اختراق الحاسوب : مصطلح الإختراق "Hacking" يعرف على أنه اختراق الأنظمة عن طريق التهرُّب و/أو تعطيل أنظمة الأمن في النظام المراد إختراقهُ. ولكن كلمة إختراق أو "Hack" ليس بالضرورة معناها الإختراق بقصد التخريب أو التدمير أو سرقة البيانات بل قد تُسخدم من قبل البعض لغرض التًّعرف على أخطاء الأنظمة من حيث قوة نظام حماية المستخدم. إلا أن الغالبية تستخدم المصطلح لغرض الإشارة إلى الإختراق غير القانوني.

أنواع الأختراق الألكتروني :

Spam: هي رسائل دعائية يتم إرسالها بكميات كبيرة أو إلي عدد كبير من ال Emails بغرض دعائي, مثلا دعايه لبرمجيات معينه او منتجات معينه إلخ.

Phishing: هي رسائل إحتيال إلكتروني يتم إرسالها أيضا إلي كميات كبيرة من ال Emails بشكل عشوائي بغرض سرقة حساباتهم البنكية او بطاقات الإئتمان Credit Cards أو كلمات المرور الخاصة بهم أو طلب من المستخدم أن يفتح ملف معين بغرض إختراق جهازه.

Spear Phishing: هو نفسه ال Phishing ولكن الفرق هنا أن ال Spear Phishing يتم إرساله إلي أهداف معينه ومحدده ويتم إرساله بشكل مدروس وليس عشوائيا, مثال إذا كان أحد المخترقين يستهدف شركة بعينها فإنه يقوم بعملية بحث علي مواقع التواصل مثل LinkedIn وغيرها وينتقي موظفين في وظائف معينة داخل الشركة ويقوم بإنتحال شخصية أحدهم لإرسال رسائل إلي زملائه في الشركة حتي يكسب ثقتهم في فتح ملفات معينه تسمح للمخترق بالتحكم في أجهزتهم او بسرقة كلمات المرور الخاصة بهم.

Vishing: هو نفس فكرة عمل ال Phishing لكنه يتم من خلال الإتصال بهاتف الضحية Voice Phishing حيث يقوم الهاكر بالإتصال بهاتف الضحيه من أي خدمة إتصال من خلال الإنترنت وينتحل صفة البنك او شركة الإتصالات إلخ ويطلب من الضحيه بياناته الشخصية والتي ستساعده فيما بعد في الوصول إلي حسابات الضحية.

Zeroday وتطلق علي الثغرات التي تصيب تطبيقات معينة وتكون الثغرة غير منتشرة علي الإنترنت والشركة صاحبة التطبيق المصاب لديها 0 أيام لإصدار ترقيع للثغرة قبل نشرها علي الإنترنت وفي بعض الأحيان حتي الشركة صاحبة التطبيق تظل لشهور أو سنوات لا تعلم عن الثغرة شئ.

APT :APT هي إختصار ل Advanced Persistent Threat وهي تطلق علي المخترقين اللذين يقومون بإستخدام برمجيات متطورة ومتقدمة تسمح لهم بالبقاء داخل شبكات الشركات وأجهزتها لمدة طويلة جدا دون أن يتم إكتشافهم وهؤلاء النوعية من المخترقين غالبا ما يستخدمون ثغرات من نوعية ال Zeroday لكي يقوموا بعملية الإختراق وزرع ال Backdoors الخاصة بهم داخل أجهزة وشبكات الشركات التي يقومون بإختراقها.

State Sponsored Attack: المخترقين اللذين يطلق عليهم كلمة State Sponsored هم المخترقين اللذين يعملون تحت مظلة الأجهزة الحكومية والإستخباراتية التابعة لبلادهم ويتم دعمهم ماديا وخططيا وعدديا ومعلوماتيا من تلك الجهات الحكومية/الإستخباراتية, وبما أن هؤلاء المخترقين هدفهم دائما هو البقاء داخل شبكات الجهات التي قاموا بإختراقها لأطول فترة فإنهم يطلق عليهم لقب ال APT الذي تم شرحه بالأعلي ودائما ما يستخدمون ثغرات من نوعية Zeroday في إختراقاتهم. أهداف ال State Sponsored Attackers دائما ما تكون أهداف حكومية, عسكرية, إستخباراتية أو حتي أهداف سياسية.

الأمن الألكتروني : علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى:-

أنظمة حماية نظم التشغيل

أنظمة حماية البرامج والتطبيقات.

أنظمة حماية قواعد البيانات.

أنظمة حماية الولوج أو الدخول إلى الأنظمة.

الفيروسات

الفيروس هو برنامج صغير مكتوب بأحد للغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعني انه يتركز علي ثلاث خواص وهي التخفي، التضاعف، وإلحاق الأذى.

مصادر الفيروس

يكمن مصادر الفيروس من خلال الرسائل الإلكترونية المجهولة، صفحات الإنترنت المشبوهة، نسخ البرامج المقلدة، استخدام برامج غير موثقة، كذالك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وارسال الملفات داخل الشبكة المحلية. للفيروس ثلاث خواص مؤثرة وهي:

التضاعف: تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملاين العمليات مما يسبب البطء في العمل أو توقف الحاسب عن العمل.

التخفي: لابد للفيروس من التخفي حتى لا ينكشف ويصبح غير فعال، ولكي يتخفي فأنة يقوم بعدة أساليب منها علي سبيل المثال، صغر حجم الفيروس لكي سيناله الاختباء بنجاح في الذاكرة أو ملف آخر.

إلحاق الأذى: قد يتراوح الأذى الذي يسببه الفيروس بالاكتفاء بإصدار صوت موسيقي أو مسح جميع المعلومات المخزنة لديك، ومن الأمثلة الاخري في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا أو إلغاء البرنامج المكتوب على BIOS.

طرق وأدوات لحماية أمن المعلومات

1. التأمين المادي للأجهزة والمعدات.
2. تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
3. تركيب أنظمة كشف الاختراق وتحديثها.
4. تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.
5. عمل سياسة للنسخ الاحتياطي.
6. استخدام أنظمة قوية لتشفير المعلومات المرسلة.
7. دعم أجهزة عدم انقطاع التيار.
8. نشر التعليم والوعي الأمني.

طرق انتقال الفيروس: تنتقل الفيروسات في الحاسوب بطريقتين رئيسيّتين، وهما:

* العدوى المباشرة (Direct Infector): يغزو الفيروس ملفات الحاسوب وعندما يتم تشغيل أو استخدام أحد هذه الملفات فإن الفيروس يبدأ بنشاطه وانتشاره وينتقل بين الملفات الموجودة على جهاز الحاسوب، وفور انتقال العدوى لأي ملف فإنه يتم تحميله ونقله إلى الذاكرة تلقائياً ومن ثم تشغيله.
* العدوى غير المباشرة (Indirect Infector): يُنقل البرنامج المصاب بالفيروس إلى ذاكرة جهاز الحاسوب فور بدء تشغيل الملف المصاب وينفذ الحاسوب أوامر الملف الأصلي، وبعد ذلك تنتقل الإصابة بالفيروس لأي ملف يتم تحميله إلى الذاكرة، ويتوقف هذا النوع من الانتشار في حال فصل التيار الكهربائيّ عن جهاز الحاسوب أو إعادة التشغيل.

أنواع الفيروسات تقسم فيروسات الحاسوب إلى أنواع، وهي على النحو التالي:

الفيروسات المخادعة (ذات قدرة تحويليّة متعددة): وهي البرامج التخريبيّة التي تمتلك القدرة على الديناميكيّة في التحوّل والتخفي من خلال تغيير شفرتها عند بدء بانتقال عدوتها بين الملفات، وذلك لعدم الكشف عنها. فيروسات قطاع التشغيل: يتمركز هذا النوع من الفيروسات في المواقع التي يقرأها جهاز الحاسوب من خلال القرص الصلب، ويبدأ مفعولها التخريبي بالسريان عند بدء إقلاع القرص الصلب وتستقر في ذاكرة جهاز الحاسوب وتبدأ بفك شفرتها وتنفيذ الأوامر. فيروسات الماكرو: يعتبر هذا النوع من أكثر أنواع الفيروسات الحاسوبية حداثة، ويعتمد المبرمجون على برنامج معالجة النصوص Microsoft word في كتابته، ويغزو الملفات التي تحتوي على البيانات وبشكل أدق ملفات الأوفيس.

الفيروسات ذات الملفات المتعددة: يدخل هذا النوع من الفيروسات إلى جهاز المستخدم بصيغة معيّنة وفور استقراره بالجهاز وتمكنه منه يبدأ بالتحوّل لأكثر من صيغة ليستهدف الملفات جميعها.

الفيروسات الخفيّة: يستقر هذا النوع في ذاكرة جهاز الحاسوب، ويتولّى مهمة إعاقة فحص نظام التشغيل وقطاعه، ويرسل تقرير بسلامة الجهاز وعدم العثور على أي فيروسات. فيروسات الملفات التنفيذيّة: تجعل هذه الفيروسات من نفسها ملحقاً مع ملفات البرامج التنفيذيّة ومرافقاً لها باستمرار، ومن هذه البرامج التنفيذية Command.com.

فيروسات ذات مهام متعددة، تغزو قطاع بدء التشغيل مع الملفات الموجودة على جهاز الحاسوب في آن واحد، أي أنّها تغزو جميع محتويات الحاسوب.

فيروسات قطاع التشغيل (Boot Sector): يُعتبر هذا النوع من أكثر أنواع الفيروسات خطورة ويهدّد بشكل مباشر المقطع التشغيليّ في القرص الصلب ويصيبه.

الفيروسات الطفيليّة: تتطفل هذه الفيروسات على الملفات التنفيذية وتتمركز في الذاكرة، وتبدأ عملها فور استخدام المستخدم لأي من البرامج المصابة، وتبدأ بعدها بغزو أي برنامج يتم تشغيله. الفيروسات المتطوّرة: لديها القدرة على الانتقال من جهاز حاسوب إلى آخر من خلال التحول من شفرة إلى أخرى.

\*\* تصنيفات الفيروسات تصنف برامج فيروسات الحاسوب إلى عدة أنواع، وهي:

أولا : تصنيفات الفيروسات وفقاً للنوع:

1. الفيروس: وهو عبارة عن برنامج تخريبي تنفيذي يحمل الامتداد (.scr, .pif, .bat, .exe, .com),يستهدف نظام الحاسوب ويلحق الضرر به. ديدان الحواسيب: ينتقل هذا النوع بالاعتماد على الاتصال بالشبكة العنكبوتيّة العالمية ويكون عادة عبر البريد الإلكترونيّ.
2. أحصنة طروادة (Trojan Horse): يدخل هذا الفيروس برفقة أحد البرامج إلى جهاز الحاسوب بشكل سريّ، ويبدأ بعمله بعد أن يتم تنفيذ البرنامج الذي دخل برفقته ويمارس أعماله التخريبيّة.

ثانيا : تصنيفات الفيروسات وفقاً للسرعة:

1. فيروسات بطيئة الانتشار.
2. فيروسات دائمة النشاط.
3. فيروسات مؤقتة النشاط.

\*\* أتأثير الفيروسات في الحاسوب

1. إبطاء عمل جهاز الحاسوب، وحدوث أخطاء مجهولة عند تشغيل البرامج وتنفيذ أوامرها.
2. توسيع حجم الملفات وزيادتها، وكما يزيد من المدة التي يتم بها تحميل البرامج والملفات إلى ذاكرة جهاز الحاسوب.
3. ملاحظة وجود تأثير غير مسبوق ورسائل على الشاشة. ظهور رسالة FATALI/o ERROR عند بدء قراءة الأقراص وزيادة المدة الزمنيّة في قراءتها في حال كانت محميّة. ملاحظة المستخدم صدور نغمات موسيقية غير مألوفة له.
4. إحداث تغييرات في تواريخ تسجيل الملفات.
5. اختلال عمل لوحة المفاتيح. تراجع المساحة المتوفرة في ذاكرة الجهاز، نظراً لما يشغله الفيروس من مساحة كبيرة. إظهار رسائل تكشف عن عدم وجود ذاكرة كافية لتحميل البرامج والملفات.
6. عدم صلاحيّة بعض المساحات للتخزين في القرص الصلب.
7. إلحاق الضرر بالنظام من خلال تعطيل BOOT Sector.
8. تعرض البيانات والملفات للإتلاف.

\*\* الوقاية من فيروسات الحاسوب يُنصح المستخدم عادةً بحماية جهازه من الفيروسات ووقايته منها، وذلك باتباع الخطوات التالية:

1. عدم تحميل أي برامج دون إجراء فحص لها، وكذلك الأمر بالنسبة للملفات المحملة والمنقولة من الشبكة العنكبوتيّة فيتوجب الفحص قبل التشغيل.
2. تحميل البرامج الخاصة للكشف عن وجود الفيروسات ومكافحتها في جهاز الحاسوب.
3. الاحتفاظ بنسخ احتياطيّة (Backup) للملفات والبرامج.
4. الاعتماد على برامج الجدار الناري التي تقف عائقاً في وجه الفيروسات.
5. تنصيب أنظمة تشغيل أكثر أماناً كنظام التشغيل جنو/لينكس.
6. عدم تشغيل ملفات وبرامج مجهولة المصدر.
7. أخذ الحيطة والحذر من الرسائل التي تصل عبر البريد الإلكترونيّ والروابط المجهولة المصدر وفحصها قبل فتحها.

\*\* إزالة فيروسات الحاسوب يُنصح المستخدم في حال اكتشافه وجود فيروسات بجهازه اتخاذ الإجراءات التالية:

تنصيب برامج حماية من الفيروسات (Anti-Virus). البدء بعمل Scan لكل الملفات الموجودة. وكما يمكن ذلك من خلال الاتصال بشبكة الإنترنت والولوج إلى مواقع الإنترنت والقيام بعملية الفحص، وتوفر Microsoft.com ذلك، إذ يتطلب ذلك من المستخدم الوصول إلى صفحة (برنامج مكافحة الفيروسات من MIcrosoft) على الشبكة العنكبوتيّة، واختيار "Download Now" التنزيل الآن، واتباع التعليمات لحين الانتهاء من التنزيل.