E-mail: God.Hacked@Yahoo.com

Website: Www.Expolit.Net.Tf

ملاحضات:

با سلام از اینکه مقاله من را جهت اموزش انتخاب کردین سپاس گزارم. اما کاربر گرامی این مقالات فقط جهت اموزش نوشته شده و در اختیار شما قرار گزاشته شده و هر گونه استفاده غیر اموزشی از ان بر عهده خود کاربر میباشد و اینجانب هیچ گونه مسئولیتی بر عهده نمیگیرم. با تشکر: پیام ایزدی.

((آشنایی با انواع اگسپلوییت ها و کاربرد آن))

روز به روز به تعداد اسیب پذیریهای کشف شده و همچنین اکسپلویت هایی که از این اسیب پذیری ها استفاده میکنند افزوده میشود. به همین دلیل باید با انواع اگسپلویت های مختلف اشنا شد. من پیام ایزدی برای راحتی شما تمام اگسپلویت ها را کامل توضیح داده و دسته بندی کرده ام.

اکسپلویت ها به دو دسته تقسیم میشوند:

۱) Remote
۲) Local

اکسپلویت های **Remote** به چند دسته تقسیم میشوند:

۱) Dos
۲) Buffer Overflow
۳) Stack Overflow
۴) Remote Code Execution
۵) File Include
۶) XSS
۷) SQL Injection

همه ی اکسپلویت های بالا با پسوند Remoteبه کار می روند به عنوان مثال:
Remote Buffer Overflow Exploit

اکسپلویت های Local به چند دسته تقسیم میشوند:

۱) Dos
۲) Privilege Escalation
۳) Arbitrary Code
۴) Stack Buffer Overflow

همه ی اکسپلویت های بالا با پسوند Local به کار می روند به عنوان مثال:
Local Stack Buffer Overflow

در ادامه به توضیح در مورد هر یک از موارد بالا میپردازیم.

Remote Dos:

این اکسپلویت میتواند یک سیستم راه دور را از کار بیندازد یعنی با حمله به برنامه ی اسیب پذیر و دستکاری آن باعث به وجود امدن اختلال در پردازش به صورتی که می تواند به سیستم اسیب برساند این نوع حملات غیر قانونی بوده و جرایم سنگینی به دنبال دارد.

Remote Buffer Overflow:

بیشترین نوع اکسپلویت هایی که استفاده میشود این نوع است بیشتر هکر های تازه کار و حتی حرفه ای برای دسترسی به سیستم به صورت راه دور از این اکسپلویت استفاده میکنند این اکسپلویت هم با اختلال بر روی پردازش یک سیستم و دستکاری پردازش های برنامه آسیب پذیری یک Port را بر روی سیستم هدف باز میکند که میتوان به ان پرت Telnet کرد و وصل شد. اگر بر روی سیستم طرف فایروال وصل باشد امکان دسترسی به سیستم و وصل به ان بسیاد کم خواهد شد. بنابر این بیشتر این اکسپلویت ها به صورتی نوشته میشوند که به صورت خودکار بعد از باز کردن پورت ما را به ان سیستم وصل میکنند. به این نوع اکسپلویت ها اکسپلویت های معکوس یا Reverse میگویند. این نوع اکسپلویت ها توانایی عبور از فایروال ویندوز را دارند .

Remote Stack Overflow:

بخشی از حافظه Stack یا پشته است که در این مقاله جای توضیح ان نیست. عملکرد ان مانند Buffer Overflow ی است و تقریبا توضیحات ان در مورد Stack Overflow نیز صدق میکند.

Remote Code Execution:

این اکسپلویت ها که اغلب برای استفاده از اسیب پذیریهای برنامه های کاربردی تحت وب نوشته میشوند قابلیت اجرای یک دستور خاص را دارند یعنی میتوانند یک فرمان سیستم عامل و یا فرمان های دیگر را اجرا کنند. به عنوان مثال اگر اکسپلویتی برای Phpbb از این نوع داشته باشیم پس اجرا و دسترسی به سیستم میتوانید فرمان های عامل لینوکس را اجرا کنید این فرمان میتواند مانند دانلود کردن یک BackDoor از ادرسی مشخص بر روی سیستم هدف باشد و یا باز کردن یک پرت برای دسترسی به سیستم.

Remote File Include:

این نوع اکسپلویت ها نیز برای برنامه های کاربردی تحت وب هستند و میتوانند فایلی را از آدرس مشخص بر روی سیستم هدف دانلود کنند این فایل ها نیز میتوانند یک Shell Scripمانند Rhtoolsو یا C99باشند.

SQL Injection:

این نوع اکسپلویت ها در واقع همان کدهای SQL Injection هستند که می توان از آنها در قالب یک اکسپلویت استفاده کرد این نوع اکسپلویت ها به data Baseاصلی به صورت خودکار وصل شده و سپس کد SQL Injection را وارد میکنند مثل:

http://www.victim.com/maxisepetdirectory/default.asp?git=11&link=SQL

که به جای SQL باید مد SQL Injection را گزاشت و البته برخی دیگر نیز به طور خودکار این کار را انجام میدهند یک کد SQL Injectionمثل زیر است:

'or'='

'or'a'='a

'or=--'

اکسپلویت های Local نیز در برخی از موارد کاربرد بسیاری دارند به عنوان مثال فرض کنید به یک سیستم لینوکس دسترسی nobody دارید یعنی نمیتوانید کارهایی را که کاربرد Root در لینوکس میتوانید انجام دهید را بدهید . این جا اکسپلویت های Local به کمک شما خواهند آمد. در ادامه به توضیح بیشتر میپردازیم.

Dos:

این نوع اکسپلویت ها تنها سیستم را از کار می اندازند و در اصل کار دیگری انجام نمیدهند.

Privilage Escalition:

از این نوع اکسپلویت ها بیشتر از همه استفاده میشوند کار اصلی این اکسپلویت ها بیشتر بالا بردن دسترسی محدود به ان دارید با اجرای این اکسپلویت ها شما در یک سیستم عامل لینوکس میتوانید دسترسی خود را از **nobody** به **Root** بالا ببرید به این نوع اکسپلویت ها که در لینوکس دسترسی بالایی دارند **Local Root** هم گفته میشود باید توجه کنید که اکسپلویتی را برای این کار استفاده کنید که برای **Kernal** سیستم هدف شما نوشته شده باشد.

Arbiraty Code:

این نوع اکسپلویت ها فرمان مورد نظر شما را بر روی سیستم اجرا میکنند.

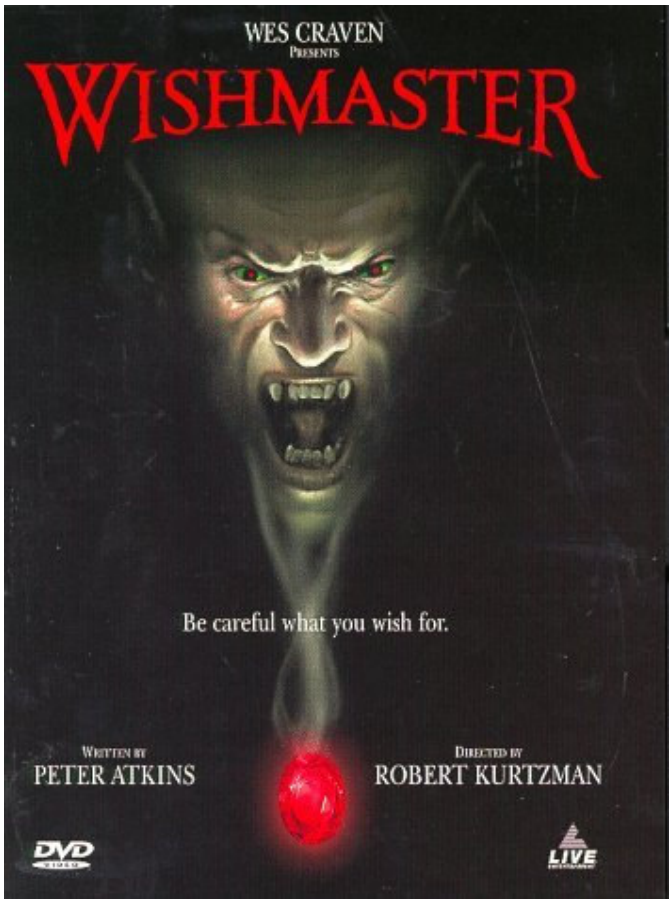
Stack Buffer Overflow:

این نوع اکسپلویت ها در واقع با دستکاری در پردازش های یک برنامه پورتی را بر سیستم باز میکنند و میتوان از این پورت به صورت Remoteاستفاده کرد در واقع اولین گام نوشتن ان ها به صورت localاست که در بعد remote میشوند

توضیحات:

Nobody: در سیستم عامل لینوکس کاربردی با نام nobodyوجود دارد که تنها میتواند فایل ها ببیند و اجازه ویرایش را ندارد در واقع دسترسی پایینی به سیستم دارد.

Root: در سیستم عامل لینوکس کاربردی به نام Root مجود دارد که مدیر سیستم است و تمام اختیارات را دارد در واقع بالاترین دسترسی را دارد.



Hacked By God.Hacked