Cyber War

الحرب السيبرانية

الحرب السيبرانية ادواتها وقودها خسائرها

الكاتب

محمد سعد محمود

الحرب السيبرانية

اصبحت شبكة المعلومات الالكترونية جزءا لا يتجزأ من حياتنا اليومية ، اليوم جميع المؤسسات الحكومية والاهلية وحتى الاستخدامات الشخصية تستخدم المعلومات الرقمية وتقوم بمعالجتها وتخزينها ومشاركتها ، ومع زيادة هذه المعلومات وانتشارها ، اصبحت حماية هذه المعلومات اكثر حيوية ولها تأثير فعال لأمننا القومي واستقرارنا الاقتصادي . فالكل يعرف اليوم ان الحرب الحالية والقادمة هي حرب المعلومات . من هنا جاء مصطلح الامن السيبراني او Cyber security . عندما نفكر في كيفية حماية بلدنا او منازلنا من السراق والمخربين وحتى كيفية بناء جيش قوي على مستوى الدولة يتمتع بكافة المعداد والاسلحة للحماية والرد . اليوم اصبح التفكير اوسع بكثير فالأمن المعلوماتي اصبح من الضروري او من الاوليات التي تقاس بها الدول .

لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات من المعلوم أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. بالإضافة إلى ما تقدم، فقد أعلنت دولة كثيرة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية.

وبكلمات أخرى، فان الأمن السيبراني يشكل مجموع الأطر القانونية والتنظيمية، الهياكل التنظيمية، إجراءات سير العمل بالإضافة إلى الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني.

الامن السيبراني هو الجهد المستمر لحماية شبكات وبيانات المؤسسات والافراد من الاستخدام الغير مصرح به او اي اذى او اختراق يلحق بالشبكة .

على المستوى الشخصي ، تحتاج إلى حماية هويتك وبياناتك وأجهزتك الحاسوبية. على مستوى الشركة او المؤسسة ، يتحمل الجميع مسؤولية حماية سمعة الشركة وبياناتها وعملائها. على مستوى الدولة ، فإن الأمن القومي وسلامة المواطنين ورفاهيتهم على المحك.

انت اليوم بدون اتصال بالأنترنيت جميع الاشخاص القريبين عليك في المنزل او العمل والاصدقاء يعرفون معلوماتك الشخصية مثل اسمك او عمرك او المكان الذي تعيش فيه . مع الاتصال بالأنترنيت سوف تقدم نفسك للأخرين عبر هذا الاتصال والذي يتضمن معلوماتك الشخصية واسم المستخدم وغيرها هنا يجب ان تأخذ الحذر في تقديم كمية محدودة من المعلومات عنك بحيث لا تكون هذه المعلومات هدف للغرباء وتكون فريسة سهله للجرائم الالكترونية . في اغلب الدول المتقدمة يكون للفرد معلومات كاملة من جميع النواحي ... مثلا لكل فرد له سجلات طبية في كل مره يذهب الشخص الى الطبيب يضاف في السجل الصحي له حالته والتغيرات التي حصلت وجميع هذه الاشياء هي بيانات حتى الاجهزة الطبية مثل اجهزة اللياقة البدنية وغيرها ممكن ان توفر بيانات حول ضغط الدم والسكر لتصبح جزءا من سجلاتك الطبية . بالإضافة الى ان هناك كثير من الامثلة والمجالات من ضمنها التعليم وبياناتك في هذا المجال والسجلات المالية وغيرها من البيانات التي يتم حفظها . كل هذه المعلومات ممكن ان تستخدم ضدك او من الممكن الاستفادة منها بطرق غير شرعية .

الحرب السيبراني

الجزء الثاني... اين بياناتك وكيف تستغل .

في اغلب الدول تتوزع البيانات وتنتقل من مكان الى الاخر ومن شركة الى اخرى ، ويتم الاستفادة من هذه البيانات حسب مكان تواجدها . وهذه التنقلات للبيانات تجعلها اكثر عرضة للسرقة ، فمثلا البيانات الطبية الخاصة بك ممكن ان يتم مشاركتها مع شركة التأمين . اضافة الى ان دخولك الى السوبر ماركت وشرائك بضاعة او ماركة معينة ك معجون اسنان مثلا ، يقوم المتجر بتجميع ملف تعريفي لمشترياتك واستخدام تلك المعلومات لاستهداف المشتري بعروض خاصة ، باختصار سيكون للمتجر ملف شخصي لسلوك العميل الشرائي.

لو تكلمنا على الانترنيت وان تقوم بمشاركة صورك مع اصدقاءك ، قد يكون لا صدقاءك نسخ من صورك على حاسباتهم الشخصية في حال تم مشاركتها بشكل عام قد يكون للغرباء نسخ منها ايضا . بالإضافة الى خزن هذه الصور في سيرفرات موجوده في اجزاء مختلفة من العالم ... الان لم تعد الصور موجودة على اجهزة الكومبيوتر الخاصة بك فقط !!!

اذا كان لديك اي شيء ذو قيمة . فان المجرمين يريدون ذلك . فبيانات الاعتماد الخاصة بك على الانترنيت هي قيمة حيث تمنح بيانات الاعتماد هذه اللصوص امكانية الوصول الى حسابتك . ايضا تكلمنا على التامين الطبي الخاص بك ممكن سرقته والاستفادة من فوائده الطبية الخاص بك لأنفسهم .

هذه المقدمة تجعلنا نعطي نوعين من البيانات التنظيمية :-

البيانات التقليدية Traditional Data

وتشمل بيانات الشركة ومعلومات الموظفين والبيانات المالية ، كشف الرواتب ، العروض ، القرارات ، براءات الاختراع ، خطط المنتجات الجديدة . واسرار الشركة والخطط المستقبلية وكل هذه البيانات اذا تم فقدانها قد تكون كارثة على مستقبل الشركة .

انترنيت الاشياء والبيانات الكبيرة Internet of Things and Big Data

مع ظهور IOT هناك الكثير من البيانات التي سيتم توليدها .... IOT عبارة عن شبكة كبيرة من الاشياء المادية مثل المستشعرات والمعدات التي تمتد الى ما بعد شبكة الكمبيوتر التقليدية ، اضافة الى الخدمات السحابية Cloud والافتراضية . كل هذه البيانات وهذا النمو الكبير خلقت تقنية جديدة ومجالا واسعا يسمى البيانات الضخمة Big Data .... مع هذا التنوع والانتاجية للبيانات فأن سرية هذه البيانات وسلامتها وتوفرها اصبح من اهم الامور الضرورية لبقاء المنظمات والمؤسسات تعمل بشكل أمن

الحرب السيبرانية

الجزء الثالث ... Confidentiality, Integrity, and Availability

السرية والتكامل والتوافر ... المعروفة باسم CIA

وهي مختصر لأول الحروف للكلمات اعلاه . هذه الكلمات الثلاثة يجب تكون بمثابة دليل لأمن المعلومات لكل منظمة. فلابد من فهمها وتحقيقها .

السرية او الخصوصية Confidentiality:- يجب على الشركة او المؤسسة وضع سياسات تقيد الوصول الى المعلومات من قبل الموظفين المصرح لهم والتأكد من ان الافراد المرخص لهم فقط يشاهدون هذه البيانات ويفضل تجزئة البيانات وتقسيمها وفقا لمستوى الامان او مستوى حساسية هذه البيانات . علاوة على ذلك يجب تدريب الموظفين لفهم افضل الممارسات في حماية المعلومات الحساسة لحماية انفسهم وشركتهم من الهجمات ، مثل ضمان تشفير البيانات ، واسماء المستخدمين ، وكلمات المرور ، والمصادقة للدخول وغيرها من الامور التي تقلل من التعرض الى هجمات .

التكامل Integrity :- وهي نزاهة البيانات وموثوقيتها وتكاملها . بمعنى عند نقل الملفات من مكان الى اخر ، هل وصلت نفس الملفات ام اصبح عليها تعديل او تغير .. هناك خوارزميات تقوم بهذا الدور تعمل دور الهاشنك مثل MD5 و SHA-1 و SHA 256 و SHA512 . حيث تقوم هذه الخوارزميات بتحويل البيانات الى سلسلة ثابتة من الارقام والاحرف تمثل البيانات الاصلية حيث تقوم بتوليد قيمة تسمى Hash Value ، عند تحميل الملفات من الجهة الثانية يمكنك التأكد من عدم العبث او تلف الملفات خلال التنقل من خلال نفس القيمة التي تم توليدها اثناء الارسال . وهذا ما كان يستخدم سابقا اثناء الحروب عند ارسال الرسائل بين الدول حيث يتم تشفير الاحرف حسب رمز متفق عليه سابقا مثلا حرف A يرمز له ب ١١١

التوافر Availability :- وهي العمل بشكل مستمر للحفاظ على الشبكة والنظام مثل تحديث البرامج وانظمة التشغيل ، انشاء نسخ احتياطية للبيانات ، تنصيب برامج الحماية والاختراق ، تنصيب اجهزة الجدران النارية Firewall ... وغيرها من الامور ، بحيث نكون قيد الاستعداد لاي هجمات ووضع خطط مناسبة للتعافي من اي كوارث طبيعية او من صنع الانسان .

الحرب السيبراني

الجزء الرابع .. Lab – Compare Data with a Hash

الهدف من اللاب هو معرفة التغيرات التي طرأت على ملف معين ، هل تم اتلاف البيانات او العبث بها .

الخطوة الاولى : -

فتح برنامج Notepad المتوفر في جميع الحاسبات وكتابة اي جملة داخله مثلا

.This is a Text File that will be used to verify data integrity

لنعتبر هذا الفايل مهم ويجب علينا ارساله والتأكد من هذا الفايل قد استلم بدون اي تلاعب او تغير .

الخطوة الثانية :-

تنصيب برنامج HASHCalc من خلال المتصفح يمكن تنصيب هذا البرنامج وهذا رابط البرنامج

.http://www.slavasoft.com/download.htm

بعد فتح البرنامج من خانة Data نختار الملف ونفعل مثلا تشفير بواسطة MD5 سوف نلاحظ قيمة Hash value بعد الضغط على Calculate

مثلا :- b71f7456a4bb03bb930e770ea95899٧٣

الخطوة الثالثة :-

لو قمنا بالتلاعب في النص الموجود مثلا اي حرف او كلمة او رمز .... لنقوم بإضافة (.) اخرى في نهاية الملف وقمنا بحساب القيمة مرة اخرى لنلاحظ تغير قيمة Hash Value لتصبح مثلا

f96f9eeaf0b94efe4b01c1e60d842bb1

وهذه القيمة تختلف اختلاف جذري عن القيمة الاولى بالتالي نعرف ان هناك اصبح تغير وتعديل بالملف .

حاول تطبيق هذا اللاب للاستفادة من المعلومات .

الحرب السيبرانية

الجزء الخامس ... امثلة واقعية حصلت مع شركات عالمية.

ان حماية اي منظمة من هجوم الكتروني محتمل امر صعب وذلك لعددت اسباب ، قد تكون الخبرة اللازمة لأعداد وصيانة الشبكة الامنية مكلف جدا ، اضافة الى ان المهاجمون دائما يستمرون في البحث عن ثغرات وطرق جديدة لاستهداف الشبكة ، ستكون الاولية حينها الى مدى سرعة استجابة فريق الحماية والامان للهجوم لتقليل فقدان البيانات ووقت التعطيل والعودة من جديد . موضوع الاختراق من المواضيع المهمة والخطرة في مسيرة اي شركة او منظمة فهي بمثابة السمعة لها اضافة الى ذلك فان الشركة ستكون لابد من ان تكون على استعداد لايٍ تقاضي وقرارات تؤخذ ضدها كونها لم تكن قادرة على حماية ملفات عملاءها علاوة على حماية نفسها .

مثال ١ :- علَّقت شركة في تك V tech لتقنيات وألعاب الأطفال التداول في بورصة هونج كونج بعد الإقرار بتعرضها لاختراق إلكتروني أسفر عن سرقة بيانات نحو ٤.٨ ملايين عميل، بما في ذلك معلومات حساسة عن الأطفال ووالديهم. وتم اختراق حسابتهم وعنوانهم البريدي ومعلومات اكثر ، اضافة الى اسئلة الامان التي لم تنتبه الشركة وتجعلها مشفرة ، باعتقادي تعتبر هذه من الاختراقات الخطرة لأنها تتعامل مع معلومات اطفال ، لو فكرنا قليلا وقلنا لو قام المخترقون بجعل هذا الاختراق يعمل تجسس لكل طفل تم اختراقه .... ماهي الكوارث ؟؟؟!!!

مثال ٢:- في تموز ٢٠١٥ اكتشفت شركة Last Pass نشاطا غير معتاد على شبكتها ، حيث تبين ان مجموعة من المهاجمين قد سرقوا عناوين البريد الالكتروني للمستخدمين و رسائل التذكير الخاصة بكلمات المرور ولحسن الحظ لم يتمكنوا من معرفة المعلومات المخزنة بسبب المصادقات المشفرة التي وضعتها الشركة .

مثال ٣ :- تعرضت البيانات الشخصية الحساسة الخاصة بـ١٤٣ مليونا من عملاء شركة Equifax الائتمانية في الولايات المتحدة للخطر من قبل مجرمي الإنترنت، في واحدة من أكبر حوادث اختراق البيانات في تاريخ الولايات المتحدة.

وعلى الرغم من أن قواعد بيانات الائتمان الاستهلاكي والتجاري لم تتأثر، إلا أن الشركة صرحت بأن القراصنة تمكنوا من الوصول إلى أرقام الضمان الاجتماعي وتواريخ الميلاد وعناوين خاصة بالعملاء في الفترة بين منتصف مايو ويوليو ٢٠١٧، بالإضافة إلى ذلك، تأثرت أرقام بطاقات الائتمان لحوالي ٢٠٩٠٠٠ من المستهلكين.

مثال ٤:- شركة سوني ؟؟؟ اختراق سوني بيكتشرز انترتينمنت هو هجوم سيبرانية حصل في ٢٤ نوفمبر عام ٢٠١٤ من قبل حراس السلام(Guardians of Peace) ضد شركة سوني هناك تقارير تقول ان حجم الخسائر التي تعرضت لها الشركة هي

٧٧ مليون أيميل أنسرق.

٢٥ مليون حساب لمستخدمي سوني تهكر.

١٠٧٠٠ لبطاقات الخصم .

١٢٧٠٠ بطاقة ائتمان.

مراسلات سرية بين الموظفين.

سيناريوهات لأفلام سوف تصور قريبا ومن بينها فلم جيمس بوند.

خمس أفلام كان من المفترض أن يبدأ عرضها تسربت مثل Annie, Mr Turner, To Write Love On Her Arms

انخفاض أسهم بورصة سوني بنسبة ٦,٦ بالمئة.

خسائر مبدئية تقدر بي ١٠٠ مليون دولار.

و أخيرا سوني تعلن إيقاف عرض الفلم أو تأجيله...

لو عملت بحث في الانترنيت لوجدت الكثير من الشركات التي تم اختراقها والامثلة كثيره لا يسع ذكرها ، الهدف من ذكر هذه الامثلة ليس سردها والانتقاص من شركة معينه لكن لنبين للقارئ مدى خطورة الموضوع وان اي مؤسسة او شركة هي عرضة لأي اختراق قد يحصل ..... الى هنا اعتبر الاجزاء السابقة هي مقدمة عامة لكي نوضح للجميع مدى اهمية الحماية وماهي خطورة الاستهانة بها .

الحرب السيبرانية

الجزء الخامس ... انواع المهاجمون

المهاجمون او Attackers هم افراد او مجموعات يحاولون استغلال نقاط الضعف الموجودة في اي شبكة لتحقيق مكاسب شخصية او مالية ، يهتمون باي شيء ذو قيمة بدءا من بطاقات الضمان وتصميمات المنتجات وغيرها من الامور العامة والشخصية .

الهواة او Amateurs وهم عادة مهاجمون لديهم مهارات قليلة أو معدومة ، وغالبا ما يستخدمون الأدوات أو التعليمات الموجودة على الإنترنت لشن هجمات. البعض منهم مجرد فضول ، بينما يحاول آخرون إظهار مهاراتهم وإحداث الضرر. قد يستخدمون الأدوات الأساسية ، ولكن النتائج لا تزال مدمرة.

القراصنة او Hackers :- القراصنة هم مجموعة من المهاجمين الذين يعتمدون على هدف او اهداف في عملية الاختراق ، يتم تنصيفهم الى ثلاث انواع <<< القبعات البيضاء white hat ، القبعة الرمادية Gray hat ، القبعة السوداء Black hat

القرصان ذو القبعة السوداء- Black hat يعرف القرصان ذو القبعة السوداء بأنه مجرم إنترنت، حيث إن وظيفته تكمن في اختراق أنظمة الكمبيوتر إما الكيد أو المال. ويستغل القرصان ذو القبعة السوداء أي ثغرة أمنية في أنظمة الكمبيوتر لاختراقها، وإن لم يجد ثغرة فيقوم بتطوير برمجيات من شأنها إيجاد باب خلفي back door يستطيع الدخول من خلاله. ويبدأ القرصان ذو القبعة السوداء عمله، إما بدافع من مؤسسات أو أفراد تريد الاستيلاء على معلومات لدى جهات أخرى، أو تخريب أنظمة الكمبيوتر بها، بالإضافة إلى أنه قد يقوم بسرقة البيانات بنفسه، ثم يسوقها ويبيعها إلى من يعنيه الأمر مقابل المال. ويعد هذا النوع من قراصنة الإنترنت الأسوأ على الإطلاق، حيث يتم تصنيفهم ضمن المجرمين مثلهم كمثل اللصوص والقاتلين.

القرصان ذو القبعة البيضاء - White hat يعرف القرصان ذو القبعة البيضاء بأنه قرصان أخلاقي **Ethical Hacker** ، وتكمن وظيفته في اكتشاف العيوب والثغرات المتواجدة في أنظمة الشركات والمواقع والمؤسسات. ويستخدم القرصان ذو القبعة البيضاء خبراته وقدراته من أجل اختبار متانة الأنظمة، وإن اكتشف ثغرات بها، فيقوم على الفور بإبلاغ الجهة صاحبة النظام من أجل إصلاحها، حتى لا يستغلها القراصنة ذو القبعات السوداء. وهناك تصنيف خاص بالقراصنة ذوي القبعات البيضاء متعدد المراحل، تمامًا مثل تصنيف المنتخبات والأندية في عالم كرة القدم.

القرصان ذو القبعة الرمادية - Grey hat يقع هذا النوع من القراصنة بين النوعين المذكورين أعلاه، فهو كالراقصة، حيث يمكنه العمل على سرقة البيانات لصالح جهات أخرى، على رأسها الحكومات ووكالات الاستخبارات، بالإضافة إلى قدرته على اختراق أنظمة المؤسسات بنفسه واكتشاف ثغرات بها، ومن ثم إبلاغهم مقابل الحصول على الأموال.

القراصنة المنظمون Organized Hackers - وهم مجرمون وقراصنة محترفون ومنظمون بعملهم يركزون في عملهم على السيطرة على ثروات وقدرات دولة بأكملها وقد يكونون مدعومين من نفس الدولة ، وعادا ما يكونون مدربون تدريب عالي وممولين بشكل كبير ، قد يقومون حتى بهجوم الكتروني خدمة لمجرمين اخرين .

هناك ايضا نوعين من التهديدات التي يجب اخذها بنظر الاعتبار

الهجوم الداخلي internal Security Threats :- وهذه الهجمات تنشا من داخل المنظمة او من خارجها مثل الموظفين الموجودين او شركاء العمل ، وممكن اين يكون بقصد او بدون قصد . قد يكون عن طريق فلاش يعطى للموظف داخل الشركة او عن طريق البريد الالكتروني ، هذه التهديدات التي تكون من الداخل اقوى بكثير من الخارج لأن المستخدمين الداخليين لديهم إمكانية الوصول المباشر إلى المبنى وأجهزته الأساسية. يمتلك الموظفون أيضًا معرفة بشبكة الشركة ومواردها وبياناتها السرية ، بالإضافة إلى مستويات مختلفة من امتيازات المستخدم أو الإدارة.

التهديدات الخارجية External Security Threats :- وهي التي تأتي من الهواة أو المهاجمين المهرة من خلال استغلال نقاط الضعف في الشبكة أو أجهزة الكمبيوتر .

نصيحة :- حاول ان تتأكد من اي جهاز يدخل ويوضع على اي كومبيوتر داخل المؤسسة ايضا حاول التأكد من البريد الالكتروني قبل فتحه والتأكد من التصفح بالمواقع الامنة مع البرامج الموضوعة... اضافة الى ذالك حاول التأكد من الموظفين الموجودين داخل المؤسسة .

الحرب السيبرانية

الجزء السابع ... Cyber warfare

لم تعد الحروب تقتصر على استخدام الأسلحة الفتاكة التي تحملها الطائرات أو المدرعات أو الجنود، فهذه توشك أن تتوارى في المستقبل وراء ظل حروب ربما تكون أكثر فتكا وهي الحروب الإلكترونية.

فالحرب الإلكترونية (Cyber warfare) هو صراع ميدانه شبكة الإنترنت وينطوي على هجمات ذات دوافع سياسية على المعلومات ونظمها، حيث يمكنها تعطيل مواقع الويب الرسمية والشبكات وتعطيل الخدمات الأساسية أو سرقة وتعديل البيانات السرية، وتخريب الأنظمة المالية، وذلك من بين العديد من الاحتمالات الأخرى.

وحاليا فإن ثمة سباق بين الدول الغنية لتطوير برمجيات يكون من شأنها امتلاك قدرات هجومية وأخرى دفاعية قادرة على التصدي لأي هجمات مشابهة من هذا القبيل، فالولايات المتحدة تبذل جهودا كبيرة لتطوير أنظمة دفاع تحمي شبكاتها من القراصنة والهجمات المدمرة من جانب حكومات أجنبية، خاصة الصين وروسيا، كما أنها تسعى للحصول على قدرات هجومية إلكترونية تمكنها من تعطيل شبكات الحاسوب لدى العدو.

وبحسب صحيفة واشنطن بوست، فإن الجيش الأميركي وبقية الجيوش في العالم ترى في البرمجيات التخريبية أداة أساسية جديدة من أدوات الحرب الإلكترونية، وذلك في ظل تعرض شبكات الحاسوب العسكرية وشبكات وأنظمة الحاسوب المعنية بالبنى التحتية للدول وشبكات الاتصالات للتخريب.

وتفيد دراسة لمركز الدراسات الاستراتيجية والدولية بأن ١٥ دولة في العالم -وهي الدول التي تمتلك الميزانيات العسكرية الأضخم- تستثمر في مجالات متخصصة من أجل الحصول على قدرات هجومية إلكترونية عن طريق الإنترنت، ودمج القدرات الإلكترونية في عملياتها العسكرية.

وتشجع الولايات المتحدة الشركات المتخصصة فيها على ابتكار تقنيات من شأنها تدمير أو تعطيل أو إضعاف أي هجمات إلكترونية معادية، كما أن سلاح الجو الأميركي يحث باستمرار الشركات والجهات المتخصصة على تطوير مشاريع تقنية يكون من شأنها شن هجمات إلكترونية سريعة ضد الأهداف المعادية والتصدي لمثل تلك الهجمات في اللحظة ذاتها.

ويقول خبراء إنه سيصار إلى استخدام الأسلحة الإلكترونية قبل أو أثناء الصراعات بالأسلحة التقليدية، وذلك من أجل العمل على تعطيل شبكات العدو الإلكترونية أو التشويش عليها، بما في ذلك تعطيل شبكات الاتصالات لدى الجهات المعادية.

ويعد فيروس "ستاكس نت" -الذي تسبب في إلحاق أضرار بأجهزة التخصيب النووي الإيراني- من أبرز الأدلة على الهجمات الإلكترونية الحديثة، إذ أطلقته الولايات المتحدة وإسرائيل في ٢٠١٠ ضد حواسيب تابعة للمنشآت النووية الإيرانية بهدف إبطاء عملها.

ومن الأمثلة الأخرى الهجوم الأميركي الإلكتروني على نظام الدفاع الجوي الصربي سنة ١٩٩٨ لاختراقه بهدف تسهيل قصف أهداف صربية، وكذلك الهجوم الذي يعتقد أن مصدره روسيا واستهدف إستونيا سنة ٢٠٠٧ وأدى إلى تعطيل كافة مواقع الويب الحكومية والخاصة ووسائل الإعلام عبر البلاد. هنالك الكثير من الهجمات لا يسع المجال لذكرها ...

ويعتبر تأمين المعلومات والشبكات أكثر الطرق فعالية للحماية من الهجمات الإلكترونية، ويجب تطبيق التحديثات الأمنية على كافة الأنظمة، بما فيها تلك التي لا تعتبر حساسة، وذلك لأن أي ثغرة في النظام يمكن استغلالها لشن هجمات.

الحرب السيبراني

الجزء الثامن ...

طرق وتقنيات الهجمات

ايجاد نقاط الضعف Finding Security Vulnerabilities

الثغرات الامنية تحدث في البرامج software وفي المعدات والاجهزة Hardware وهذا ما يسبب استغلال من قبل المهاجمين

Software vulnerabilities الثغرات البرمجية :-

تحدث بسبب اخطاء موجودة في نظام التشغيل او في الكودات الخاصة ببرمجة النظام او البرامج ، اغلب الشركات تقوم ببذل الجهود لتصميم برنامج معين ، خالي من الثغرات وبعد فتره نلاحظ ظهور ثغرات جديدة او اخطاء معينه بالتالي دائما ما نلاحظ هناك تصحيحات وتحديثات جديدة من قبل الشركات تنزل بشكل مستمر لتفادي هذه الاخطاء وهذا ما نراه في اجهزة الكومبيوتر واجهزة الموبايل والبرامج التي تم تحميلها . اذا موضوع التحديث مهم جدا من الناحية الامنية هذه النقطة تجعلنا في تواصل مستمر لتقليل الثغرات الموجودة . في عام ٢٠١٥ تم اكتشاف نقاط ضعف رئيسية في راوتر سيسكو تسمى SYNful Knock في Cisco ios بسبب ان نسخة النظام للراوتر كانت غير كاملة وبعدها تلافت سيسكو الموضوع وتم رفع تحديث جديد للنظام.

التحديث مهم واغلب الشركات لديها فرق للاختبار مكرسة للبحث وللتأكد من سلامة النظام وعدم وجود ثغرات وتقوم بعمل تحديث لأي نقطة ضعف قد توجد بصورة دورية. ومن الامثلة على هذه الفرق Google project zero ،،، حيث قامت كوكل بوضع فريق مختص للبحث على نقاط الضعف في منتجاتها .

هناك عدة انواع للثغرات البرمجية سأكتفي بذكرها ممكن البحث عنها بالأنترنيت والاطلاع عنها وهي ضرورية لمصممي البرامج . من ضمنها Buffer overflow , Non-validated input , Race conditions , Access-control problems , Weaknesses in security practices

Hardware vulnerabilities الثغرات الخاصة بالأجهزة :-

وغالبا ما تحدث عن طريق عيب في تصميم المعدات ، مثال غالبا ما تصنع المكثفات الخاصة بأجهزة الخزن العشوائية RAM قريبة من بعضها البعض ، وهذا القرب سوف يؤثر سلبا على مكثفات الجوار وبالتالي تم انشاء استغلال يسمى Row hammer وهذا قد يسبب في استرداد البيانات من خلايا ذاكرة العناوين القريبة .

من هنا يجب ملاحظة الحماية الشخصية من البرامج الضارة والامان المادي كجزء مهم من الحماية الشخصية

الحرب السيبرانية

الجزء التاسع انواع البرامج الخبيثة Types of Malware وبعض النصائح للعلاج منها وتجنبها

البرامج الخبيثة تختصر بكلة malware ... Malicious software هي البرامج الضارة او اي شفرة او كود يسبب في سرقة او ضرر بالبيانات ومن هذه الانواع :-

Spyware :- برامج التجسس .

وهي برامج تثبت خلسة على اجهزة الحاسوب للتجسس على المستخدمين بدون علم المستخدم ، هذه البرامج تتجاوز الرصد والمراقبة بل ممكن جميع مختلف المعلومات الشخصية اضافة الى قيامها بعدة مهام مثل تركيب برامج اضافية ، فتح مواقع ضارة ، او تغير اعدادات الكومبيوتر .... اغلب هذه البرامج تتركب بالحواسيب بسبب البرامج والالعاب التي يتم تحميلها من الانترنيت اضافة الى التحديثات الغير موثوقة والضغط على الاعلانات ، ايضا الكثير منا يلاحظ عند تنزيل برنامج معين يتم تحميل اكثر من برنامج اضافي له ، وغيرها من الادوات المتخفية بهيئة حماية موجودة في شبكات الانترنيت . او قد يقبل المستخدم تنصيب ملفّ تجسُّس على جهازه عند تنصيبه لبرمجيّة معيّنة دون أن يدري، وذلك من خلال قبول شروط استخدام أو ترخيص هذه البرمجيّة دون قراءتها، فقد تتضمَّن هذه الشروط قبول المستخدم بعض أنشطة جمع المعلومات عن جهازه، لذا تجدر به قراءة شروط ترخيص أي برنامج يريد تثبيته على جهازه. النقطة المهمة في الحماية من هذه المضار هي تحميل برامج خاصة للحماية من التجسس ، اغلب الشركات المعروفة الخاصة بالحماية تمتلك نسخ حماية خاصة بالتجسس قد تكون مدموجة مع المضاد للفايروسات نفسة او معزول بشكل برنامج اخر مثل Kaspersky و AVG وغيرها ،

ايضا هناك طرق تقليدية منها الدخول الى register او Startup ومسح ملفات معينة من خلال اوامر regedit و msconfig . من المهم ايضا اذا احسست باي شيء الخطوة الاولى فصل الجهاز عن الانترنيت والبدء بخطوات ثابته كمسح البرامج الغير معروفة وتنصيب البرامج الحماية من التجسس وغيرها من الخطوات . غالبًا ما تجمع برامج التجسس نفسها مع البرامج الشرعية أو مع أحصنة طروادة . Trojan horses .

- ادوير Adware

:- وهي كودات تظهر داخل اعلانات تظهر بشكل تلقائي تظهر عند تصفح المواقع او حتى مع تنزيل البرامج وقد تثبت مع بعض البرامج ، هدفها الاعلان والدعاية لكن من الشائع ايضا ان تأتي الاعلانات متسللة ببرامج تجسس وقد تصنف من ضمن Spyware ، ايضا ممكن ان تكون عن

طريق البريد الالكتروني من خلال مسابقات او جوائز او انقر هنا او حمل من هنا وغيرها من الطرق ،،، حاول الانتباه على هذه الامور اضافة الى هناك اداة متوفرة لمسح adware مثل adware removal.

Bot :- شبكة الروبوت: Botnet

هي مجموعة ضخمة (يبلغ تعدادها بالآلاف وقد يصل للملايين) من الأجهزة التي تم اختراقها عن طريق الإنترنت كل واحد منها يسمى بوت تخدم مكون البوتنت أو ما يسمى بسيد البوت (Bot Master). يستخدم سيد البوت قناة أوامر وتحكم (Command and Control Channel CaC) لإدارة شبكته وتنفيذ هجماته، وتسمية البوتنت هذه مشتقة من كلمة (Robot Network) أي شبكات الروبوت حيث أن الأجهزة تخدم سيد البوت دون اختيارها، تمامًا مثل أجهزة الروبوت. وبمجرد أن ينضم الجهاز لشبكة الروبوت فإن سيد البوت يستطيع التجسس على صاحب الجهاز دون أن يشعر بذلك.

ولا يتوقف ضرر البوتنت على الأشخاص فقط، فالبوتنت أحد أهم وأخطر المشاكل الأمنية التي تواجه الشركات والدول أحيانا وأبرز مثال لذلك الهجوم الذي وقع على دولة إستونيا عام ٢٠٠٧، حيث تعطلت مواقع الوزارات والشركات لثلاث أسابيع!

لها مخاطر على الشبكة مثل التجسس وسرقة المعلومات وحجب الخدمة وارسال رسائل مزعجة هناك عدة طرق لضم الأجهزة إلى شبكة الروبوت يمكن أن نقسمها إلى مباشرة وغير مباشرة.

• الطريقة المباشرة تكون بإرسال رسائل قصيرة لمعرفة إذا ما كان هناك ثغرة يمكن استغلالها للسيطرة على الجهاز وهو ما يعرف بـ (Scanning) ومن ثم تحميل برامج التحكم.

• الطريقة الغير مباشرة تكون عن طريق استدراج الضحية لتحميل فايروس أو برامج خبيثة بالضغط على رابط وضعه سيد البوت، ورسائل البريد المزعجة (Spam) تعتبر أشهر مثال على هذه الطريقة.

ومن الطريف في الأمر أن سيد البوت قد يبيع الأجهزة التابعة له في السوق السوداء، فيعطي المشتري كلمة السر للتحكم بهذه الأجهزة، ولا تدري قد يكون جهازك يباع ويشترى وأنت لا تعلم.

كما ذكرنا سابقا أن هناك طرق مباشرة وغير مباشرة لضم الأجهزة إلى شبكة الروبوت، فلمنع الطريقة المباشرة ينصح بتحميل جدار حماية جدار حماية، والذي يمنع عمليات المسح (Scanning) التي يقوم بها مكون البوت. ولمنع العمليات الغير مباشرة ينصح بتحميل برامج حماية من الفيروسات مع خاصية التحديث التلقائي.

ومن الجدير بالذكر ام من اهم برامج الجدار الناري Firewall هي Comodo Firewall وغيرها
ومن المهم معرفة ان الفايرووول ممكن ان يكون على شكل سوفت وير او ممكن هارد وير

الحرب السيبرانية

الجزء العاشر تكملة انواع البرامج الخبيثة Types of Malware وبعض النصائح للعلاج منها وتجنبها

-: Ransom ware

هو نوع من أنواع البرامج الخبيثة التي خطت خطوات واسعة وأصبحت منتشرة في الوقت الحالي بشكل لا يصدق. تضم هذه الأنواع من الفيروسات نوعين رئيسيين هما: برامج تشفير، وبرامج حظر.

تصيب برامج التشفير جهاز الكمبيوتر، وتعمل على تشفير البيانات المهمة، بما في ذلك الوثائق والصور ومحفوظات الألعاب وقواعد الألعاب وغير ذلك. وبمجرد تشفير هذه الملفات، يتعذر فتحها ولا يستطيع المستخدم الوصول إلى أي منها بعد ذلك. وهنا يأتي دور المجرمين ليطلبوا فدية مقابل منح مفتاح التشفير لاستعادة إمكانية الوصول إلى هذه الملفات.

أما برامج الحظر، فقد سميت بهذا الاسم لأنها تمنع الوصول إلى الجهاز المصاب، وهو ما يشير إلى عدم إمكانية الوصول إلى ملفات الضحية، فضلاً عن عدم إمكانية الوصول إلى النظام بأكمله. عادة لا تكون الفدية المطلوبة لبرنامج الحظر كبيرة مقارنة بالفدية المطلوبة لبرنامج التشفير.

إذا نجحت فيروسات الفدية في الوصول إلى النظام وتشفير ملفاتك، فلن يكون بإمكانك فك تشفير الملفات الموجودة على النظام الخاص بك. أمامك خياران أساسيان هما: إما أن تستسلم وتدفع الفدية

أما الخيار الثاني والذي يعد الأفضل فيتمثل في زيارة الموقع الإلكتروني noransom.Kaspersky.com ومعرفة إذا كنا نمتلك برنامج فك تشفير يمكنه فك تشفير ملفاتك. تتوفر أدوات فك التشفير الخاصة بنا مجاناً، علماً بأننا لا نمتلك أداة مخصصة لكل فيروس فدية معتمد على التشفير.

وبناءً على ما سبق ذكره، يتعين عليك عدم الانتظار لحين حدوث أشياء لا يحمد عقباها، بل يتعين عليك أن تسير قدماً دون تردد وتتخذ التدابير الوقائية.

كيف تحمي نفسك من فيروسات رانسوم وير؟

١- تجنب فتح مرفقات البريد الإلكتروني المشكوك فيها وتجنب زيارة المواقع الإلكترونية المجهولة، كما تجنب تنزيل البرامج من أي مواقع بخلاف المواقع الإلكترونية الرسمية التابعة للمطور ومتاجر التطبيقات الخاصة به. تعلم اكتشاف رسائل الاصطياد، ولا تنقر فوق الروابط التشعبية الخاصة بها.

٢- احرص دائماً على عمل نسخة احتياطية لبياناتك. إذا كانت ملفاتك مخزنة على جهاز الكمبيوتر الشخصي وأقراص خارجية أو على السحابة الإلكترونية، فيمكنك استخدام برنامج مكافحة الفيروسات لإزالة فيروسات الفدية، ومن ثم استرجاع الملفات الخاصة بك من النسخ الاحتياطية.

٣- قم بتثبيت برنامج جيد لمكافحة الفيروسات

٤- نصح بعض خبراء أمن المعلومات بإغلاق ميزة SMB في نظام ويندوز وذلك من خلال الذهاب إلى لوحة التحكم ثم إزالة البرامج Add/Remove Programs أو Programs في ويندوز ١٠ ومن القائمة الجانبية اختر Turn Windows Features ON/OFF، ستظهر نافذة جديدة، قم بإزالة علامة صح من المربع الصغير أمام خيار SMB

-: Scare ware

كلمة scareware قد يتضح من تقسيم الكلمة مفهومها كلمة ‘‘scare’’ و هو الخوف او الرعب و ‘‘ware’’ ما تعنى منتج او سلعة و هنا المقصود بها برنامج فتعنى بالترجمة بشكل كامل ’’ برامج الرعب ’’

Fake Av و هي برامج حماية كاذبة و وهمية و هي تحاول اقناع المستخدم بشكل رهيب ان الحاسب الخاصة به و النظام لديه مصاب بفيروسات ضخمة و تظهر له تحذيرات كاذبة و وهمية تقنعه بان لديه فيروسات لا يمكن حذفها الا عن طريق برنامج الحماية الوهمي ذاك و تظهر له شكل برنامج حماية له وجه رسومية GUI و تقول له انه البرنامج قد حدد الفيروسات جميعها و قادر على ازالتها و لكن عند شرائك للنسخة الكاملة من البرنامج فقط . و اذا اردت حذف هذه الفيروسات يجب ان تقوم بعملية الشراء و كتابة رقم الفيزا الخاصة بك حتى تحصل على نسخة البرنامج مفعله و يقوم بعدها بتخليصك من هذه الفيروسات الخبيثة . لكن سيتم سرقة جميع معلومات الفيزا لديك . هذا النوع يعتبر من انواع التلاعب والتحايل .

-: Rootkit

هذا النوع من البرمجيات الخبيثة من أصعب الأنواع التي يُمكن إيجادها و التعرُف عليها ‘‘واضح من اسمها’’، فهي دائماً ما يحاول إخفاء نفسه عن المُستَخدم، نظام التشغيل، و برنامج مُقاومة الفيروسات. هذا النوع من البرمجيات يستطيع تنصيب نفسه على الحواسيب من خلال العديد من الطُرق منها الثغرات في نظام التشغيل من اهم الادوات لفحص الروتكت هو McAfee Rootkit Remover

الحرب السيبرانية

الجزء الحادي عشر تكملة انواع البرامج الخبيثة Types of Malware وبعض النصائح للعلاج منها وتجنبها

-: Virus

الفيروس عُبارة عن برنامج بسيط يقوم بعملية نسخ ذاتية و يستطيع التنقُّل من حاسوب إلى آخر. من أجل القيام بذلك، يحتاج الفيروس إلى السيطرة على ملف (exe) و إتلافه. عند تشغيل ذلك الملف، يقوم الفيروس بالانتشار و الانتقال إلى ملفات (exe) أخرى. بمعنى آخر، حتى يتمَكن الفيروس من الانتشار و السيطرة على الحاسوب، يحتاج الفيروس لمُساعدة المُستَخدم عن طريق فتح الملفات التنفيذية "ذات امتداد exe".

بُناءً على هذا الأمر، يُفَضل عدم تحميل ملفات (exe) المُنفَردة من على الإنترنت من مصادر غير موثوقة، فتوجد بالفعل أنواع من الفيروس التي تتمَكن من الدخول على الملف التنفيذي و الاستحواذ عليه بدون تغيُر حجمه إطلاقاً . اغلب الفايروسات تنتقل عن طريق CD و Flash و عن طريق رسائل البريد الالكتروني او تنصيب البرامج الغير معروفة . هناك طرق للوقاية من الفايروس

١. استخدام برامج للكشف عن الفيروسات في الجهاز.

٢. احتفظ بنسخ احتياطية من البرامج والملفات الموجودة على الحاسب.

٣. إجراء الفحص على البرامج المحملة (المنزلة) أو المنقولة من شبكة الإنترنت قبل تشغيلها.

٤. استخدام برمجيات الجدار الناري .

٥. لا تشغل أي برنامج أو ملف لا تعرف ما هو بالضبط.

٦. الحذر من رسائل البريد الإلكتروني غير معروفة المصدر وفحصها قبل الإقدام على فتحها

-: Trojan horse

حصان طروادة - حصان طروادة هو برنامج خبيث يقوم بعمليات خبيثة تحت ستار العملية المطلوبة. يستغل هذا الرمز الخبيث امتيازات المستخدم الذي يشغله. في كثير من الأحيان ، يتم العثور على أحصنة طروادة في ملفات الصور والملفات الصوتية أو الألعاب. حصان طروادة يختلف عن فيروس لأنه يربط نفسه إلى الملفات غير القابلة للتنفيذ.

-: Worms

برمجيات Worms أو كما يُطلق عليها (الدودة) تشابه بشكل كبير مع الفيروس، باستثناء أنها تستطيع إعادة نسخ نفسها بنفسها، فهي لا تحتاج إلى ملف تنفيذي للقيام بهذه العملية، فهي غالباً ما تستخدم الشبكة للقيام بذلك، مما يجعلها أخطر من الفيروسات. هذا الأمر يعني أن برمجيات Worms تستطيع إتلاف الشبكة ككُل، على عكس الفيروس الذي يُرَكز فقط على الملف التنفيذي.

يوجد نوعان من برمجيات Worms، النوع الأول يقوم بإعادة نسخ نفسه و الانتشار على الحاسوب و الشبكة، مما يعمل على تقليل سُرعة الجهاز و عملية الاتصال بالإنترنت نتيجة الاستحواذ على مقدار كبير من عرض النطاق التردُدي المُتوافر، أما بالنسبة للنوع الثاني، فيقوم هذا النوع بإعادة نسخ نفسه و القيام بالعديد من الأمور الأخرى مثل إزالة الملفات، إرسال رسائل البريد الإلكتروني، توفير اتصال لاسلكي للمُختَرق الذي يستعمله، و العديد من الأمور الأخرى.

برمجيات Worms تنتشر بسبب الثغرات في نُظم التشغيل، و بُناءً على ذلك، يُفَضل تحميل و تنصيب التحديثات المُختَلفة لنظام التشغيل في أسرع وقت مُمكن.

(Man-In-The-Middle(MITM

ويسمى ايضا هجوم الوسيط (بالإنجليزية: Man-in-the-middle attack) في التشفير و أمن الحاسوب هو نوع من الاختراق حيث يتسلل المهاجم بين متحاورين في شبكة دون علم كل منهما ، والمتحاورين يكونا اما شخصين على الشات او شخص و موقع الكتروني بحيث يقوم المهاجم بالتسلل الى الشبكة ثم التسلل الى البيانات المرسلة بين الشخصين ورؤيتها بكل وضوح .

يمكن اعتماد هذا النوع من الهجمات في تبادل مفتاح ديفي-هيلمان عند غياب عملية التعرف على الهوية (Authentication).

كيف يحدث هجوم رجل في وسط الهجوم :

لنفترض أن محمد يرغب في التواصل مع علي عبر محادثة كتابية . وفي الوقت نفسه، و احمد وهو المتسلل في يرغب اعتراض المحادثة والتنصت وربما توصيل رسالة زائفة علي . يمكنه ذلك باستخدام هجوم رجل في الوسط .

ويحدث عن غالبا عن طريق شبكات الواي فاي ضعيفة الحماية ، والتي غالبا ما يقوم المتسلل بالدخول الى شبكات الواي فاي وتسميم الشبكات بملفات تمكنه من الولوج الى اي معلومة يقوم ارسالها الى المستخدمون الحاليين في داخل الشبكة

كيف نقوم بحماية انفسنا من هذه الهجمات :

قم بتأمين الشبكة الخاصة بك برقم سري قوي وايضا استعمل تشفير الشبكة من نوع WEP2 .
اضافة الى النصائح السابقة التي تم ذكرها .

اختصرت الكثير عن هذا الهجوم لا نه يحتاج الكثير من الكلام والتفاصيل سوف اقوم بشرحة بالتفصيل فيما لحق .

الحرب السيبرانية

الجزء الثاني عشر

أعراض البرامج الضارة

بغض النظر عن نوع البرامج الضارة التي يصاب بها نظام ، فهذه أعراض شائعة للبرامج الضارة:

١-هناك زيادة في استخدام وحدة المعالجة المركزية.

٢- هناك انخفاض في سرعة الكمبيوتر. او ملاحظة تجمد او تعطل الكومبيوتر ٥-ظهور رسائل مزعجة على سطح المكتب.

٤- هناك انخفاض في سرعة تصفح الإنترنت.

٥- هناك مشاكل غير قابلة للتفسير او غير طبيعية مع اتصالات الشبكة.

٦- يتم ملاحظة حصول تعديل للملفات.

٧- يتم ملاحظة حصول حذف للملفات.

٨- ظهور برامج جديدة على الحاسوب لم يتم تنصيبها.

٩- هناك عمليات مجهولة قيد التشغيل. ممكن ان تلاحظها.

١٠- يتم إيقاف البرامج أو إعادة تكوين نفسها.

١١- يتم إرسال البريد الإلكتروني دون علم المستخدم أو موافقته

١٢- فتح نوافذ جديدة واعلانات

١٣- تعطيل برامج الحماية تلقائيا

١٤- خروج متصفحك عن السيطرة ممكن تكتب كوكل قد يتحول الى موقع ثاني ١٥- عدم فتح ملفاتك او يتم اخفاءها . ١٦- قد يخبرك اصدقاءك بانك ترسل اليهم رسائل مزعجة

وغيرها من الامور التي تحدث بصورة مفاجئة . قد يكون اسبابها امور اخرى لكن الاكثر احتمالا هي وجود برامج ضاره .

الحرب السيبرانية

الجزء الثالث عشر . طرق التسلل Methods of Infiltration

١- Social Engineering الهندسة الاجتماعية

الهندسة الاجتماعية هي فن استخدام الحنكة والتلون لخداع الشخص بحيث يقوم بشكل إرادي بكشف معلومات سرية أو بإعطاء المهاجم الفرصة للوصول للمعلومات السرية الخاصة به . . ما يطلق عليه احيانا علم أو فن اختراق العقول.

لا تعتمد أساليب الهندسة الاجتماعية على معرفة تقنية عميقة بالتالي يستطيع أي شخص يتوافر لديه قدر معين من الحنكة والدهاء القيام بهجمات الهندسة الاجتماعية.

تستخدم مصطلح الهندسة الاجتماعية عملية الخداع Phishing او التصيد الاحتيالي هو استلام رسالة خبيثة كمثال بريدًا إلكترونيًا مخادعًا متنكراً على أنه مصدر شرعي وموثوق به. هدف الرسالة هو خداع المستلم إلى تثبيت برامج ضارة على أجهزته أو مشاركة معلومات شخصية أو مالية. مثال على التصيّد الاحتيالي هو رسالة بريد إلكتروني مزورة لتبدو وكأنها مرسلة من سوبر ماركت او شركة معينة تطلب من المستخدم النقر فوق رابط للمطالبة بالجائزة. قد ينتقل الرابط إلى موقع مزيف يطلب معلومات شخصية ، أو قد يقوم بتثبيت فيروس.

من وجهة نظري البسيطة اعتبر الهندسة الاجتماعية من اخطر انواع الاختراقات لأنها لا تعتمد على امتلاكك معلومات فنية تساعدك من معرفة هجوم معين بل هي تعتمد على الخداع ، ولا نستبعد ان بعض المحترفين ومن لديه معلومة قد يكون معرض لهكذا خداع ، لا نه يعتمد على اساليب عدة وطرق كثيرة .

أغلب من يقوم بهجمات الهندسة الاجتماعية هواة وغير خبراء، لكن إن ترافقت المعرفة التقنية بأساليب الهندسة الاجتماعية فإن ذلك يشكل تهديد أكبر بكثير من مجرد المعرفة التقنية أو الحنكة بشكل فردي.

الهندسة الاجتماعية Social Engineering يمكن أن تتم عن طريق اجراء مكالمة هاتفية مخادعة أو أن يقوم مختبر الاختراق بتظاهر على أنه موظف مصرح له بالوصول للنظام او غيرها من طرق الخداع التي يتم استخدامها .

فيما يلي سرد أهم أساليب الهندسة الاجتماعية التي يعتمد عليها المهاجمون لإيقاع ضحاياهم . من المحتمل ان هناك طرق اخرى يجب عليك الانتباه اليها .

١ـ استغلال الشائعات :ـ اعتماد أغلب عمليات الاحتيال للحصول على كلمات السر أو للسيطرة على الحواسيب على تغليف البرنامج الخبيثة أو الرابط الخبيث في غلاف جذاب يغوي الضحية إلى

تشغيله أو فتحه. في اغلب الاحيان يستغل المهاجمون الشائعات او الأحداث التي تحصل في منطقة معينة بغض النظر عمن وراء الشائعات . مثلا اضغط على الرابط ادناه لمعرفة تفاصيل معينة او نتائج الانتخابات او نتائج المراحل الدراسية او الفيديو ادناه يبين حادثة معينه . بالمناسبة هناك طرق تجعل من الروابط والصور الخبيثة روابط صحيحه تظهر للعالم ، بحيث تره ان الرابط تابع لليوتيوب مثلا لكنه مغلف برابط اخر . وهذه من الامور الخطرة والتي يجب اخذ الحيطة تجاهها .

٢- استغلال العواطف والاطباع الشخصية :- حيث يتم استخدام صور او نصوص تخاطب عواطف الناس وتؤدي الى سقوطه بالفخ من الامثلة التي يستخدمها المهاجمون ... عوطف الحقد ، الانتقام ، الحزن ، الكره ، عواطف الحب ، الشوق ، الحنين يضاف اليها المشاعر الدينية والطائفية والعشائرية وغيرها ....

٣- استغلال المواضيع الساخنة:- بعكس الشائعات، المواضيع الساخنة أخبار حقيقية ولا تحتوي على تضخيم أو افتراء. تنتشر عادة بسرعة على وسائل الإعلام ذات المصداقية العالية بشكل أخبار عاجلة. كل هذا يجعلها طعما مناسبا لإيهام الضحية بأن الرابط صحيح.

٤- استغلال موضوع الامن الرقمي :- في هذا النوع من الهندسة الاجتماعية يدعي المهاجم أن رابطا ما أو ملفا ما سيسهم بحماية جهاز الضحية. في حين أنه في الحقيقة الملف ملف ملغم أو الرابط ملغم .

٥- انتحال الشخصية Identity Theft :- في هذه الحالة قد يقوم المهاجم بأنشاء حساب على فيسبوك او سكايب او غيرها بأسم مستعار او باسم مطابق لاسم صديق او شخص معين لاستغلال الثقة للحصول على معلومات معينة .

٦- اصطياد كلمات السر Passwords Phishing :- تعتمد الطريقة على إيهام الشخص المستهدف بأنه على الموقع الصحيح المعتاد حيث يدخل كلمة سره عادة للدخول إلى حسابه على الموقع (كموقع البريد الالكتروني) لكن في الحقيقة يكون الموقع موقعا "شريرا" يديره أحد لصوص كلمات السر. بالتالي إذا خدع المستخدم وأدخل كلمة سره في ذلك الموقع تصل كلمة السر بكل بساطة إلى اللص.

٧- خيانة الثقة :- في كثر من الاحيان يكون المهاجم صديقا أو زميلا للضحية. يستغل المهاجم ثقة الضحية به بسبب طبيعة علاقة الصداقة بينهما أو بسبب الزمالة في المهنة أو المؤسسة حيث يعملا. فقد يطلب المهاجم من الضحية ببساطة كلمة سر حسابه. أو يطلب منه فتح رابط معين يرسله عبر البريد الإلكتروني أو يطلب منه فتح رابط أو ملف معين يمرره له على يو إس بي ستيك USB stick. قد يقوم المهاجم بالتلصص على زميله خلال إدخاله كلمة سر حسابه. استغلال الثقة أحد أكثر أساليب الهندسة الاجتماعية شيوعا.

٨- استغلال السمعة الجيدة لتطبيقات معينة :- المهاجم في هذه الحالة يستخدم رابطا أو ملفا هو نفسه النسخة المحدثة مثلا من تطبيق معين، لكنه في الحقيقة يتضمن ملفا خبيثا ، وهذه الحال شاهدتها منتشرة كثيرا مع برامج Flash Player . وهناك أيضا حالات أخرى يقوم فيها الرابط بتحميل الملف الخبيث وتنصيبه ثم تحميل التطبيق الحقيقي وتنصيبه بصورة اوتماتيكية بحيث يعتقد الضحية أنه قام بتنصيب التطبيق الحقيقي ولا يعلم أنه قام بتنصيب الملف الخبيث. أما الحالات الأكثر دهاءا نسخة معدلة عن التطبيق ذو السمعة الجيدة يبدو ويعمل كالتطبيق الحقيقي لكنه يتضمن في الوقت نفسه جانب خبيث. وقد ذكرنا في الكتابات السابقة التركيز والانتباه على هذه الامور وتحميل البرامج من مواقعها الحقيقية والرسمية .

الحرب السيبرانية

الجزء الرابع عشر

الوقاية من الوقوع ضحية للهندسة الاجتماعية :-

بناء على أساليب الاحتيال المفصلة في الكتابة السابقة وبناء على الأمثلة المذكورة يمكن إدراج النقاط التالية كأسلوب للوقاية من الوقوع ضحية لهجوم باستخدام الهندسة الاجتماعية.

كي لا تكون ضحية سهلة راعي النقاط التالية:

• احرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لأن المهاجم قد يستخدمها لانتحال شخصيتك ومهاجمة صديق لك أو قد يستخدم المعلومات ليصيغ الهجوم عليك بشكل مقنع أكثر.

• لا تشارك أسماء أو عناوين حساباتك مع غير المعنيين وتأكد من اي شخص تضيفه الى اي قائمة لديك.

• لا تثق بأحد لان اي احد ممكن ان يتعرض لأي هجوم في اي وقت. واجعل الجميع سواسيه من الناحية الامنية.

• تحقق من شخصية من يراسلك سواء عبر البريد الالكتروني Email، أو برامج المراسلة مثل Skype، أو عبر وسائل التواصل الاجتماعي مثل فيسبوك Facebook أو تويتر Twitter.

• انظر بعين الشك إلى كل بريد الكتروني أو رسالة أو تعليق يصلك يحتوي على ملفات وروابط مرفقة. ولا تستثني اي احد.

• عند الشك برسالة ما أو بجهة اتصال مشبوهة، لا تقم بفتح الملفات أو الروابط المرفقة في الرسالة. قم بالاتصال بالقسم المسؤول في المؤسسة أو بخبير أمن المعلومات . ولا تهمل الموضوع لتفادي المزيد من المشاكل.

• في حال رغبتك بفتح أي ملف أو رابط يصلك قم قبل ذلك بالتأكد من أنه ليس خبيث عبر استخدام موقع فايروس توتال Virus Total https://www.virustotal.com. ممكن يفي بالغرض ، لكن من المهم ملاحظة ان اغلب الروابط تغلف بغلاف مواقع رسمية يجب عليك بالبدء كتابة الرابط على المتصفح يدويا للتأكد منه.

• تقييم الضرر والأشخاص المتأثرين وهذا دور المسؤولين عن موضوع امن المعلومات.

• إعلام الجهات (مؤسسات، زملاء، أصدقاء، معارف، أفراد عائلة) والتي من الممكن أن تكون قد تضررت أو تأثرت بسبب وقوع المستخدم ضحية للهجوم.

• عدم الرد والاستجابة لأي طلبات تأتي عن طريق البريد الالكتروني من اي جهة كانت تسال عن معلومات شخصية الا بعد التأكد من الامر.

• لا تدخل اي معلومات تخص ارقام الحسابات البنكية والمصرفية وكروت الشحن الا في مواقع محمية ومعروفة .

• لا تشارك في اي استبيان او اسئلة الا مع شركات رصينة ومعروفة .

• لا تحاول كتابة كلمات السر او اي معلومات شخصية داخل مذكرات او كتاب او حتى على شكل ملاحظات ملصقة مكتبية او على الحاسبة .

• لا تعطي معلومات شخصية مهمة للبرامج والالعاب الغير مرخصة او التي لا تحتاج معلومات شخصية فيها. اضافة الى عدم مزامنتك لأي امور انت لا تحتاجها.

• النقطة الاخيرة والمهمة والتي اراها في مجتمعاتنا وسببت الكثير من المشاكل ، هي عدم الانتباه على الاطفال في المنزل ، حيث اغلب الاطفال يستخدمون اجهزة الموبايل الخاصة بهم او اجهزة احد افراد العائلة وهنا الخطر الاكبر خصوصا اذا كان الجهاز متزامن مع صور شخصية او معلومات مهمة . ويبدئ الطفل بتحميل الالعاب واعطاء المعلومات الشخصية ومزامنة الموقع والصور واي شيء اخر لا جل تشغيل برنامج معين او لعبة معينه وهنا تبدء الكوارث .

ايضا لا تنسى النصائح التي قدمتها في الكتابات السابقة بصورة عامة ، قد تكون هناك نقاط اخرى لتجنب الوقوع ضحية هجوم الهندسة الاجتماعية وخصوصا الموضوع يتطور دائما ويتم استحداث طرق جديدة ، لكن حاولت ان اعطي هذه النقاط بشكل عام لا عطاء القارئ فكرة عامة عن الموضوع .

الحرب السيبرانية

الجزء الخامس عشر

الطريقة الثانية للتسلل Methods of Infiltration

Exploiting vulnerabilities الثغرات الامنية

هي احدى الطرق الشائعة للتسلل ، بصورة عامة الثغرات الامنية هي مصطلح يطلق على نقاط الضعف والمناطق الضعيفة الموجودة في الشبكة ، وانظمة التشغيل ، برامج او تطبيقات ، مواقع ويب ..... هذه المناطق تجعل من المهاجمين بابا مفتوحا للتسلل والتجسس والتدمير للأهداف التي يسعون اليها .

هناك بعض الطرق الشائعة لاستغلال نقاط الضعف .

١- جمع المعلومات حول النظام المستهدف، ممكن القيام بذلك بطرق عدة مثل

Port Scanner او Social-Engineering الهدف هي معرفة اكبر قدر ممكن حول الكمبيوتر المستهدف .

سوف ابين ما هو Port لان هذه السلسلة عملت بشكل عام لجميع المستويات ، وقد يخفى على القارئ معناه . بصورة مختصرة تخيل انك تمتلك منزل كبير ويحتوي هذا المنزل على ابواب خارجية كثيرة كل واحدة من هذه الابواب تقدم خدمة معينة لكن يجب ان تلاحظ ان كثرة الابواب المفتوحة قد تجعلك عرضة للسرقة والهجوم . هذا المثال ينطبق على اجهزة الكمبيوتر والشبكة هذه البوابات والمنافذ هي عبارة عن ممرات لتبادل البيانات ، حيث يبلغ عدد المنافذ في الجهاز الى ٦٥٥٣٥ منفذ، مرقمة ومقسمة وكل من هذه المنافذ له وظيفة او خدمة محددة او تطبيقات محددة . مثال لو فتحت المتصفح الخاص بالأنترنيت سوف تحتاج الى بورت رقم ٨٠ . ايضا كل تطبيق له بورت معين بحيث عندما تأتي بيانات الى جهاز معين على بورت معين فسوف يعرف الجهاز لأي تطبيق تنتمي هذه البيانات بعدها يقوم بأرسالها لهذا التطبيق الذي يقوم بمعالجتها . مثال عند ارسال بريد الكتروني الى شخص ما سوف يذهب مباشرا الى برنامج outlook لحفظ البريد الالكتروني . فتح هذه البورتات مثل فتح الابواب في مثالنا فهي تجعلك عرضة للسرقة والهجوم والاختراق وقد توجد هناك كثير من الادوات التي تعمل بحث لكشف البورتات المهمة المفتوحة في الشبكة Port scanner تجعل من المهاجم يجمع معلومات عنك وعن الشبكة ، هناك نصيحة مهمه ان لم تستخدم منفذ معين قم بإغلاقه حتى لاتكن عرضة لأي هجوم ،هذه بصورة مختصرة يمكن الاطلاع اكثر ومعرفة تفاصيل اعمق من خلال البحث في مواقع الانترنيت . سوف تجد طرق عدة حول كيفية غلق البورتات المفتوحة والخطرة .

هناك برنامج ومجاني خاص بفحص الشبكات والانظمة ويعتبر من اقوى البرامج التي يستخدمها الهاكرز وحتى خبراء الحماية ومدراء الشبكات اسمة network Mapper (NMAP)

بدأ Nmap كبرنامج بسيط لفحص المنافذ لكنه تطور بشكل كبير خلال السنوات الماضية وأضيفت عليه الكثير من الميزات جعلت منه Security Scanner فالبرنامج قادر على فحص نطاق شبكة كامل وفحص الأجهزة الموجودة فيها وتحديد المنافذ والخدمات التي يستخدمها والكثير الكثير من الأمور والميزات الأخرى.

٢- في الخطوة السابقة سيقوم المهاجم بجمع معلومات عن نظام التشغيل واصداره وباقي التفاصيل ، بعدها سيبدأ بالبحث عن اي ثغرات معروفة ومحددة لهذا الاصدار من نظام التشغيل او خدمات نظام التشغيل الاخرى . وعند العثور على اي ثغرة سيبدأ باستغلالها حسب طرق استغلال مكتوبة مسبقا ، ان لم تؤثر سيبدأ يفكر بكتابة كودات جديدة يمكن ان يهاجم بها .

٣- هناك طرق متقدمة للتهديد تسمى التهديدات المستمرة المتقدمة

(APT) Advanced persistent threat

هي مجموعة من العمليات والطرق المتعددة الاشكال وغالبا ما تكون طويلة الامد ومتقدمة ضد هدف محدد ، نظرا لمستوى التعقيد والمهارة المطلوبة ، غالبا ما تكون هذه التهديدات ممولة لكي يتم استخدامها في تهديد دول او منظمات لا هداف تجارية او سياسية .

الحرب السيبرانية

الجزء السادس عشر

هجوم الحرمان من الخدمة Denial of Service (DoS) attack

هجوم الحرمان من الخدمة الموزعة (Distributed DoS Attack (DDoS

تخيل انك مدير لشركة معينه وفي وقت معين يدخل السكرتير اليك لتوقيع اوراق معينه لنفرض عددها ١٠ بكل سهولة ستقوم بتوقيعها ، لو قمت بتعين موظف اخر (سكرتير) وفي نفس الوقت كل منهما سيدخل عليك ١٠ اوراق ليصبح العدد ٢٠ ورقة ايظا ستقوم بتوقيعها مع قليل من الوقت والجهد ، الان لو اصبح عدد الموظفين ١٠ سوف تلاحظ على مكتبك ١٠٠ ورقة لو قمت بتعين ١٠٠ موظف سوف تلاحظ ١٠٠٠ ورقة الى حد الوصول الى العجز والغرق بالأوراق ،،،، هكذا الحال مع DOS لكن سيتم غرق الاجهزة بكم كبير جدا من البيانات يصعب تحليلها، كل جهاز على وجه الارض له قدرة وحدود من الطاقة والسرعة والخزن لا يستطيع تجاوزها وتبقى أيضا كمية البيانات التي يعالجها محدودة ، مهما بلغت هذه البيانات من ضخامة فالحواسيب محدود بكمية معينة يستطيع معالجتها فأن زادت هذه البيانات خارج طاقته لا يستطيع تحملها وبعدها يبدأ بالبطيء والانهيار بالتالي لا يستطيع اعطاء الخدمة وهذا هو مبدأ عمل هجمات الحرمان من الخدمة بكل انواعها ، وهو اغراق الهدف المقصود بكمية ضخمة من الطلبات والبيانات حتى نصل إلى حجم اكبر من طاقة الهدف فينهار او يخرج عن الخدمة وبهذا حققت أيقاف الخدمة عن ذلك الهدف من العمل أو حرمان من يستخدم ذلك الهدف من الاستفادة منه.

ممكن ان يكون الهجوم بإغراق الاجهزة بكم من البيانات والطلبات التي يصعب تحليها الى حد ان يبطئ الجهاز ويتوقف ، تسمى Overwhelming Quantity of Traffic . او يقوم بأرسال حزم منسقة ضاره وتحمل برامج وأكواد خبيثة ليصعب فهمها وتفسيرها وبالتالي سنصل الى نفس النتيجة وهذا وما يسمى Maliciously Formatted Packets .

ظهرت بعض الحمايات التي تصد من هجمات الحرمان من الخدمة والتي تعمل على وضع قواعد وسياسات بكمية معينة من الطلبات يمكن استلامها ، على سبيل المثال يمكن أن يستلم الهدف ١٠ طلبات في الثانية الواحدة من المستخدم ، إذا زادت هذه الطلبات فأنه يتم تجاهلها ولا يتم قبلوها أو الانشغال بمعالجتها ، ولزيادة الحماية احياناً يقوم الهدف بشكل تلقائي بحظر ذلك المهاجم الذي يحاول أن يرسل العديد من الطلبات والبيانات ولا يتم استلام منه أي طلبات اخرى.

لنوضح الامر اكثر . السيرفر هنا يمتلك حماية رائعة بسببها لم يستطيع احد تنفيذ الهجوم وارسال عدد كبير من الطلبات ، بعد وضع الحماية وتحديد ١٠ طلبات في الثانية لكل مستخدم ، في هذه

الحالة اذا كان هناك ٥٠٠٠٠٠ مستخدم يسمح لكل مستخدم ١٠ طلبات العدد الكلي تقريبا = ٢٥٠٠٠٠٠٠ طلب في الثانية هذا رقم مخيف جدا ولا يمكن لأي سيرفر تحمل هذا الكم من الطلبات في حالة كانت الطلبات من اجهزه تحمل خط انترنت سريع وتنقل باندويث عالي على السيرفر سوف ينهار في الفور ، ولكن السؤال الآن كيف للمهاجم أن يحصل على ٥٠٠٠٠٠ مستخدم ويستغلهم للهجوم ؟ الآن هجوم DDOS يقصد به استغلال كمية من الناس في مساعدته في تنفيذ هجمات الحرمان من الخدمة وتنفيذ الهجوم على أي هدف يريد لا يوجد أي شيء يمكنه إيقافك ، لأنك في الواقع لم تقوم بأي شيء غير شرعي على حسب قواعد الجدار الناري للسيرفر ، تم تحديد ١٠ طلبات نحن لم نخرج عن القاعدة طلبنا ١٠ طلبات فقط لكن الخدعة هي ان هناك ١٠ طلبات فقط من الألاف من المستخدمين . وهذا ما يسمى (Distributed DoS Attack (DDoS الحرمان من الخدمة الموزعة ، اذ يقوم المهاجم باستخدام مصادر متعددة تساعده في الهجوم .

حيث يتم استغلال الاجهزة عن طريق البوت نت BOTNET لإغراق خوادم مواقع معينه بطلبات استعراض الصفحات مثلا ، مما يجعل الطلبات العادية للمستخدمين غير قابلة للتنفيذ نتيجة الضغط الهائل على الخوادم.

ولكي تتم إضافة حاسوب إلى شبكة بوتنت، فإن على المخترق أولا أن يتمكن من التحكم به، من خلال الثغرات في نظام تشغيل الحاسوب لتحميل برمجيات خبيثة تسمح للمخترقين الوصول عن بعد بشكل دائم إلى الحاسوب. وقد تكلمنا سابقا عن البوت نت وماهي مخاطر وطرق تجنبه .

أنواع هجمات الحرمان من الخدمة :

: Application layer DDOS attack

بعض هذه الهجمات مثل:

- HTTP GET DOS ATTACK •
- HTTP POST DOS ATTACK •
- HTTP Slow Read •

وهناك أنواع أيضا لـ SMTP , DNS وأنواع اخرى.. الخ

:Protocol DDOS attack

لو حاولنا تقسيم الهجمات من حيث نوع البيانات المرسلة سيتم تقسيمها الى

١- UDP Flood

٢- ICMP (Ping) Flood

٣- SYN Flood

٤- Ping of Death

ايضا هناك ادوات كثيرة لتنفيذ هجمات الحرمان من الخدمة وهناك طرق حماية من الهجمات ودراسات حول وضع قواعد للجدار الناري للمنع والتقليل من هذه الهجمات ايضا هنالك بعض الأدوات المساعدة للحماية من هجمات الحرمان من الخدمة . مثل CSF Firewall و clouderflare وغيرها من الادوات والاجهزة المستخدمة في الحماية ، الموضوع كبير جدا ومتشعب اتمنى ان اكون قد اعطيت الخطوط العامة له .

الحرب السيبرانية الجزء السابع عشر

التدابير والنصائح الامنية المهمة التي يجب اخذها بنظر الاعتبار تجاه شركتك او منظمتك او حتى بصورة شخصية.

اغلب مسؤولي ومدراء الشركات ليست لهم معلومات كافية عن الامن الرقمي والمخاطر التي تأتي من خلاله ، ايضا انشغال المدراء بأمور اخرى في تصورهم اهم من الامن الرقمي يجعلهم هم وشركتهم عرضة للهلاك . هذا الامر مهم ويجب ملاحظة ويجب عمل فريق مشترك من الاشخاص المعنين وتحديد جميع النقاط والمسؤوليات ، سوف اسرد لكم بعض التدابير لتكون بمثابة دليل للشركات يمكن ان يتم تطبيقها لتفادي بشكل كبير الهجمات التي من الممكن التعرض لها . ايضا مهمه جدا من الناحية الشخصية.

١- تحديد نقاط الضعف الخاصة بك :- في البداية يجب عليك تحليل البيانات الخاصة بشركتك وتقسيمها بما يناسب اقسامها ، هذه العملية تتم عن طريق فرق متخصص في مجال امن المعلومات لتحديد نقاط الضعف التي ممكن ان تستغل .

٢- تحديث دوري للبرامج وانظمة التشغيل من مصادرها الرئيسية ، وهذا يعتمد على شراء نسخ اصلية.

٣- تنصيب برامج مكافحة الفايروسات والتجسس على حاسبات الشركة مع مراعاة تحديثها دوريا .

٤- تجهيز واعداد جدار حماية للشبكة ، حيث تعمل الجدران النارية على فصل اجزاء مختلفة من الشبكة مما يعطي صلاحيات لكل جزء اضافة الى مرور البيانات المرخصة وغيرها . سواء كان الجدار الناري برنامج منعزل او الذي يأتي مع انظمة التشغيل.

٥- عدم اخراج اجهزة اللاب توب خارج المكتب الا اذا كانت محمية ولا تحتوي على معلومات حساسة فقط حتى لا تكون عرضة للسرقة .

٦- اجراء النسخ الاحتياطية للبيانات الهامة .قم بنقل ملفاتك دوريا في مكان ثاني امن بعيد عن اي اتصال خارجي .

٧- اذا فكرت بنسخ ملفاتك في Cloud يجب ان تراعي الشركة التي سوف تشترك معها من ناحية سمعتها ، ايضا يجب ان تشفر الملفات الخاصة بك عند ارسالها الى الكلاود عن طرق كثير من البرامج الموجودة والمتوفرة .

٨- كلمات المرور مهمه جدا ، حاول ان تختار كلمات مرور مختلفة لأي موقع او خدمة من الخدمات ، تغير كلمات السر بشكل دوري ، اختيار كلمات سر قوية.

٩- التحقيق باستخدام خطوتين لفتح اي حساب لديك .

١٠- اعطاء الصلاحيات : يجب عليك ان تعطي الصلاحيات للموظفين للدخول الى حسابات معينه ومنع الاخرين من ذلك .

١١- التركيز على حماية شبكة الواي فاي حيث يجب عليك ان تتأكد من تشغيل جمع ميزات الامان وايضا الامور التي تقيد الوصول لاسلكيا الى الشبكة .

١٢- تصفح الانترنيت بأمان ، هناك طرق تجعل من اتصالك مشفر ومضمون الخصوصية داخل الشبكة العنكبوتية ، ان من افضل الطرق التي تشفر اتصالك استخدام برامج VPN لمنع ظهور نشاطك داخل الانترنيت بالرغم من ان VPN له موثوقية وامان وغني بعدة مميزات لكن تكلفة الاموال الخاصة بالاشتراك السنوي الخاص به قد يراها البعض مكلفة لكن بالحقيقة هي بسيطة مقابل الامان الذي توفره .

١٣- اضافة مميزات الامان الخاصة بالمتصفح . هناك ادوات كثيرة تضيف الامان لأي متصف تستخدمه ممكن ان تجدها من خلال الموقع الرسمي للمتصفح نفسة .

١٤- تقيد سياسة الموظفين الذين يعملون في الشركة عن بعد حيث يكون اتصالهم والوصول الى البيانات الخاصة بالشركة عن بعد .

١٥- حماية ملفات العملاء ، وهذه النقطة جدا مهمه في حال كان الموقع الخاص بك يعرض بضائع يتم تسويقها عن طريق الموقع الالكتروني بمعنى يتم دفع الاموال خلال الموقع نفسه .

١٦- اهم نقطة في نظري الشخصي هي تطوير الكادر المسؤول داخل الشركة بأفضل الدورات الحديثة والمتقدمة ، والاهم هو زرع ثقافة الامن الالكتروني داخل الموظفين او في كل مكان داخل عملك ،والعمل على توعية شاملة للجميع ، في كيفية التعامل مع الملفات والبريد الإلكتروني والروابط المزيفة والبرامج الضارة وغيرها .

١٧- اختيار الموظفين الموثوقين والعمل على متابعتهم وتقديرهم

١٨- التامين الرقمي ايضا له علاقة وطيته بالأمن الخاص بالشركة والبناية والدخول للغرف والاماكن المهمة ، يجب اخذها بنظر الاعتبار .

١٩- يفضل ان تقوم بعمل بلوك الى جميع البريد الالكتروني المرسل اليك والذي يحتوي على اعلانات وامور مزعجة من اشخاص غرباء .

٢٠- اذا كنت صاحب شركة او مؤسسة يجب عليك ان تفكر في اجهزة IDS/IPS لما تملك من مميزات في تحليل والكشف والمطابقة وغيرها من الامور . نعم قد يكون مكلف لكن مقابل القيمة الامنية التي يقدمها .

٢١- ايضا عدم الضغط على اي روابط غير متأكد من جهة ارسالها او منها اصلا .

٢٢- لا تشتري اي شيء من المواقع الغير معروفة او الغير مؤمنة .

٢٣- حاول ان لا تنسى غلق اجهزتك عند عدم استخدامها .

امر مهم تضيفه سيسكو هو ان IOT (انترنيت الاشياء) له مخاطر اكبر من الحواسيب واجهزة المحمول بسبب ان اجهزة IOT لها برامج ثابتة اصلية لا تحدث بشكل دوري مثل اجهزة الحواسيب والمحمول بالتالي يعرضها لوجود ثغرات امنية خصوصا ان اغلب الشركات المصنعة لأنترنيت الاشياء تعتمد على الشبكة المحلية للأنترنيت بالتالي فأنها تتيح الوصول الى الشبكة والبيانات المحلية الخاصة بالعميل . هنا تنصح سيسكو باستخدام شبكة معزولة خاصة بأجهزة انترنيت الاشياء . حسب اعتقادي ان هذا الامر مؤقت حيث ان انترنيت الاشياء الان في مرحلة الانشاء والتطوير والبحوث بالتالي سوف تأخذ هذه المشكلة وتوضع لها الحلول . الموقع التالي يعمل مسح لأجهزة انترنيت الاشياء على الانترنيت https://www.shodan.io/ .

النقاط اعلاه ضرورية جدا نعم قد يكون بعضها مكلف لكن تحسب الامور حسب وضعية واهمية المكان الذي انت فيه وماهي الحاجة منه .

الحرب السيبرانية

الجزء الثامن عشر

ادارة كلمات المرور للحسابات .

اغلبنا لديه اكثر من حساب على الانترنيت كان يكون حساب بريد الكتروني او حساب لمواقع تواصل اجتماعي مثل الفيس بك وغيرها من المواقع ، هناك خطا شائع لدى الكثير وهو استخدام نفس كلمات المرور لجميع الحسابات التي يمتلكها لتجنب النسيان ، مع استخدامك لنفس كلمات المرور ستكون انت وبياناتك عرضة للمجرمين السيبرانيين ، حيث يشبه استخدامك استخدام نفس المفتاح لفتح جميع الابواب المغلقة لمنزلك . فو تعرض اي حساب الى سرقة ستتعرض باقي الحسابات الى ذلك .

اغلبنا يعاني من حفظ كلمات المرور لعدة مواقع او يصعب عليه استخدام كلمات مرور قوية وذو تنوع مختلف من الاحرف والارقام والرموز .

ان احد الحلول لهذه المشكلة هي استخدام برامج لإدارة كلمات المرور ، حيث تقوم هذه البرامج بتخزين وتشفير كل كلمات المرور المختلفة والمعقدة الخاصة بك . يمكن لهذه البرامج مساعدتك لتسجل الدخول الى حساباتك عبر الانترنيت تلقائيا .م عليك سوى تذكر كلمات المرور الرئيسية للوصول الى مدير المرور وادارة جميع حساباتك وكلمات المرور الخاصة بك .

هناك أيضاً مشكلة قد تواجهنا مع برامج مدير كلمة المرور فكلما اعتمدت عليها زادت احتمالية نسيان كل كلمات المرور فيما عدا كلمة المرور الرئيسية. فماذا لو أردت الدخول على أحد الحسابات الخاصة بك من خلال جهاز شخص آخر؟ على سبيل المثال، قد يحدث ذلك إذا كنت تود عرض بعض الصور لأحد الأصدقاء وهو في مكانه من مساحة تخزين سحابية أو كنت ترغب في اللعب معه عبر الإنترنت على أحد الألعاب المرتبطة بحسابك على منصة ستيم. قد لا تستطيع تذكر كلمة المرور الخاصة بهذه الخدمة، كما أن تثبيت برنامج مدير كلمة المرور على جهاز الكمبيوتر الخاص بشخص آخر أو على الهاتف الذكي ليس فكرةً جيدةً.

سيساعدك برنامج مدير كلمة المرور Kaspersky Password Manager في حل هذه المشكلة. اذ يحتوي على واجهة ويب يمكنك الوصول إليها من على حساب My Kaspersky الخاص بك. حيث يمكنك إدخال كلمة المرور الرئيسية إلى هذا الحساب لتعرض قائمة من كلمات المرور الخاصة بك. فقط كل ما عليك هو نسخ كلمة المرور الصحيحة ولصقها في الخدمة السحابية أو منصة "ستيم" أو غيرها. وأنت لست في حاجة إلى تثبيت برنامج مدير كلمة المرور Password Manager على جهاز أحد الأفراد الآخرين، حتى لا تتثنى له فرصة الوصول إلى كلمات المرور الخاصة بك (وإذا اضطررت لذلك فأنت في حاجة إلى تسجيل الخروج عند الانتهاء).

ايضا هناك نصائح لاختيار كلمة مرور جيدة تعطى وتوصي بها اغلب الشركات من ضمنها .

١- عدم استخدام كلمات شائعة او معروفة .

٢- لا تستخدم اسماء اجهزة الكومبيوتر او اسماء الحسابات.

٣- استخدم كلمة مرور من ١٠ احرف او اكثر . تحتوي على احرف كبيرة وصغيرة ورموز .

٤- حاول تفعيل خدمات الموثوقية لكلمات المرور .

٥- لا تستخدم نفس كلمات المرور للحسابات كما ذكرنا .

الحرب السيبرانية

الجزء الثامن عشر:

الفريق الاحمر والفريق الازرق

تتوجه المجتمعات التقنية الان الى استعمال فرق خاصة بحماية المؤسسات والمنظمات من الهجمات السيبرانية ، وسأتكلم على أهم فريقين في مجال الامن السيبراني.

ينقسم أعضاء الفريق الأمني إلى مجموعتين : فريق أحمر وفريق أزرق.

الفريق الأحمر يلعب دور القوة المعادية للشركة أو المؤسسة

والفريق الأزرق يلعب دور المُدافع عن المنظمة.

هدف الفريق الأحمر هو العثور على نقاط الضعف في أمن المنظمة واستغلالها.

يقوم الفريق الأزرق بالدفاع عن المنظمة أو المؤسسة من خلال إيجاد نقاط الضعف والتصحيح والاستجابة للاختراقات الناجحة.

ما هو الفريق الأحمر Red Team

يمكن اعتباره الفريق المهاجم، عبارة عن فريق يتكون من مجموعة مستقلة من الهاكر أصحاب القبعات البيضاء، تلعب دور المهاجم أو الهاكر وتقوم بمحاكات دور المخترقين، وتطبيق ما يسمى اختبار الاختراق، لاكتشاف الثغرات وايجاد الاستغلال المناسب لها، وهذا تحت برنامج خاص بالتمرين يعمل على المحاكاة والتدريب، حيث يتم تقسيم أعضاء المنظمة إلى فرق للمنافسة في التمارين بمجال أمن المعلومات ، بحيث يتم تصميم التمرين لتحديد نقاط الضعف وإيجاد ثغرات أمنية في البنية التحتية للشركة بالإضافة لتدريب موظفي الأمن كذلك.

وهذا يشكل تحدى للمنظمة بدافع تحسين فعاليتها بطريقة غير مباشرة. المخابرات الأمريكية ومؤسسات خاصة مثل IBM وكالة المخابرات المركزية استخدمت الفرق الحمراء لفترة طويلة لحماية البنية التحتية الخاصة بها من الاختراق.

تبني عقلية المهاجم أو الهاكر للشركات يقوم بتعزيز فرصها بشكل فعال في تأمين نفسها ضد التهديدات المتغيرة والمتجددة باستمرار.

من ناحية أخرى ، يتعين على أعضاء الفريق الأحمر أن يكونوا على دراية كاملة لأي منافس محتمل لـ TTP (التكتيكات والتقنيات والإجراءات) ، والتي من المتوقع أن يكتشفها الفريق الأزرق ومواجهتها.

الإبداع هو مفتاح الفريق الأحمر

فأنت تحاول باستمرار التفكير خارج الصندوق حول كيفية منع التهديدات باستخدام مجموعة واسعة من الأدوات.

أحد الأمثلة على ذلك هو القرصنة الأخلاقية وهي استراتيجية أساسية للفريق الأحمر حيث تساعد على حماية أنظمة الشركة بشكل أفضل من خلال التفكير كالمخترقين للعثور على نقاط الضعف في الأنظمة.

مجالات الفريق الأحمر

Network Pentest

Web app Pentest

Exploit Writing

Python Security

ماهو الفريق الأزرق Blue Team

يمكن اعتباره الفريق المُدافع، يتضمن عمل Blue Team الوصول إلى بيانات السجل ، باستخدام SIEM ، وتجميع معلومات استخباراتية للتهديدات المحتملة، وإجراء تحليل تدفق البيانات وحركة المرور...، يمكننا مقارنة مهمتهم بإيجاد الإبرة في كومة قش ...

الفريق الأزرق : هو مجموعة مكونة من الأعضاء الذين يقومون بإجراء تحليل لنظم المعلومات لضمان الأمن وتحديد عيوب الأمن ونقاط الضعف، والتحقق من فعالية كل التدابير الأمنية وللتأكد من أن جميع التدابير الأمنية بأنها فعالة.

يجب ألا يعتمد الفريق الأزرق على التكنولوجيا وحدها فلا يمكن الاستغناء عن الحدس البشري والخبرة والمهارات والذكاء و تقنيات الهندسة الاجتماعية (مثل التصيد العشوائي). يجب أن يعترض الهجوم ويمنع الفريق الأحمر من الوصول إلى هدفه.

مجالات الفريق الأزرق

Linux Forensic

Windows Forensic

Network Forensic

Malware Analysis

كما رأينا ، يتعين على الفريقين إنجاز مهام معقدة - لكن السؤال هو:

ما الذي يجعل أنشطتهما فعالة؟

الفريق الاحمر والفريق الازرق ما الذي يجعل أنشطتهما فعالة؟

عنصر أساسي لنجاح الفريق الأحمر هو قدرته على تبني عقلية عدوانية أو وجه الهاكر الحقيقي. لذلك ، لا ينبغي اختيار أعضائها من بين الذين ساهموا (أو ما زالوا يساهمون) في الدفاع عن البنية التحتية.

هناك حاجة إلى "عقلية خارجية" ، ويمكن معالجة هذه الضرورة بشكل أفضل من خلال الاعتماد على المساعدة الخارجية أو الأفراد غير المشاركين.

يقوم المهاجم الحقيقي أي الهاكر بالتغاضي عن أي قاعدة أو آداب أو قضية أخلاقية (فقد يكون إرهابيًا أو مجرمًا أو حتى موظف سابق مستاء) ولهذا قد يكون تبني مثل هذه العقلية أمرًا صعبًا.

يجب إجراء اختبار اختراق فعلي، كلما كان ذلك ممكنًا ، ويجب أن تركز أيضًا على أضعف نقطة في النظام الأمني ونعني بذلك العنصر البشري (أي الموظفين).

قد تتاح للفريق الأحمر فرصة مراقبة استجابة الموظفين لبعض المدخلات من مرفقات البريد الإلكتروني الضار ، ومحرك أقراص USB وفي مرافق HQ (مواقف السيارات أو غرفة الاستراحة).

إذا كانت الشركة قد أصدرت بالفعل سياستها الأمنية الخاصة ، فستكون جهود الفريق الأحمر قادرة على تقييم معرفة الموظفين ووعيهم وانضباطهم ، وكذلك قدرة الشركة على إنفاذ القواعد.

في حين يجب عدم إهمال السلامة الجسدية للموظفين وسلوكهم، ولا ننسى الشبكات اللاسلكية فهي تشكل ساحة معركة أخرى تستحق أقصى درجات الاهتمام. لأن أحد أكثر التهديدات خطورة على

الشبكة اللاسلكية هو ما يسمى Wardriving ، الذي يمهد الطريق لمتابعة الأنشطة الضارة والاستغلالية بطريقة عشوائية. ومن لا يعرف هذا الهجوم سأقوم بتعريف بسيط له

Wardriving هو عملية البحث عن شبكات Wi-Fi اللاسلكية بواسطة شخص عادة في مركبة متحركة ، باستخدام كمبيوتر محمول أو هاتف ذكي.

الفريق الأرجواني

نظرًا لأن كل فريق يسعى جاهداً للوصول إلى أهدافه الخاصة - وعند تعريفه - مؤشرات الأداء الرئيسية الخاصة به - فإن جعل الاثنين يعملان بشكل متآلف ليس بالأمر السهل.

ومع ذلك ، فإن الهدف النهائي هو مساعدة الأعمال على تحقيق مستوى أعلى من الأمان ؛ سيتعين على هذا الممثل الجديد ، الفريق الأرجواني، تعظيم وضمان فعالية نشاط المجموعات "التقليدية" ، من خلال الجمع بين الروتين الدفاعي للفريق الأزرق ونقاط الضعف التي كشف عنها الفريق الأحمر ، وبالتالي إنتاج جهود متماسكة تهدف إلى تعظيم النتائج ومؤشرات الأداء الرئيسية والقياسات التجارية

الحرب السيبرانية الجزء عشرون

مصطلحات مهمة في اختبار اختراق المواقع والسيرفرات

هذا الموضوع يمكن اعتباره مدخل بسيط ومعلومات اولية الى عالم اختبار اختراق المواقع والسيرفرات، ويتوجب على من يريد الدخول بهذا المجال أن يتعرف على هذه المصطلحات المهمة والتي تمثل نقطة البداية أو الأساس.

١- ماهو السيرفر أو الخادم أو الملقم

عبارة عن جهاز كمبيوتر ذو مواصفات قوية ومتخصص في أداء وظيفة معينة وتلبية الطلبات التي ترده من حواسيب أخرى على الشبكة بحيث يتميز بعدد كبير من الرامات أكثر ومساحات اكبر من وحدات التخزين Harddisk ووحدات المعالجة البروسيسور وهو أيضا عبارة عن منظومة متكاملة متصلة بشبكة الانترنت.وتتميز تلك الخوادم بقدرتها العالية وسرعتها في معالجة البيانات وأيضا له القدرة على العمل بشكل متواصل دون توقف

أنواع السيرفرات حسب الوظيفة ولأنظمة المشغلة

كل خادم يختلف عن غيره في نوع الوظيفة المطلوبة منه

من حيث الأغراض هناك الأتي :

سيرفر استضافة مواقع WebHosting Server

سيرفر استضافه حسابات مثل : Email- FTP - SSH - MySQL

سيرفر تحميل أو بروكسي

من حيث أنظمة التشغيل :

Widnows server مثل: windows server 2016 , windows server 2012 , windows server 2008

توزيعات Linux مثل توزيعات سانتوس وديبيان وأوبنتو.

توزيعة FreeBSD

٢- ماهى الداتا سنتر أو مركز البيانات

عبارة عن غرفة ضخمة تتكون من رفوف وممرات تحتوي على الخوادم بمعنى أخر مكان مجهز بوسائل الحماية والتبريد وأيضا متصل بالانترنت بأفضل السبل ويستفاد منه في حفظ كميات ضخمة جدا السير فرات أو الخوادم التي تقوم بتخزين ومعالجة كميات ضخمة جدا من البيانات وربطها ببعضها البعض وتوصيلها بشبكة الانترنت.

٣- ماهو vps

عبارة عن سيرفر شخصي وهمي أو Virtual Private Server بمعنى أخر عبارة عن تقسيم السيرفر إلى مجموعة من الأقسام لكل قسم خصائص وموارد خاصة به ويتم ذلك عن طريق برامج خاصة بالتقسيم والتوزيع بحيث إن كل قسم منفصل ومعزول عن القسم الأخر وله الحق في التحكم الكامل في المساحة المخصصة له من حيث تنصيب البرامج أو إزالتها.

٤- ماهو الرسيلرReseller

هو جزء من السيرفر ويستخدم لاستضافة عدة مواقع باستضافة واحدة لكن بلوحة تحكم منفصلة او تقسيمها من شركات الاستضافة الصغيرة والمبتدئة لخطط استضافة واعادة بيعه بالتجزئة إلى عملاء جدد. من خلال لوحة الادمن WHM يمكنك إنشاء، تشغيل، وقف، حذف و ترقية حسابات العملاء.

٥- الدومين أو النطاق

يعرف ايضا بنطاق الموقع، هو عنوان الموقع الذي تكتبه فى المتصفح للوصول اليه كمثال لذلك http://www.site.com

٦- ماهي الاستضافة أو الهوست

هي عبارة عن شركة تقوم بشراء سيرفر بمساحة معينة موجود على داتا سنتر ويمكن أن تجد شركات استضافة تملك داتا سنتر خاص فيه مثل استضافة موقع Google طبعا الاستضافة هي التي تملك المساحة الخاصة بك لترفع عليها ملفاتك وموقعك وقد تستخدم عدد من الطرق والمميزات مثل إعطائك vps أو رسيلر أو مساحة عادية على السيرفر.

٧- ماهو ip بروتوكول الإنترنت Internet Protocol

ip عبارة عن عنوان خاص لكل جهاز على الشبكة يمكن تشبيهه برقم الجوال الخاص بكل شخص، وعن طريقه يتم ربط الجهاز بالشبكة وباجهزة أخرى مثلا **١٠٥.١٠٤.٥٥.٦٦**.

الرقم الاول يعبر عن الدولة الموجود بها الجهاز والرقم الثاني المدينة والثالث المستضيف او شركة الاتصال والرقم الاخير رقم الجهاز وهناك نوع أخر داخلي فقط على الشبكة مثل ١٠.٠.٠.١ او ١٢٧.٠.٠.١ أو ١٩٢.١٦٨.١.١.

ماهي فائدة ip

الهدف منه وهو اعطاء كل مستخدم للأنترنت عنوان يمكن الوصول له وارسال المعلومات واستقبالها وايضا له فوائد كبيرة منها ان تبحث من خلال البرامج ومنها Advanced Port Scanner ولها انواع عدة وفائدتها تبحث لك عن منافذ ports لأي ip ويمكنك عن طريقها اختراق الاجهزة او تزودك بمعلومات عن جهاز الضحية مثل بلده أو مزود الخدمة ...

٨- ماهو DNS

Domain Name System هو بمثابة دليل الهاتف بالنسبة لمواقع الإنترنت، دليل الهاتف يجمع بين اسم الشخص ورقم هاتفه، أما DNS فيجمع بين اسم النطاق Domain Name وعنوان IP الخاص به.

٩- ماهي البروتوكولات Protocols

هي القوانين التي تحكم عالم نقل واستقبال البيانات من الجهاز الى الشبكة الى السرفر والعكس مع اختلاف انظمة التشغيل واختلاف برمجتها وترميزها وهي التي تسمح لكل جهاز يقوم بأرسال أو استقبال البيانات بفهم المرسل اليه او المستقبل منه.

ماهي وظيفة البروتوكولات وهل لها انواع ؟

تقوم البروتوكولات على تقسم وتجزئة البيانات على شكل حزم صغيرة وتقوم بترقيمها ثم تقوم بأرسالها للجهاز المستقبل الذي يقوم دوره بتجميع تلك الحزم داخل الذاكرة وعند استكمالها يقوم بعرضها بالشكل الصحيح على الشاشة وتختلف انواع البروتوكولات على حسب عملها وكمثال لها.

Application Protocols برتوكولات التطبيقات وهذه البرتوكولات تقوم بتبادل الملفات وقواعد البيانات والبريد الإلكتروني ومواقع الأنترنت وعدد كبير من هذه البرتوكولات ومن أشهرها

DHCP · DNS · FTP · HTTP · Gopher. IRC · POP3 · RTP · SIP · SMTP · SNMP · SSH · TELNETRPC · RTCP · RTSP · TLSSDP · SOAP · GTP · · STUN · NTP

من اهم البروتكولات التي سنتعامل معها في المواقع هي بروتوكول ftp الذي يستخدم للاتصال بالموقع او السيرفر ورفع الملفات او حذفها. وبروتوكول TELNET وبروتوكول HTTP ايضا هوا بروتوكول للنقل الملفات ولكن يقوم بعرض البيانات على شكل صفحات ويب وهوا البروتوكول المستخدم في التصفح للمواقع ايضا بروتوكول SMTP و POP3 يستخدم لنقل واستقبال الرسائل والايميلات وبروتوكول SSH .

١٠- ماهي المنافذ او البورتات Ports

يمكن وصفها ببوابات للجهاز وهناك عدد من المنافذ في كل جهاز ولكل منها غرض محدد تلك المنافذ هيا التي تسمح بنقل البيانات سواء استقبال او ارسال، وكل خدمة لها بورت معين داخل النظام.

مثلا: بورت 21 هو لخدمة نقل الملفات الى الموقع. والبورت 80 يستخدمه المتصفح

١١- لوحة تحكم cpanel

هي لوحة تحكم تعتمد على الويب وتحتوي على جميع المميزات التي تسمح لك بإدارة النطاق عبر واجهة ويب، وامكانية تثبيت السكربتات ، ومسؤولية إدارة موقعك على الإنترنت بشكل اسهل واسرع، ولديك ايضا إمكانية إدارة جميع واجهات البريد الإلكتروني، إدارة الملفات، النسخ الاحتياطي، FTP، برمجيات CGI، و جميع إحصائيات الموقع وايضا قواعد البيانات وغيرها من الامكانيات الجبارة.

١٢- ماهي قواعد البيانات (Database) الفائدة منها وماهي امثلتها

هي مجموعة من عناصرِ البيانات المنطقية المرتبطة مع بعضها البعض بعلاقة رياضية، وتتكون قاعدة البيانات من جدول واحد أو أكثر من جدول. ويتكون الجدول من سجل (Record) أو أكثر من سجل ويتكون السجل من حقل (Field) أو أكثر من حقل ومثال على السجل :السجل الخاص بموظف معين يتكون من عدة حقول مثل رقم الموظف - اسم الموظف - درجة الموظف - تاريخ التعيين - الراتب - والقسم التابع له...إلخ من بيانات الموظف تخزن في جهاز الحاسوب عَلى نحو

منظّم، حيث يقوم برنامج (حاسوب) يسمى محرك قاعدة البيانات (Database Engine) بتسهيل التعامل معها والبحث ضمن هذه البيانات، وتمكين المستخدم من الإضافة والتعديل عليها..يتم استرجاع البيانات باستخدام أوامر من لغة للاستعلام (Query language)، حيث تعتبر معلومات تساعد في عملية اتخاذ القرار. بعض اللغات أو الأمثلة على قواعد البيانات :

MySQL وهي أشهرها على الإطلاق

أكسس تستخدم عادات داخل أنظمة الوندوز

PostgreSQL

قاعدة بيانات بيركيلي

Borland Interbase

Microsoft SQL Server

Informix

B-trieve

IBM DB2

Sybase

١٣- ماهي لغة php وكيف يتم التعرف عليها

بي إتش بي PHP: Hypertext Preprocessor الصفحة الرئيسية الشخصية كانت مجموعة من التطبيقات التي كتبت باستخدام لغة بيرل أطلق راسموس اسم Personal Home Page Tools ("المعالج المسبق للنصوص الفائقة") هي لغة برمجة نصية صممت أساسا من أجل استخدامها لتطوير وبرمجة تطبيقات الويب. كما يمكن استخدامها لإنتاج برامج قائمة بذاتها وليس لها علاقة بالويب فقط. يتم التعرف عليها من خلال تواجد العلامتين <؟ ؟> بداية ونهاية الكود.

١٤ - ماهو السكربت ؟

هو مجموعة من الاكواد المجمعة والتى تكون برنامج من أمثلة الاسكريبتات المكتوبة بلغة php مثلا اسكريبت المنتديات VB و المدونات والمواقع مثل جوملا ووردبريس.

١٥- ماهو السيرفر الشخصي (localhost)

عبارة عن برنامج يقوم بتحويل جهازك الى سيرفر او خادم مصغر بحيث يسمح لك بتطبيق وتشغيل السكربتات المبرمجة بلغة php

وايضا يسمح لك بتنصيب تلك السكربتات وربطها بقاعدة بيانات خاصة داخل السرفر الشخصي ومن هنا ظهرت اهميته الكبرى

من حيث انه يساعد المبرمجين والمطورين ومكتشفي الثغرات في تصفح وفحص السكربتات بكل سهولة ويسر

١٦- بعض اللغات وكيفية التعرف عليها وفوائد اللغات المختلفة

اللغة الاولى بعد لغة php هيا perl (البيرل) يتم التعرف عليها بمجرد رؤية السطر الاول تجد هذا الكود

usr/bin/perl/!#

وتجد الملفات المبرمجة بتلك اللغة بأمتداد pl

اللغة الثانية من حيث القوة لغة Python (البايثون) حلت الكثير من مشاكل التخطي في اغلب السيرفرات بعد منع الكثير من الدوال الخاصة بلغة php وايضا عدم التصريح للتشغيل ملفات perl ويتم التعرف عليها من خلال السطر

usr/bin/python/!#

وتجد الملفات المبرمجة بتلك اللغة بأمتداد py

اللغة الرابعة وهي ruby (روبي) يكثر استخدام هذه اللغة في برمجة اسكربتات الثغرات ويتم التعرف عليها من السطر

usr/bin/ruby/!#

وتجد الملفات المبرمجة بتلك الغة بأمتداد rb

اللغة الاخيرة معانا هي c (السي) طبعا تشتهر جميع الثغرات المكتوبة بهذه اللغة بخطورتها العالية وتشتهر هذه اللغة في كتابة الوكلات او السكربتات الخاصة بسحب صلحيات المدير من السيرفر ويتم التعرف عليها من خلال تواجد سطر الاوامر

include#

وتجد الملفات المبرمجة بتلك اللغة بأمتداد c

١٧- الاستغلال Exploits

الاستغلال عبارة عن مصطلح شامل لعدة أشياء، تقوم بعض الانواع من الإكسبلويت باعطائك صلاحية لعرض ملفات الموقع و تقوم بعضها بالدخول الى السيرفر و التجول فيه، كما توجد اكسبلويتات تقوم بعمل هجوم حجب الخدمة على بورت معين في السيرفر حتى تحدث كراش crash للنظام.

هناك أنواع من الاستغلال منها ال CGI Exploits أو ال CGI Bugs و منها ال Unicodes Exploits و منها ال ، Buffer Overflow Exploits ، و منها ال PHP Exploits ،و منها الDOS Exploits و التي تقوم بعملية حجب الخدمة للسيرفر إن وجد فيها الثغرة المطلوبة لهذا الهجوم و ان لم يكن على السيرفر أي فايروول Fire Wall .

و هناك بعض الإكسبلويتات المكتوبة بلغة السي و يكون امتدادها (.c).

هذه الإكسبلويتات بالذات تحتاج الى كومبايلر او برنامجا لترجمتها و تحويل أي اكسبلويت الى اكسبلويت تنفيذي عادي يستخدم من خلال المتصفح ، و لتحويل الإكسبلويت المكتوب بلغة السي هذه الى برنامجا تنفيذيا ، نحتاج إما الى نظام التشغيل لينوكس او يونكس، او الى اي كومبايلر يعمل ضمن نظام التشغيل ويندوز .

أشهر هذه الكومبايلرات (المترجمات أو المحولات) برنامج اسمه

Borland C++ Compiler و هي تعمل تحت نظام التشغيل ويندوز كما ذكرنا سابقا.

١٨- ماهي الثغرات وما الفائدة منها

الثغرات هي عبارة عن اخطاء من قبل المبرمج في احدى اكواد اللغة بحيث تسمح للمخترق الوصول الى معلومات حساسة على السيرفر مثل اسم العضوية والباسورد الخاص بمدير الموقع انواع الثغرات كثيرة جدا ولكن من اشهرها ثغرات sql بجميع انواعها

مثل injaction او blind

١٩- ماهو السيف مود safe mode

هو احدى الخصائص التي تعيق عمل المخترق من حيث انها تقوم بمنع التنقل بحرية داخل السيرفر وايضا تمنع الكثير من التطبيقات البرمجية التي يعتمد عليها apache لذالك نجد ان اكثر الشركات الكبرى لاتستخدم تلك الخاصية لتجنب الاضرار بأسكربتات المواقع المستضيفة لديها.

٢٠- ماهو Open Basedir

هيا ايضا خاصية داخل السيرفر تقوم بمنع بعض الدوال الخطيرة التي يمكن استخدمها من قبل المخترق للتنفيذ اوامر تضر بمصلحة مدير الموقع من حيث التنقل داخل السيرفر او سحب المعلومات الحساسة التي من ضمنها ملفات قواعد البيانات.

٢١- ماهو Magic_Quotes

عباره عن خاصيه في البي اتش بي عند تفعيلها تقوم بأضافته Backslash على ‘ او ” او \ والفائده من هذا منع من مرور الرموز سليمه لكي يتجنب بعض انواع الثغرات مثل sql injection ولاكن يوجد بعض المشاكل فيها عندما نرسل معلومات نريد ان لايتم تغيرها مثل You’re The Best

اذا كان مفعل بيتم طباعه التالي

You\'re The Best

واذا لم يكون مفعل بيتم طباعته هكذا

You're The Best

٢٢- ماهو الكونفق Config او قاعده البيانات

هوا اسكربت يختلف اسمه من مصمم للاخر يستفاد منه في تكوين وربط قاعدة بيانات الاسكربت مثل vb او joomla مع phpMyAdmin التي تحتوي على قاعدة بيانات الموقع وتحتوي ايضا على بيانات المدير من اسم المستخدم او كلمة السر الخاصة بالقاعدة.

٢٣- ماهو الهاش Hashing

هيا عبارة عن رموز تشفيرية للكلمات الحساسة مثل كلمة المرور وهي تعتمد على حسابات ومعادلات معقدة يتم خلالها تشفير كلمة المرور الى رموز يصعب فكها مرة اخرى وهناك العديد من التشفيرات من اشهرها md5 التي تعرف من خلال تكونها من ٣٢ حرف ورقم ويمكننا تشبيه الهاش ببصمة الانسان فلا يمكن ان تجد شخصين ببصمة واحدة.

وهذه بعض من أنواع الهاشات:

MD5 , MD4 , MD2 , NTLM , LM , SHA1 , SHA256 , SHA384 , SHA512 , MySQL

٢٤- ماهو Zend وماهو ionCube ؟

هيا احدى طرق التشفير للملفات وقواعد البيانات (config) بحيث تصعب على الهكر الوصول لبيانات قاعده البيانات لمحة سريعة عن كيفية اختراق السيرفرات او الخوادم او مايسمى بـ ميكانيزوم اختراق الخادم ؟

٢٥- ثغرات الفيض Buffer overFlow

تعتبر ثغرات الـ Buffer Overflow أحد أخطر أنواع الثغرات البرمجية المتواجدة في التطبيقات حتى يومنا والتي قد ينتج عنها التحكم الكامل في جهاز الضحية الذي يتواجد به التطبيق المصاب.
وتكمن خطورتها في إمكانية استغلال بعضها (ما يعرف ب RCE-Remote Code Execution) دون الحاجة للتواصل مع الضحية أو الضغط على رابط أو فتح ملف ما.

٢٦- الجدار الناري FireWall

الجدار الناري أو الفايروول هو حاجز الحماية الأول في الحاسوب أو السيرفر وحتى الهاتف ، حيث يقوم بفلترة ما يدخل إلى جهازك ثم يسمح أو يمنع كل ما يشتبه به من الوصول إلى جهازك .
الفايروول قد يكون برامج مثل البرامج العادية comodo firewall، أو عبارة عن أجهزة خاصة نستعملها لحماية السيرفرات من الولوج غير المصرح لداخل الشبكة من قبل المتطفلين.

٢٧- الشيل Shell

الشيل هو سكربت أو أداة مبرمجة بلغة php (طبعا أشهرها) نقوم برفعها عن طريق ثغرة على الموقع الذي اخترقناه، بهدف تنفيذ أوامر معينة على السيرفر، مثل: حذف او تعديل او اعادة تسمية للملفات، ونستخدمها في الحصول على اسماء المستخدمين وحتى في عمل كومبايل لثغرات الكيرنل بهدف الحصول على صلاحيات الروت. أشهر أنواع الشيل هو wso shell.

تقبلوا تحياتي