Basics Buffer overflow

أساسيات البفر اوفر فلو

هل تجهل هذا النوع من الثغرات..؟

هذا الكتاب متخصص في فهم ديناميكية هذا نوع من الثغرات !

>>>>>>>>>>>>>>>

[0x00] – المقدمة
[0x01] - العرض
[0x02] - الخاتمة
[0x03] - توضيحات
[0x04] – حول

<<<<<<<<<<<<<<<

الكاتب :
SKULL- HACKER

EMAIL : WIZARD- SKH@HOTMAIL.COM

HOME : WWW.S3CURITY- ART.COM

>>>

المقدمة - [0x00]

البفر اوفر فلو Buffer Overflow

البفر اوفر فلو : هو عباره عن اخطاء برمجية او نقص برمجي يغفل عنه مبرمج البرنامج
مما يسمح لنا هذا الخطاء او النقص البرمجي ان تعمل تحكم في الذاكره طبعا الكثير يجهل هذا النوع
من الثغرات وانطلاقا من هذا الكتاب سيتمكن المشاهد من فهم جميع الطرق المتعلقة بال 'المكدس'
الذاكرة' الفيض' إدخال قيم كبيرة' أخطاء البفر'
ومصطلحات عدة....
ولتوضيح اكثر

فهو مثل أمر فيزيائي مبتكر لنفترض قمت يملئ كأس ماء إلى أخره وقمت بإضافة أشياء داخل
الكأس على سبيل المثال ثلج ..
بطبيعة الحال سوف تخرج المياه من الكأس لآن المياه ممتآلة إلى أخر الكأس
ولتقليل الضغط على الكأس ننقص المياه الى نص الكأس ونملأه إلى الآخر في
هذه الحالة فالثلج هو الذي سيتساقط إلى خارج الكأس
:)

لكي تنتقل إلى مجال البفر أو البافر اوفر فلو لازم ان تكون لديك خبرة متوسطة في البرمجة ونتكلم عن البرمجة بلغة
Python/Ruby/c++/CGI/perl/c/assembly/

كل هده اللغات البرمجية تعطيك خلفية ممتازة عن البفر اوفر فلو وفهم تركيبته.. ويمكن اكتشاف التغرات عن طريق هذه اللغات البرمجية..
خصوصا لغة التجميع يجب أن تكون لك خبرة فيها وبالخصوص كيفية التعامل مع الموديل البرمجي للمعالج8086

وطبعا في مجال استخدمها في اشياء ضارة فهي متقسمة الى قسمين

LOCAL

و

REMOT

أي التحكم بشكل مباشرة و تحكم عن بعد .. طبعا ليس موضوعنا الاختراق بل شرح أساسيات البفر فقط وفهمها مع بعض

Buffer البفر

البفر : هو مكان تخزين مؤقت للبيانات ..

overflow الفيض

الفيض : هو الزيادة عن تحمل الشيء أو انك تزيد عن شئ فوق المسموح

Registers المسجلات

سجلات : يتم استخدامهم من قبل بروسيسور الخاص لإجراء المعلومات وتنفيذ السيطرة..

.

المؤشرEBP

هو المؤشر الأساسي ، الذي يشير إلى أعلى المكدس باستدعاء دالة معينة يتم الضغط عليها إلى العودة

المؤشر EIP

هذا مؤشر لسجل 'registrer' يشير الى الأمر EBP

points Vulnerability نقاط الضعف

نقاط ضعف برنامج معين تستغل بأكثر من ثغرة تسمح للمهاجمين بفعل أشياء ضارة.

Exploit doné استغلال التغرة

أي الاستفادة من التغرة'استغلالها'

Shellcode الشل كود

شل كود : هو مجموعة من التعليمات أو كود بلغة التجميع
أو كود برمجي صغير يستخدم في عدة أشياء على أساس كتابته وتوجد عدة أدوات تقوم بتحويل ملفات تنفيذية إلى شل كود,كما يمكن لنا استغلاله في تغرات لوكال بعدة صلاحيات وعلى مشروع الميتاسبلويت على شكل بايلودات ..
بالنسبة لثغرات التحكم عن بعد بأستغلال نقاط ضعف العمليات وله اقسام عدة سأشرححها فيما بعد لأن شرحنا ليس الاختراق بل تعريف فقط على شيئ اساسي في تغرات البفر اوفر فلو ..
هنا رابط لاستغلاله على شكل بايلود .. ينصح برفع الملف التنفيذي وطرحه في خيار data
http://metasploit.com:55555/PAYLOADS?MODE=SELECT&MODULE=win32_downloadexec

وهنا شرح : فيديو : تحويل آي ملف تنفيذي الى = SheLLCode

< شرح تحويل اي ملف تنفيذي الى شل كود 1 >
http://www.youtube.com/watch?v=Cf2jcQhI0A4

< Video Arabic : Conversion shellcode >
http://www.youtube.com/watch?v=nCd1pYiWRNo

وشرح بعض خصائص ادوات مختصة فتحويل الى شل كود

تحويل : من شكل الى آخر shellcode
Find : البحث في موازنة واحدة أو سلسلة من بايت
checkval : المقدمة shellcode معرفة ما اذا كان يحتوي على قيم

Test : shellcode يبدأ تنفيذ الشل كود ويضيف أيضا نقطة توقف عند مدخل

C, Ruby, PERL ,Python : وتحويلها في الأشكال التالية Shellcode كما يمكن أن تقرأ عن عن طريق سكربت او برمجة خاصة!

GDB المصحح العام

هوا لذي يتم استخدامه في متابعة البرامج ومعرفة الملفات الأساسية داخله..

Stack: الكومه

الكومة تحدث عندما يكون هناك مساحه كبيره من الذاكره مستخدمه. فالستاك يعتمد على ان يكون للبرنامج مساحه محدده - عادة تكون عند بدء تشغيل البرنامج - في حين ان يقوم البرنامج باستخدام ذاكره اكبر، و هنا يحدث الفيض.
اي كسر البرنامج،، و قد يكون سبب الستاك ايضا program crash من هنا نستنتج ان الستاك قريب جدا من ال تزاحم استدعاء الدوال..
دون ان يتم الانتهاء من استدعاءها functions.
ويحتوي على عنوان مقطع المكدس في الذاكرة..,

NOP

نقطة الاسمبلي تشكل جزء هاما من الشل كود مع امكانية الاشارة الى العناون الصحيحة..

Heap:المساحة

[مساحة البرنامج]

Returning Address : RET

Returning Address عنوان العودة
و أمر Ret يستخدم في عدة أوامر داخل البرنامج نفسه لرجوع إلى نقطة الإدخال

SFP : Starting Address

تشغيل أول عنوان البرنامج
'المضلل بالأسود داخل برنامج المنقح'
المنقح: Olly

العرض - [0x01]

أسئلة وأجوبة

س- هل توجد تغرات للبفر أوفر فلو في برامج مشهورة .. ؟
ج – بالتآكيد هناك مواقع سكيورتي خاصة في طرح تغرات من هذا النوع الخطير في أشهر البرامج واكترها استخداما ويوجد عدة أشخاص تقوم بهذه العملية لغرض الاختراق وبعضهم لغرض كسب المال من شركة البرنامج وبعضهم لتطوير قضراتهم ..

>>

س- هل يمكن استغلال البرنامج المصاب بكل صيغه ؟
ج- غالبا متكون كل صيغ البرنامج مصابة لاكن اغلبها تكون في برامج لقراءة الصوتيات التي تحمل مساحة اكبر ..

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

س-كيف يتم استغلال مثل هده الثغرات ؟
ج- سآسآلك أولا في ماذا تريد استغلالها ..
آدا كنت استغلالها للبرامج الضارة فهذا يتطلب منك المرور في عدة مراحل منها الملف الذي تريد تحويله إلى شل كود ومن تم الى الصيغة المصاب بها البرنامج .. ويمكنك الاختيار أيضا آدا كنت تريد استخدامها بشكل مباشر ويدوي أو بشكل أوتوماتيكي باستخدام أداة قام ببرمجتها شخص ما لتوفير التعب واستغلالها عبر اتصال بورت معين على سبيل المثال البورت الحالي 445 لو تم استغلال تغره بشكل أوتوماتيكي آما بشكل مباشر فيتطلب عناء أكثر ..

>>

س- أي للغة برمجية يمكنني أستخدمها في اكتشاف نقطة ضعف برنامج .. ؟
ج- توجد عدة للغات برمجية رائعة تمكنك من اكتشاف نقاط ضعف عبرها ..
C programming language,
perl programming language,
python programming language,
c++ programming language,
c++ programming language,

ETC

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

س-إذا قمة بتنصيب البرامج الغير المتواجدة في مواقع الحماية وترقيع الثغرات وتنصيب برنامج تجميد لنضام و حماية شاملة لجهازي هل يمكن لشخص ما استغلال برامج ضارة تجاهي ؟

ج-لايمكن معرفة حماية جهازك الحاسوب حتى إن قمة بتنصيب البرامج الغير المتواجدة في مواقع الحماية توجد عدة تغرات تنل بشكل يومي اغلبها خطيرة وحتى لنفترض جهازك الحاسوب لاتوجد فيه ثغرات هده البرامج فيمكن ان تكون تغرة متواجدة في نضامك مثل
Windows xp و microsoft
حتى ان لمن تجد برامج مصابة في مواقع الحماية وترقيع الثغرات برنامج تستعمله في يمكن لمخترق معين بآكتشاف تغرة لايرد إنزالها في موقع الحماية ولتوضيح أكتر فمثل هده لمواقع تستغل للاختراق أكتر ليس الحماية أقصد موقع
Milw0rm
ويمكن أيضا للمخترق أختراقك عن طريق فحص عدة ايبيات وبورتات مصابة يمكن ان يكون الايبي لك من ضمنهم
>>>

س- بعد تعلمي لاكتشاف نقاط ضعف البرامج كيف أستغلها بالطريقة الصحيحة وان يكن اريد استغلالها في طرق ضارة تمكنني من اختراق الحواسيب..

ج- استغلالها يكون على حسب أقسام البفر اوفر فلو وعلى حسب اختيارك ليس بالضرورة استغلالها في برامج ضارة او على طريقة
Remot Buffer Overflow Exploit
أو
Local Buffer Overflow Exploit
أو
Command Injection Buffer Overflow Exploit

أو يمكنك البرمجة والاعتماد بشكل كبير على البافر وعلى حماية برنامجك أو العمل على مجال
Pentetsing
على البرامج مقابل قدر مال معين مع شركات..
أو بيع ثغرات الخطيرة للمخترقين لأن أغلب المخترقين يعتمدون على الاستغلال ليس الاكتشاف والاستغلال معا وهذا عبئ كتير من المخترقين..
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

س-ماهي البرامج التي تمكنني من فحص بشكل شامل للبرامج ومعرفة الاوفر فلو داخلها..

ج-بدون منازع برنامج المنقح
OLLYDBG
يتيح لك معرفة كل شئ فالبرنامج وكيف مصاب وكيف استغلاله إلى أخره

على شكل

ebp 0x41414141 0x41414141

وطبعا يتم ذالك بآدخال عدة بايتات الى البرنامج بالصيغ المشكوك بآصابتها مثل
.m3u
ادا كان قارء صوتيات
واستخدام بايلودات مثل

reverse_tcp اتصال عكسي
bind tcp حقن ملفات dll

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Crash
يمكن وقوع كراش مع البرنامج في حالة اصابته

الخاتمة – [0x02]

الشيء الذي زاد عن حده انقلب ضده
XD

حكمة الكتاب /

توضيحات – [0x03]

ملاحظة

لفهم المزيد لي آلية البفر اوفر فلو ينبغي عليك دراسة جد متعمقة في للغات برمجية تعد أساسية في استغلال البافر ابتدي في لغة الآسمبلي ومن تم إلى

C++/c
Perl
Python
Shellcoding

ETC

[0x04] – حول

SkuLL-HacKeR

EMAIL : WIZARD-SKH@HOTMAIL.COM

HOME : WWW.S3CURITY-ART.COM

HOME-2 : WWW.DOS02.COM