بسم الله الرحمن الرحیم

# آشنایی با انواع اکسپلویت ها و کاربرد هر یک از آن ها

روز به روز به تعداد آسیب پذیری های کشف شده و همچنین اکسپلویت هایی که از این آسیب پذیری ها استفاده می کنند افزوده می شود.به همین دلیل باید با انواع اکسپلویت ها ی مختلف آشنا شد.

اکسپلویت ها به دو دسته تقسیم می شوند:

1) Remote
2) Local

اکسپلویت های Remote به چند دسته تقسیم می شوند:

1) DoS
2) Buffer Overflow
3) Stack Overflow
4) Remote Code Execution
5) File Include
6) XSS
7) SQL Injection

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

اکسپلویت های Local به چند دسته تقسیم می شوند:

1) DoS
2) Privilege Escalation
3) Arbitrary Code
4) 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 می پردازیم

Remote DoS:

این اکسپلویت می توانند یک سیستم راه دور از کار بیندازند؛یعنی با حمله به برنامه ی آسیب پذیر و دستکاری آن ، باعث به وجود آمدن اختلال در پردازش به صورتی که می تواند به سیستم آسیب برساند ، شود.این نوع حملات غیر قانونی بوده و جرایم سنگین را به دنبال دارد.

:Remote Buffer Overflow
بیشترین نوع اکسپلویتی که استفاده می شود این نوع است.بیشتر هکرهای تازه کار و حتی حرفه ای برای دسترسی پیدا کردن به سیستم به صورت راه دور ، از این اکسپلویت استفاده می کنند.این اکسپلویت هم با اختلال بر روی پردازش یک سیستم و دستکاری پردازش های برنامه ی آسیب پذیر ، یک Port را بر روی سیستم هدف باز می کند که می توان به آن پورت Telnet کرد و وصل شد. اگر بر روی سیستم هدف فایروال نصب شده باشد ، امکان دسترسی به پورت و وصل شده به آن بسیار کم خواهد شد. به همین دلیل بعضی از این اکسپلویت ها طوری نوشته می شوند که به صورت خودکار بعد از باز کردن پورت ما را به آن پورت وصل می کنند.به این نوع اکسپلویت ها ، اکسپلویت معکوس و یا Reverse می گویند.این نوع اکسپلویت ها توانایی عبور از فایروال را دارند به این صورت که مانند یک برنامه از روی سیستم هدف درخواست وصل شدن به سیستم ما را می کند و به همین دلیل فایروال اجازه ی دسترسی برنامه را به اینترنت می دهد و به این صورت می توان به سیستم هدف دسترسی پیدا کرد.نوشتن این اکسپلویت سخت تر از دیگر اکسپلویت ها است به همین دلیل اکثر اکسپلویت نویس های حرفه ای برای آن دسته از اکسپلویت هایی که کاربرد زیادی خواهند داشت این کار را انجام می دهند.

:Remote Stack Overflow
بخشی از حافظه Stack یا پشته است که در این مقاله جای توضیخ آن نیست.عملکرد آن مانند Buffer Overflow است و تقریبا توضیحات آن نیز در مورد Stack Overflow نیز صدق می کند.

:Remote Code Execution
این اکسپلویت ها که اغلب برای استفاده از آسیب پذیری های برنامه های کاربردی تحت وب نوشته می شوند ، قابلیت اجرای یک دستور خاص را دارند؛یعنی می توانند یک فرمان سیستم عامل و یا فرمان های دیگر را اجرا کنند.به عنوان مثال اگر اکپسلویتی برای phpBB از این نوع داشته باشید ، پس از اجرا و دسترسی به سیستم می توانید فرمان های سیستم عامل لینوکس را اجرا کنید.این فرمان می تواند مانند دانلود کردن یک Backdoor از آدرسی مشخص بر روی سیستم هدف باشد و یا بازکردن یک پورت برای دسترسی به سیستم.

:Remote File Include
این نوع اکسپلویت ها نیز برای برنامه های کاربردی تحت وب هستند و می توانند فایلی را از آدرس مشخص بر روی سیستم هدف دانلود کنند.این فایل ها نیز می توانند یک Shell Script مانند rhtools و یا c99 باشند.

:XSS
این نوع حملات چندان کارایی بالایی برای دسترسی به سیستم هدف ندارند و فقط می توانند کاربران را مورد حمله قرار دهند.از این نوع حملات و کدها که اکثرا جزو اکسپلویت ها قرار نمی گیرند و به عنوان Script های خطرناک گفته می شوند ، در حملات Session Hijacking و یا Cookie Hijacking استفاده کرد.

:SQL Injection
این نوع اکسپلویت ها در واقع همان کدهای SQL Injection هستند که می توان از آن ها در قالب یک اکسپلویت استفاده کرد.این نوع اکسپلویت ها به Data Base اصلی به صورت خودکار وصل شده و سپس کد SQL Injection را وارد می کنند.مانند:
http://www.victim.com/maxisepetdirectory/default.asp?git=11&link=SQL
که به جای SQL باید کد SQL Injection را گذاشت و البته برخی دیگر نیز به طور خودکار این کار را انجام می دهند.یک کد SQL Injection مانند زیر است:
‘or’=’
‘or 'a'='a
‘or = --‘

اکسپلویت های Local نیز در برخی از موارد کاربرد بسیار فراوانی دارند.به عنوان مثال فرض کنید به یک سیستم لینوکس دسترسی nobody دارید.یعنی نمی توانید کارهایی را که کاربر root در لینوکس می تواند انجام دهد را بدهید.این جا اکسپلویت های Local به کمک شما خواهند آمد.در ادامه به توضیح آن ها می پردازیم.

:DoS
این نوع اکسپلویت ها تنها سیستم را از کار می اندازند و در اصل کار دیگری انجام نمی دهند.

:Privilege Escalation
از این نوع اکسپلویت ها بیشتر از همه استفاده می شود.کار اصلی این اکپسلویت ها بالا بردن دسترسی در یک سیستم است که شما دسترسی محدود به آن دارید.با اجرای این اکسپلویت ها شما در یک سیستم عامل لینوکس می توانید دسترسی خود را از nobody به root بالا ببرید.به این نوع اکسپلویت هایی که در لینوکس دسترسی را بالا می برند ، local root هم گفته می شود.البته باید توجه کنید که اکسپلویتی را برای این کار استفاده کنید که برای kernel سیستم هدف شما نوشته شده باشد.همان طور که اکثر اکسلپویت های ویندوز XP برای ویندوز 2003 کاردبر ندارند ، هر اکسپلویت local root نیز باید با kernel سیستم هدف شما نیز مطابقت داشته باشد.برا این کار در خط فرمان لینوکس می توانید دستور uname –a را وارد کرده و شماره kernel را بیابید.در ویندوز نیز معمولا پس از حملات Buffer Overflow و دسترسی به آن ، دسترسی شما از نوع Administrator خواهد بود و احتیاجی به این نوع اکسپلویت ها نیست.اما اگر در شبکه ای هستید که مدیر آن شبکه دسترسی شما را به کامپیوتر مورد استفاده ی شما محدود کرده است ، می توانید با اجرای این نوع اکسپلویت ها دسترسی خود را بالا ببرید.

:Arbitrary Code
این نوع اکسپلویت ها فرمان مورد نظر شما را بر روی سیستم اجرا می کنند.

Stack Buffer Overflow:
این نوع اکسپلویت ها در واقع با دستکاری در پردازش های یک برنامه ، پورتی را بر سیستم باز می کنند و می توان از این پورت به صورت Remote استفاده کرد.در واقع اولین گام نوشتن اکسپلویت های Remote Stack Overflow و یا Remote Buffer Overflow نیز ، نوشتن آن ها صورت Local است که بعد از تست کردن آن ها برروی نرم افزارآسیب پذیر، برنامه نویسی شبکه را به اکسپلویت اضافه می کنند.

توضیحات:

Nobody: در سیسم عامل لینوکس ، کاربری به نام nobody وجود دارد که تنها می تواند فایل ها ببیند و اجازه ی ویرایش آن ها را ندارد.در واقع دسترسی پایین را به سیستم دارد.

Root: در سیستم عامل لینوکس ، کاربری به نام root وجود دارد که مدیر سیستم است و تمام اختیارات را دارد.در واقع بالاترین دسترسی را دارد.

Copyright© by Siahacker
2005-2006 All Right Reserved
Email:Siahacker@gmail.com