق :

١ـ عمليات البحث المفتوح في مواقع الشركات .

٢ـ اكتشاف الخيارات الخاصة بإعداد الأمن لجدر النار .

٣ـ أسماء الاتصال .

٤ـ عناوين البريد الإلكتروني .

٥ـ أنظمة الأمن الخصوصية .

٦ـ الارتباطات .

٧ـ البحث في قواعد البيانات .

ب ـ المسح Scanning :

تمثل عملية المسح المرحلة التالية لمرحلة تتبع أو اقتفاء الأثر ، وعن طريق البحث في المنافذ **Ports** يتم المسح لإمكان الدخول إلى المواقع المختلفة المستهدفة عن طريق مسح نوافذ الويندوز **TCP windows** ، وهى تكنولوجيا خاصة بالوينـدوز تعمل على التقاط المنافذ المفتوحة .

جـ ـ التعداد Enumeration :

بعد تحقق هدفي تتبع الأثر والمسح من خلال تكنولوجيا جمع المعلومات ـ تتم عملية التعداد مباشرة وهى تتلخص في التعرف على موارد الهدف وتقاسيمها والتطبيقات المستخدمة ، فيتم الكشف عن تعداد المستخدمين في جدول أسماء **Net Bios** للشبكة وإظهار أسماء المستخدمين من خلال :

١ـ الأداة **Net View** .

٢ـ الأداتين **NBSSAN, NBSTST** .

وذلك لاستخراج المضيفات **Hosts** ويعتمد هذا على نقاط الضعف في نظام التشغيل لاستغلالها للدخول .

س١٠٧: ماذا عن برنامج حصان طروادة؟

ج: حصان طروادة **Trojan Horse Program** هو من البرامج الخطرة التي يستخدمها القراصنة بل وأخطرها على الإطلاق، وتكمن خطورته في المميزات التي يتمتع بها فتجعله الأقدر على الاختراق، كما أنه من الصعوبة كشفه وتتبعه والقضاء عليه ومن ثم فقد اكتسب هذه الشهرة.

يعمل حصان طروادة في الوقت الذي يعمل فيه مستعمل الجهاز دون كشفه أو الشعور به إلا بواسطة برامج كشف الفيروسات، ويمكِّن المخترِق من الحصول على كلمة السر للدخول إلى الجهاز.

س١٠٨: ماذا تعني مستويات الاختراق؟

ج: يقسم الاختراق إلى ستة مستويات حسب درجة خطورته كالآتي:

١ـ المستوى الأول للهجوم: وهو ما يعرف بهجوم قنبلة صندوق البريد التي تؤدى إلى إعاقة النظام عن تقديم الخدمة.

٢ـ المستوى الثاني للهجوم: وهو الدخول غير المرخص به النظام المعلومات أو الحاسبات مما يتيح قراءة الملفات أو نسخها للمخترق غير المرخص له.

٣ـ المستوى الثالث للهجوم: وهو دخول المهاجم مواقع غير مرخص له في الدخول إليها.

٤ـ المستوى الرابع للهجوم: وهو تمكن المخترق من قراءة ملفات سرية.

٥ـ المستوى الخامس للهجوم: وهو تمكن المخترق من نقل ونسخ الملفات السرية.

٦ـ المستوى السادس للهجوم: وهو الذي يستطيع خلاله المخترق إيجاد قناة مفتوحة للدخول إلى النظام والعبث بمحتوياته.

س١٠٩: كيف يتم اقتحام الجهاز بحصان طروادة؟

ج : يتم اقتحام جهاز الضحية ببرنامج حصان طروادة عن طريق التسلل لزرع الحصان وتوجد عدة طرق لزرعه وهى :

١ـ إرساله كملف ملحق بالبريد الإلكتروني ويقوم المرسل إليه باستقباله وفتحه وقد لا يرسل بصورة منفردة بل مع ملفات أخرى .

٢ـ عن طريق استخدام برنامج المحادثة ICQ أو برنامج MSN .

٣ـ عند تحميل برنامج من أحد المواقع غير الموثوق فيها .

٤ـ بكتابة كود معين على الجهاز .

٥ـ عند اتصال الجهاز بشبكة داخلية أو شبكة خارجية .

٦ـ عند استخدام برامج معينة مثل برنامج FTP وهو اختصار لـ File Transfer Protocol .

٧ـ استخدام منافذ الجهاز والتي يبلغ عددها ٦٥ ألف منفذ في كل جهاز .

س١١٠: ماذا عن أوجه الاختراق الأخرى؟

ج : يتم الاختراق عن طريق الإغراق بالرسائل للبريد الإلكتروني ويعنى إرسال كم هائل من الرسائل Messages لأجهزة الحسابات الآلية المراد تعطيلها وإيقافها عن العمل ، وبالفعل فإن هذه الدفقة الواحدة ذات المساحة الكبيرة بالنسبة للمساحة الصغيرة المخصصة للصندوق ـ توقف الجهاز عن العمل على الفور لأنها :

١ـ تملأ منافذ الاتصال . ٢ـ تملأ قوائم الانتظار .

كما يتم الاختراق عن طريق استخدام الفيروسات Viruses وهى برامج مثل البرامج العادية الموجودة بالجهاز لكنها مصممة بحيث يكون لها التأثير على جميع البرامج الأخرى على الجهاز وتعمل على :

١ـ جعل جميع البرامج نسخة منها . ٢ـ تقوم بمسح جميع البرامج على الجهاز .

س١١١: اذكر المزيد عن فيروسات الكمبيوتر؟

ج : تقوم بتعطيل الجهاز وكان بداية ظهورها عام ١٩٨١م، وهى متعـددة الأنـواع وتـسمى بهذا الاسم لتشابه عملها مع عمل الفيروسات التي تصيب الكائنات الحية .

من تقسيمات الفيروسات:

١ـ فيروسات الجزء التشغيل للأسطوانة .

٢ـ الفيروسات متعددة الأنواع .

٣ـ الفيروسات المصاحبة لبرامج التشغيل .

٤ـ الفيروسات المتطفلة .

س١١٢: ماذا عن ديدان الكمبيوتر، وبماذا تتميز؟

ج : ديدان الكمبيوتر هي :

١ـ برامج صغيرة .

٢ـ قائمة بذاتها ولا تعتمد على غيرها .

٣ـ تُصَنع للقيام بأعمال تدميرية أو سرقة البيانات الخاصة ببعض المستخدمين أثناء تصفحهم شبكة الإنترنت .

تتميز الديدان worms بسرعة الانتشار وصعوبة التخلص منها للأسباب الآتية :

١ـ قدرتها على التلون . ٢ـ قدرتها على التناسخ . ٣ـ قدرتها على المراوغة .

س١١٣: ما هي الكيفية التي تعمل بها الديدان؟

ج : تختلف طريقة عمل الديدان كالآتي :

١ـ منها ما يقوم بالتناسخ بأعداد هائلة .

٢ـ بعضها يقوم بالعمل على البريد الإلكتروني فترسل نفسها إلى جميع الموجودين بدفتر العناوين .

٣ـ وبعضها يقوم بإرسال رسائل قذرة إلى بعض الموجودة عناوين في دفتر العناوين بالجهاز باسم مالك الجهاز مما يوقعه في حرج .

كما ذكر فإن الديدان مستقلة ومن ثم تكمن خطورتها حيث تأخذ حرية الانتشار .

وتنتشر الديدان من خلال الرسائل المفخخة والتي تكون عناوينها جذابة .

س١١٤: كيف يمكن تجنب الديدان؟

ج : يمكن تجنب الديدان وانتشارها عن طريق عدم فتح الرسائل المفخخة والرسائل التي تفتح تكون معلومة المصدر وموثوق بها وإلا فلا .

س١١٥: ماذا عن القرصنة المالية؟

ج : القرصنة المالية تعنى استخدام أرقام البطاقات الائتمانية عبر شبكة الإنترنت بالشراء بها لأنها تعتبر نقوداً إلكترونية ، ويتم بها الاستيلاء على مال الغير حيث من السهل الحصول على أرقام بطاقات الائتمان من خلال :

١ـ مواقع التجارة الإلكترونية .

٢ـ طرق التصوير الرقمي .

٣ـ طرق السماع لنغمات الأرقام السرية .

٤ـ طرق النصب لإدخال الرقم عن طريق برامج خاصة .

س١١٦: ماذا عن ملفات التجسس؟

ج : ملفات التجسس هي ملفات ترسل للضحية للتجسس عليه عبر الشبكة وتكون عن طريق طمع وسذاجة الضحية حيث يتم سؤاله عن شيء يفضله فيجيب بالإيجاب

ويطلب الشيء المفضل فيرسل له ملف التجسس والذي عند فتحه يكـون المرسـل هـو ملف التجسس .

مهام ملف التجسس تتلخص في:

١ـ فتح منفذ **Port** ليتم من خلاله الاتصال بين جهاز المخترق وجهاز الضحية .

٢ـ قيام ملف التجسس بتحديث نفسه .

٣ـ قيام ملف التجسس بجمع المعلومات عن التحديثات التي طـرأت علـى جهـاز الضحية لإرساله للمخترق .

س١١٧: كيف يمكن الكشف عن ملفات التجسس؟

ج : يتم الكشف عن ملفات التجسس بملفات التسجيل **Windows Registry** وهى الـتي تسجل ما يحدث من تعديلات في الملفات سواء كان التعديل بسيطاً أو غيره ثم يـتحكم المخترق في جهاز الضحية .

س١١٨: ماذا يفعل ملف التجسس؟

ج : ملف التجسس **Patch File** يقوم بفتح ما يسمى منفذ أو قناة اتصال **Port** بـين جهـاز المخترق وجهاز الضحية وبذلك تسهل مهمة المخترق عبر هذه القناة، وهذا المنفـذ هـو منفذ غير مادي، وكما أشير من قبل فإن المنافذ في الجهاز متعددة وتبلغ ٦٥ ألف منفذ .

س١١٩: اذكر بعض برامج الاختراق التي تسهل هذه العملية؟

ج : من برامج الاختراق :

١ـ **Sub Seven** .

٢ـ **Net Bus** .

٣ـ **Back office** .

ولكل برنامج من هذه البرامج منافذ معينة من الـ ٦٥ ألف منفذ يقوم بفتحها .

والذي يسهل عملية الاختراق ما يلي :

١ـ الحصول على عنوان الإنترنت **IP** وهو هام جداً للمخترق .

٢ـ ملف تجسس بجهاز الضحية .

٣ـ رقم منفذ **Port** .

س١٢: ما خلاصة الحديث عن الاختراق؟

ج : ١ـ حصول المخترق على برنامج الاختراق **Hacking Program** ومعه ملف التجسس **Patch File** من الإنترنت عن طريق مواقع الهاكرز أو البحث عنها في محركات البحث .

٢ـ تثبيت البرنامج في الكمبيوتر الخاص به .

٣ـ إرسال ملف التجسس .

٤ـ الحصول على رقم الإنترنت **IP** الخاص بالضحية أثناء اتصال الضحية بالإنترنت .

٥ـ استخدام برنامج الاختراق في تنفيذ المهام التي يريدها المخترق .