به‌نام خداوند جان و خرد

آموزش تست نفوذ با
Metasploit Framework

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندار پارس

سرشناسه : داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور : آموزش تست نفوذ با Metasploit Framework/مجید داوری‌دولت‌آبادی.
مشخصات نشر : تهران: پندار پارس، ۱۳۹۴.
مشخصات ظاهری : ۳۳۰ص.: مصور، جدول.
شابک : 978-600-6529-86-8: ۲۸۰۰۰۰ریال
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه: ص. ۳۲۵.
موضوع : متاسپلویت (منبع الکترونیکی)
موضوع : کامپیوترها -- کنترل دستیابی
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : آزمایش نفوذ (ایمن‌سازی کامپیوتر)
رده بندی کنگره : ۹/۷۶QA ۱۳۹۴ ۲د۱۶م/
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۳۹۱۹۹۳۸

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره 14، واحد 16 **www.pendarepars.com**

تلفن: 66572335 - تلفکس: 66926578همراه: 09214371964 **info@pendarepars.com**

نام کتاب : **آموزش تست نفوذ با Metasploit Framework**

ناشر : **انتشارات پندار پارس**

تدوین : **مجید داوری دولت آبادی**

چاپ نخست : **شهریور ماه 94**

شمارگان : **500 نسخه**

طرح جلد و صفحه‌آرایی : **سارا یعسوبی**

چاپ، صحافی : **روز**

قیمت : **28000 تومان** **شابک** : **978-600-6529-86-8**

فهرست مطالب

سخنی با خوانندگان

امروزه در دنیای هک و آزمایش نفوذ، ابزارهای گوناگونی به‌صورت آماده پیاده‌سازی و ارائه شده است که معمولا در قالب توزیع‌های حرفه‌ای و مخصوص نفوذ لینوکس (BackTrack، Kali و ...) و یا به‌صورت فایل اجرایی قابل نصب در محیط سیستم‌عامل ویندوز منتشر می‌شوند. بیشتر این ابزارها کمک شایانی به آزمایش‌کننده نفوذ و هکر می‌کنند و نفوذگران از آن‌ها استفاده‌های فراوانی می‌برند. یکی از این نوع ابزارها که پشتیبانی بسیار مناسبی از آن نیز به عمل می‌آید، ابزار قدرتمند Metasploit Framework است که به‌عنوان سکوی نرم‌افزاری در زمینه آزمایش‌نفوذ و هک مورد استفاده قرار می‌گیرد. در واقع با کمک این ابزار می‌توان همه‌ی مراحل یک حمله کامل را با همه‌ی جزئیات پیاده‌سازی کرد. به نوعی می‌توان گفت آزمایش‌کننده نفوذ یا نفوذگر چنانچه به این ابزار دسترسی داشته باشد و وارد محیط کنسول اصلی آن شود، به‌سادگی می‌تواند همه‌ی اقدامات نفوذی خود را انجام دهد و در بیشتر موارد نیازی به مراجعه به محیط ابزارهای دیگر برای پیشبرد اهداف خود ندارد.

هم‌اینک این ابزار در همه‌ی توزیع‌های حرفه‌ای و ویژه نفوذ لینوکس به‌صورت آماده و نصب شده موجود می‌باشد و نیازی به نصب آن در این نوع توزیع‌ها نیست، اما در سیستم‌عامل ویندوز باید آن‌را نصب کرد تا بتوان با کنسول خط‌فرمان و وب از امکانات آن استفاده کرد. هرچند، گفتنی است که توانایی‌ها و قابلیت‌هایی که در نسخه‌های لینوکسی این ابزار وجود دارد دست نفوذگر یا آزمایش‌کننده نفوذ را برای پیاده‌سازی انواع حملات هکری باز می‌گذارد و ویژگی‌های بسیاری به آن می‌افزاید؛ پس پیشنهاد می‌شود برای استفاده بهتر از این ابزار از نسخه‌های نصب شده بر روی توزیع‌های حرفه‌ای و ویژه‌ی هک لینوکس استفاده شود تا بتوان به آسانی از همه‌ی امکانات موجود در آن بهره برد. در این کتاب نیز مبنای اصلی آموزش، نسخه‌های موجود در توزیع‌های حرفه‌ای و ویژه هک لینوکس می‌باشد. این کتاب تلاش دارد تا متخصصان امنیت یا دانشجویان علم امنیت و هک را هر چه بیشتر به‌صورت عملی با انواع پیاده‌سازی حملات هکری آشنا سازد تا آن‌ها بتوانند در قالب یک محیط عملی این نوع حملات را اجرا کنند و به دنبال راه‌کارهای امنیتی و مقابله‌ای با انواع حملات باشند، زیرا این ابزار به آن‌ها نشان می‌دهد که چگونه به‌سادگی می‌توان با داشتن علم کافی در دنیای امنیت و هک و با کمک ابزارهای موجود می‌توان به سیستم مقصد نفوذ کرد.

در این کتاب از همه‌ی منابع معتبر و پایه‌ای علم هک استفاده شده است که البته با تجربیات ناچیز اینجانب آمیخته شده است تا کتابی جامع و مفید ایجاد شود. اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تالیف کتابی آموزشی به‌صورت گام به گام به‌منظور افزایش کارایی عملی متخصصان، دانشجویان و مدیران شبکه در زمینه استفاده از یکی از ابزارهای اساسی آزمایش‌های نفوذ و هک بودم تا آن‌ها را با اصول فنی استفاده از این ابزار آشنا و آگاه سازم (گرچه مدیران و متخصصان امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخود لازم دانستم که این آگاه‌سازی را انجام دهم.)

همان‌گونه که گفته شد، شیرازه‌ی اصلی این کتاب برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه‌ی امنیت داده، اصول آزمایش‌های نفوذ و علم هک، توزیع‌های استاندارد آزمایش نفوذ و هک و همچنین منابع معتبر آموزش ابزار Metasploit Framework می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملا آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام

کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را به دیده منتّ پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zzn.com)

هشدار

این کتاب تنها برای افزایش آگاهی و رشد علمی متخصصان علم امنیت و کامپیوتر تالیف شده است. درنتیجه عواقب ناشی از هرگونه سوء استفاده از مطالب این کتاب برعهده شخص خاطی بوده و مؤلف و انتشارات هیچ‌گونه مسئولیتی در این مورد برعهده نخواهند گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام این کار ناچیز فشردند، تشکر می‌کنم. برخود لازم می‌دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی کنم. زحمات خاضعانه‌ی ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانه‌ی انتشارات پندار پارس جناب آقای مهندس حسین یعسوبی و همه‌ی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب ز کمال لطف خاصم گردان

واقف به حقایق خواصم گردان

ز عقل جفا کار دل افگار شدم

دیوانه خود کن و خلاصم گردان

(مجید داوری دولت آبادی – بهار 1394)

فصل نخست

مفاهیم پایه‌ای و نصب ابزار Metasploit در لینوکس

در دنیای فناوری اطلاعات و به‌ویژه علم امنیت اطلاعات، نیاز متخصصان به ابزارها و نرم‌افزارهای مفید در این حوزه روز به‌روز بیشتر می‌شود. این نیاز چه از دیدگاه آزمایش‌های نفوذ و پیاده‌سازی حملات هکری و چه در زمینه‌ی امن‌سازی بسترهای ارتباطی و شبکه‌ای احساس می‌شود. یکی از ابزارهایی که امروزه در شاخه علم آزمایش نفوذ و پیاده‌سازی حملات نفوذگری در میان متخصصان و نفوذگران جای خود را پیدا کرده است، Metasploit Framework نام دارد که می‌توان گفت جزو بهترین و در واقع قدرتمندترین ابزارها در این حوزه به‌شمار می‌آید. این چارچوب قدرتمند که از این پس آن را MSF می‌نامیم، هم اینک جزو مفیدترین ابزارها در زمینه حسابرسی و آزمایش به‌حساب می‌آید. از ابزار گفته شده، به‌صورت وسیعی چه در شاخه‌ی علم آزمایش نفوذ و چه در شاخه‌ی نفوذگری و پیاده‌سازی حملات هکری توسط متخصصان علم امنیت و نفوذگران استفاده می‌شود.

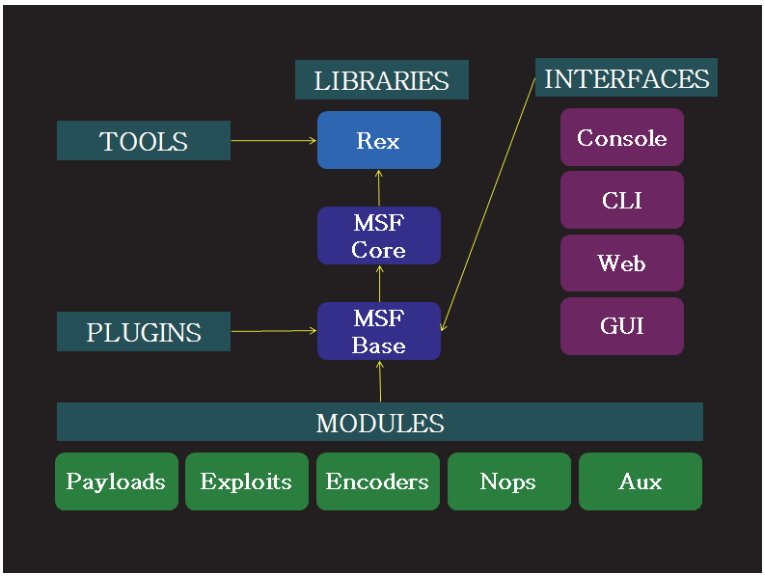
این ابزار از ابتدای پیاده‌سازی دارای ساختار و معماری منسجم و مستحکمی بوده و می‌باشد و به‌صورت بسیار گسترده در سطح گروه‌های هکری و سازمان‌های امنیتی منتشر شده است. هم اکنون نیز این معماری توسط گروه تولید کننده این ابزار حفظ شده و توسعه پیدا می‌کند. این ابزار به گفته‌ی برخی نفوذگران، جزو ابزارهای کامل و همه‌کاره علم امنیت و نفوذگری به‌حساب می‌آید که با آن می‌توان همه‌ی مراحل پیاده‌سازی یک حمله را از آغاز کار که دربردارنده‌ی شناسایی و جمع‌آوری اطلاعات از سیستم یا شبکه هدف است تا پایان عملیات که دربردارنده‌ی پاکسازی و رد گم کردن می‌باشد، انجام داد. در واقع نمونه‌ای از همه‌ی ابزارهایی که یک متخصص امنیت یا یک نفوذگر در حین پیاده‌سازی حمله (از آغاز تا پایان) به نوعی به آن‌ها نیاز دارد، در مجموعه یا سکوی Metasploit موجود می‌باشد. در این کتاب قصد داریم به بررسی کامل این ابزار و چگونگی استفاده از آن در پیاده‌سازی حملات گوناگون بپردازیم. در واقع با کمک قابلیت‌های شگفت‌انگیز موجود در این ابزار می‌توان به‌سادگی و با سرعت بسیار بالا انواع حمله‌ها و آزمایش‌ها را بر روی هدف مورد نظر انجام داد و به نتایج مورد نظر رسید. نکته‌ی مهم درباره‌ی ابزار Metasploit این است که به سرعت و روزبه‌روز توسط گروه تولید کننده‌ی ابزار در حال رشد و به‌روزرسانی است و هر چند وقت یک‌بار نسخه‌ی جدیدی با حفظ معماری اصلی در اختیار متخصصان و کارشناسان قرار می‌گیرد. همان‌گونه که گفته شد، ابزار Metasploit که نرم‌افزاری کد باز است، یک ابزار تکی و ساده نیست؛ بلکه در واقع مجموعه‌ی کاملی از ابزارها و کدهای بهره‌برداری گوناگون است که در قالب یک سکوی قدرتمند ارائه و به‌روزرسانی می‌شود.

تاریخچه ابزار Metasploit

این ابزار قدرتمند توسط پژوهشگر امنیت HD Moore در اکتبر سال 2003 توسعه داده شد. ابزار گفته شده براساس اسکریپت‌های زبان Perl توسعه داده می‌شود. این ابزار با هدف افزایش سطح اطلاعاتی کارشناسان شبکه و امنیت در این حوزه در مدت کوتاهی دوباره به زبان برنامه‌نویسی Ruby نوشته شد که بیش از صد و پنجاه هزار خط کد برنامه‌نویسی دارد. نسخه‌ی سه آن در سال 2007 طراحی و پیاده‌سازی شد. در سال 2009 این ابزار در قالب شرکت امنیتی به‌نام Rapid7 توسعه داده شد. هم‌اینک این ابزار بیش از 1000 کد Exploit، 260 ماژول Payload، 460 ماژول Auxiliary دارد؛ که برای اهداف آزمایش‌های نفوذ و بهره‌برداری علیه سیستم و شبکه‌ی هدف مورد استفاده قرار می‌گیرد.

معماری ابزار Metasploit Framework

ابزار Metasploit دارای یک معماری منسجم و ساخت‌یافته می‌باشد که پس از گذشت سال‌ها از تولید آن و تغییر زبان برنامه‌نویسی برای توسعه‌ی این ابزار، ساختار اصلی آن حفظ شده است و کماکان نیز ادامه دارد. شمایی کلی از ساختار و معماری این ابزار در شکل (1-1) نشان داده شده است.



شکل (1-1) شمایی کلی از ساختار و معماری ابزار Metasploit Framework

در برخی ساختارهای مربوط به معماری ابزار Metasploit، ماژول Post-Mods نیز اضافه شده است. در ادامه‌ی مطالب فصل، ممکن است با عبارت‌هایی مانند Shellcode و Listener برخورد داشته باشید؛ منظور از عبارت Shellcode، دستورالعملی است که از Payload برای بهره‌برداری علیه سیستم هدف استفاده می‌کند. Shellcode معمولا به زبان اسمبلی نوشته می‌شود. در واقع اگر کد Payload بر روی سیستم هدف عملیات ویژه‌ای را انجام دهد، از آن با نام Shellcode نیز یاد می‌شود. در حقیقت به Payloadهایی که هدف آن‌ها

دریافت پوسته‌ی فرمان از سیستم هدف است، Shellcode نیز گفته می‌شود. در ادامه فصل به بررسی مفهوم Payload می‌پردازیم. همچنین Listener، ترکیباتی است که در درون ابزار Metasploit پورتی نرم‌افزاری را بر روی سیستم‌عامل باز می‌کند و بر روی آن پورت به حالت فال‌گوش در می‌آید. این پورت ممکن است بر روی سیستم نفوذگر یا بر روی سیستم بهره‌برداری شده فعال باشد. پس می‌توان گفت به پورتی که به‌منظور تبادل اطلاعات بر روی سیستم قربانی باز می‌شود و به‌شکل فال‌گوش در می‌آید در اصطلاح شنونده یا Listener می‌گویند. در ادامه فصل به بررسی کامل مفاهیم اساسی در ابزار Metasploit می‌پردازیم.

سیستم‌فایل: سیستم‌فایل ابزار MSF در دایرکتوری ابزار به‌فرم زیر سازماندهی شده است:

- دایرکتوری lib: در این مسیر کتابخانه‌های مربوط به کدهای پایه‌ای سکو و ابزار MSF قرار دارند.
- دایرکتوری data: در این مسیر فایل‌های قابل ویرایش برای استفاده در ابزار Metasploit وجود دارند.
- دایرکتوری tools: در این مسیر ابزارهای خط فرمان مفید گوناگون مربوط به ابزار Metasploit موجود می‌باشند.
- دایرکتوری modules: در این مسیر ماژول‌های واقعی ابزار MSF موجود می‌باشند.
- دایرکتوری plugins: پلاگین‌های مربوط به ابزار در هنگام اجرا با این مسیر بارگذاری می‌شوند. نکته‌ی مهم این است که می‌توان دستورهای پایگاه‌های‌داده و پلاگین‌های جدید را با این مسیر به ابزار تزریق کرد. روال انجام این‌کار در فصل‌های بعدی بیان می‌شود.
- دایرکتوری scripts: در این مسیر کدهای اسکریپت ویژه ابزار MSF مانند Meterpreter و دیگر کدهای اسکریپت ابزار گفته شده وجود دارند که می‌توان با واسطهای ابزار Metasploit از آن‌ها استفاده کرد.
- دایرکتوری external: کدهای منبع ابزار به‌همراه کتابخانه‌های متفرقه دیگر در این مسیر از سیستم‌فایل ابزار قرار دارند.

کتابخانه‌ها: کتابخانه‌ی ابزار MSF همانند شکل (1-1) به‌فرم زیر سازماندهی شده است:

- کتابخانه‌ی Rex: دربردارنده‌ی کتابخانه‌ی پایه‌ای برای وظایف بیشتر است. این کتابخانه از مواردی مانند سوکت‌ها، انواع پروتکل‌های مختلف، تحول‌ها و تبدیل‌های متنی پشتیبانی می‌کند. از موارد دیگری که توسط این کتابخانه پشتیبانی می‌شود، می‌توان به SSL، SMB، HTTP، XOR، Base64 و یونیکدها اشاره کرد.
- کتابخانه‌ی Msf::Core: این کتابخانه APIهای پایه‌ای را برای ابزار فراهم می‌سازد. این APIها در ابزار Metasploit تعریف شده‌اند.
- کتابخانه‌ی Msf::Base: این کتابخانه APIهای معمول را فراهم می‌کند. در واقع در این کتابخانه APIهای ساده شده برای ابزار MSF موجود است و توسط این ابزار مورد استفاده قرار می‌گیرد.

ماژول‌ها و موقعیت استقرار آن‌ها: ابزار Metasploit دربردارنده‌ی مجموعه کاملی متشکل از ماژول‌های مفید برای استفاده می‌باشد. درحالت کلی ماژول‌های این ابزار دربردارنده‌ی موارد زیر می‌باشند:

- ماژول Payload: این ماژول قطعه‌ای از کد برای اجرا به‌صورت راه دور علیه سیستم هدف می‌باشد. در واقع این ماژول بر روی سیستم هدف اجرا می‌شود و اقدام‌های بعدی را به‌منظور اتصال نفوذگر به سیستم هدف فراهم می‌کند. نمونه‌ای از ماژول Payload، دربردارنده‌ی reverse shell و bind shell می‌باشند. به‌طور معمول کارهایی که می‌توان با کمک Payload پس از دسترسی به سیستم هدف به‌دست آورد دربردارنده‌ی ارسال و دریافت فایل‌ها، تهیه تصاویر از محیط گرافیکی سیستم هدف، جمع‌آوری کدهای Hash مربوط به

گذرواژه‌ها و غیره می‌باشند. درحالت کلی سه نوع ماژول Payload در ابزار MSF وجود دارند که دربردارنده‌ی حالت Single، Stragers و Stage می‌باشند. به‌طور معمول Payloadها در ابزار MSF درحالت Stage می‌باشند. حالت Stage با علامت / مشخص می‌شود و چنانچه پس از عبارتی مانند windows، عبارت تکی بدون علامت / وجود داشته باشد، Payload مورد نظر در اصطلاح Single می‌باشد، اما اگر پس از عبارت windows عبارت دیگری مانند shell وجود داشته باشد و در ادامه‌ی آن نیز علامت / بعدی مشاهده شود، عبارت shell یک Stage می‌باشد و عبارتی که پس از /shell وجود دارد، در اصطلاح Strager نامیده می‌شود. نمونه‌ای از ساختار یک Payload به‌فرم زیر می‌باشد. در این مثال عبارت find_tag یک Strager است:

windows/shell/find_tag

Payloadهای نوع Single، به‌فرم کاملا مستقل عمل می‌کنند و برای اهدافی مانند افزودن یک کاربر یا اجرای یک برنامه بر روی سیستم قربانی استفاده می‌شوند. Payloadهای نوع Strager در ابزار Metasploit نیز به‌منظور برقراری ارتباطات گوناگون بین سیستم نفوذگر و هدف مورد استفاده قرار می‌گیرند. Payloadهای نوع Stage نیز دربردارنده‌ی عناصری هستند که با کمک ماژول‌های Stragers دریافت می‌شوند. معروف‌ترین و مهم‌ترین Stageها در ابزار Metasploit، دربردارنده‌ی Meterpreter و VNC Injection می‌باشند که در فصل‌های بعدی به‌طور مفصل بررسی خواهند شد. درحالت کلی برخی از انواع Payloadها دربردارنده‌ی موارد زیر می‌باشند:

- Inline (Non Staged): همه‌ی Shellcodeها با کمک Payload اجرا می‌شوند. این ساختارها بسیار پایدار هستند، اما ممکن است بسیار بزرگ باشند. در واقع این نوع دربردارنده‌ی یک Payload تکی برای بهره‌برداری به‌همراه همه‌ی Shellcode می‌باشد که برای هدف انتخاب شده، در نظر گرفته می‌شود. این نوع Payload نسبت به دیگر موارد از پایداری بیشتری برخوردار می‌باشد. برخی از کدهای Exploit از این نوع Payloadها پشتیبانی می‌کنند.
- Staged: Payloadهای نوع Stager با Payloadهای نوع Stage برای اهداف و کارهای خاصی ترکیب می‌شوند. در واقع همان‌گونه که گفته شد، یک Stager کانال ارتباطی میان سیستم نفوذگر و سیستم قربانی برقرار می‌کند و در ادامه اقدام به خواندن Payload نوع Stage به‌منظور اجرا بر روی سیستم هدف می‌کند.
- Meterpreter: این Payload قالب کوچکی از Meta-Interpreter است که توسعه داده شده است و Payloadهای چند وجهی را با تزریق عملگرها به dll انجام می‌دهد. این Payload به‌طور کامل در حافظه‌ی سیستم هدف بارگذاری می‌شود و هیچ‌گونه اثری بر روی دیسک‌سخت آن سیستم ایجاد نمی‌کند؛ درنتیجه با روش‌ها و تکنیک‌های معمول پزشکی قانونی قابل تشخیص و شناسایی نمی‌باشد. در این‌حالت می‌توان همه‌ی اسکریپت‌ها و پلاگین‌ها را به آسانی بر روی حافظه RAM سیستم هدف بارگذاری کرد و پس از استفاده کاملا از روی حافظه تخلیه کرد.
- PassiveX: این نوع Payload می‌تواند کمک به‌سزایی در عبور از محدودیت‌های خروجی دیوارهای آتش به نفوذگر کند. این Payload برای ایجاد و مخفی‌سازی در مرورگر Internet Explorer از کنترل‌های ActiveX استفاده می‌کند. در واقع با استفاده از کنترل‌های ActiveX ارتباط‌هایی با نفوذگر به‌وسیله‌ی درخواست‌ها و پاسخ‌های HTTP ایجاد می‌کند.

- Ord: این نوع Payload براساس Stagerهای ویندوز پیاده‌سازی شده است و دارای مزایای متمایز و معایبی نیز می‌باشد. از مزایایی آن قدمت اجرا در هر زبان سیستم‌عامل ویندوز از نسخه 9x می‌باشد. این نوع Payloadها از لحاظ ظرفیتی بسیار کوچک هستند. همچنین، دارای دو عیب است که یکی بارگذاری فایل ws2_32.dll پیش از اجرای کد Exploit است و دیگری پایداری کم آن نسبت به Stagerهای دیگر می‌باشد.
- IPv6: همان‌گونه که از نام این نوع Payload مشخص است، برای ایجاد توابع بر روی شبکه‌های مبتنی بر آدرس IP نسخه شش ساخته شده است.
- Reflective DLL injection: با کمک این تکنیک می‌توان یک Stage Payload را در درون یک فرآیند درحال اجرا در سیستم هک شده در حافظه تزریق کرد؛ با این شرط که به هیچ عنوان اطلاعاتی بر روی دیسک‌سخت نوشته نشود. گفتنی است که Payloadهای VNC و Meterpreter هر دو از این مکانیزم استفاده می‌کنند.
- Reverse: براساس این مکانیزم پس از اجرای کد Exploit علیه سیستم هدف، اتصالی از سیستم هدف به سیستم نفوذگر برقرار می‌شود. درحقیقت به‌جای برقراری ارتباط با سیستم هدف پس از اجرای کد Exploit، ارتباطی معکوس از طرف سیستم قربانی با سیستم نفوذگر برقرار می‌شود. این روش بهتر و مؤثرتر می‌باشد؛ زیرا معمولا ارتباط‌هایی که از درون یک شبکه به سمت بیرون برقرار می‌شود، توسط دیوارهای‌آتش و سامانه‌های امنیتی فیلتر و مسدود نمی‌شوند.
- NoNX[1]: این نوع Payloadها با مکانیزم DEP[2] کار می‌کنند. این Payload کمی از ویژگی‌های ایجاد شده برای برخی پردازنده‌ها به‌منظور جلوگیری از اجرای کد در مناطق مشخصی از حافظه را فراهم می‌کند. در سیستم‌عامل ویندوز، NX به‌وسیله مکانیزم DEP پیاده‌سازی شده است. در ابزار Metasploit، Payloadهای نوع NoNX برای عبور و دور زدن مکانیزم DEP طراحی شده‌اند.

- ماژول Exploit: این ماژول در حین انجام عملیات از ماژول Payload استفاده می‌کند. در واقع Exploit قطعه کدی از نرم‌افزار و تکه‌ای از داده‌ها یا دنباله‌ای از کدها است که برای بهره‌برداری از یک اِشکال و آسیب‌پذیری مورد استفاده قرار می‌گیرد. مفهوم Exploit در این ابزار دقیقا همان مفهوم کدهای بهره‌برداری (Exploit) است که در دنیای هک علیه آسیب‌پذیری‌ها و نقاط ضعف موجود در سرویس‌ها و نرم‌افزارها نوشته می‌شود و از آن برای نفوذ به سیستم هدف استفاده می‌شود. کدهای Exploit به‌طور معمول در دو حالت فعال و غیرفعال (سمت مشتری) پیاده‌سازی و اجرا می‌شود. درحالت فعال کد Exploit پس از اجرا شدن اقدام به باز کردن یک پورت بر روی سیستم هدف می‌کند و در ادامه، ارتباط نفوذگر با سیستم قربانی برقرار می‌شود. در این‌حالت تا لحظه‌ای که عملیات Exploit به پایان نرسد، تبادل اطلاعات با سیستم هدف ادامه پیدا می‌کند. بدین معنی که کد Exploit به اجرای خود ادامه می‌دهد و در نهایت پس از پایان کار از آن بیرون می‌شود. درحالت غیرفعال باید آدرسی توسط کاربر (بر روی سیستم قربانی) اجرا شود تا نفوذگر بتواند به سیستم قربانی متصل شود. در واقع در این نوع کد Exploit برای ورود و نفوذ به سیستم هدف، کد منتظر اتصال می‌ماند تا بتواند به اطلاعات مورد نظر دست یابد. این نوع کدهای Exploit را در اصطلاح

1_No eXecute

2_Data Execution Prevention

کدهای Exploit سمت مشتری نیز می‌نامند که در فصل‌های آینده‌ی کتاب به بررسی آن‌ها خواهیم پرداخت.

- ماژول Encoder: با کمک این نوع از ماژول‌ها می‌توان کدهای Exploit و داده‌های مخرب را به‌گونه‌ای تغییر داد که درخصوص ارسال کد و دریافت آن توسط سیستم مقصد اطمینان کافی به‌دست آید. در واقع ماژول Encoder، برنامه‌ای است که ماژول‌های Payload را به‌گونه‌ای کدگذاری می‌کند تا در مسیر انتقال و در سیستم مقصد توسط نرم‌افزارهای امنیتی و ضدویروس قابل تشخیص نباشند.
- ماژول Nops: از این ماژول برای ثابت نگهداشتن و منطبق کردن اندازه Payload استفاده می‌شود. در واقع از این ابزار برای عبور از امضاها و ساختارهای امنیتی سیستم‌های IDS/IPS استفاده می‌شود.
- ماژول Auxiliary: از این ماژول مفید برای پویش، درهم شکستن و انواع حملات استفاده می‌شود.

در ابزار Metasploit درحالت کلی دو نوع ماژول وجود دارد که نوع نخست را ماژول‌های اولیه و نوع دوم را ماژول‌های ویژه‌ی کاربر می‌نامند. به‌طور معمول محل جای گرفتن ماژول‌های اصلی ابزار Metasploit مسیر نصب ابزار، یعنی مسیری همانند مورد زیر می‌باشد:

/opt/framework3/msf3/modules

اما ماژول‌های ویژه‌ی کاربر در مسیری همانند مورد زیر قرار دارند (در این مثال فرض بر این است که نام‌کاربری مورد نظر برای نصب و راه‌اندازی ابزار Metasploit، حساب‌کاربری root بوده است):

/root/.msf3/modules

گفتنی است که هم اینک در ابزار Metasploit Framework همه‌ی ماژول‌ها براساس کلاس‌های Ruby پیاده‌سازی می‌شوند. در این ابزار همه‌ی ماژول‌ها از کلاس ویژه‌ای به‌نام type-specific ارث‌بری می‌کنند. در واقع، این کلاس نیز از کلاس Msf::Module ارث‌بری می‌کند. در میان ماژول‌ها APIهای معمول به‌اشتراک گذاشته شده‌ای وجود دارند. موضوع در مورد Payloadها کمی متفاوت می‌باشد. Payloadها در زمان اجرا براساس ترکیب‌های گوناگون ایجاد می‌شوند و دربردارنده‌ی مجموعه‌ای از مراحل در کنار یکدیگر می‌باشند. در ساختار کدنویسی مبتنی بر Ruby براساس کلاس‌ها و ماژول‌ها، هر کلاس تنها یک والد خواهد داشت. در این ساختار هر کلاس ممکن است دربردارنده‌ی شمار زیادی ماژول باشد. ماژول‌ها می‌توانند روش‌های جدیدی را ایجاد کنند یا بر روی ماژول قدیمی بازنویسی شوند. ماژول‌های مبتنی بر ابزار Metasploit از Msf::Module ارث‌بری می‌کنند و دربردارنده‌ی ویژگی‌های اضافی می‌باشند.

پلاگین‌ها: پلاگین‌ها در ابزار Metasploit به‌صورت مستقیم با APIها کار می‌کنند. با کمک این ساختار می‌توان چارچوب ابزار را دستکاری کرد. پلاگین‌ها در درون زیرسیستم رویدادها قرار دارند. آن‌ها وظایف ویژه‌ای را به‌صورت خودکار یا دستی انجام می‌دهند. نکته‌ی مهم این است که پلاگین‌ها تنها در واسط کاربری msfconsole کار می‌کنند. واسط‌های کاربری ابزار Metasploit در فصل بعدی به‌طور کامل مورد بررسی قرار می‌گیرد. در واقع پلاگین‌ها می‌توانند کنسول دستورهای جدیدی به ابزار اضافه کنند. با کمک ساختار پلاگین‌ها می‌توان قابلیت‌های کلی Framework گفته شده را گسترش داد.

ابزار Metasploit هم اینک در نسخه‌هایی با نام‌های زیر ارائه و توسعه داده شده است:

Metasploit community, Metasploit express, Metasploit pro

نصب و راه‌اندازی ابزار Metasploit بر روی لینوکس

همان‌گونه که می‌دانید این ابزار به‌طور پیش‌فرض بر روی توزیع‌های لینوکس حرفه‌ای که برای امور نفوذگری و آزمایش نفوذ مورد استفاده قرار می‌گیرند، نصب می‌باشد و می‌توان با واسطهای کاربری ویژه‌ی ابزار، از آن استفاده کرد. از جمله این توزیع‌های لینوکس می‌توان به BackTrack، Kali و BackBOX اشاره کرد. در برخی موارد ممکن است نیاز داشته باشید تا ابزار Metasploit را بر روی یک توزیع لینوکس معمولی نصب کنید. در این بخش برای نمونه عملیات نصب را بر روی توزیع Ubuntu پی می‌گیریم. پس از دریافت ابزار Metasploit از سایت مربوط می‌توان آن‌را به شیوه‌های گوناگونی بر روی سیستم نصب کرد؛ مانند نصب به‌صورت کامل یا با اجرای کمترین دستورات. در هر دو شیوه، نصب به‌فرم زیر می‌باشد:

Full installer:

```
$ chmod +x framework-4.*-linux-full.run
$ sudo ./framework-4.*-linux-full.run
```

Minimal installer:

```
$ chmod +x framework-4.*-linux-mini.run
$ sudo ./framework-4.*-linux-mini.run
```

در برخی توزیع‌ها ممکن است نصب‌های اشاره شده با کد خطا مواجه شود، زیرا ممکن است موارد مربوط به وابستگی‌ها در بسته‌های نرم‌افزاری رعایت نشده باشد. در واقع در برخی از نسخه‌های توزیع Ubuntu کتابخانه‌های مربوط به زبان Ruby ناقص هستند و ممکن است عملیات نصب ابزار با مشکل مواجه گردد. برای نصب و اجرای وابستگی‌های مربوط به زبان Ruby باید بسته‌های نرم‌افزاری زیر نصب شوند:

```
$ sudo apt-get install ruby libopenssl-ruby libyaml-ruby libdl-ruby libiconv-ruby
libreadline-ruby irb ri rubygems
```

همچنین برای نصب زیرنسخه‌های مربوط به کلاینت باید از دستور زیر استفاده کرد:

```
$ sudo apt-get install subversion
```

برای ساخت و اجرای پسوندهای بومی از دستور زیر استفاده می‌شود:

```
$ sudo apt-get install build-essential ruby-dev libpcap-dev
```

پس از نصب وابستگی‌ها، ابزار Metasploit را درحالت Tarball دریافت کنید و با دستورهای زیر آن‌را بر روی سیستم نصب نمایید:

```
$ tar xf framework-4.X.tar.gz
$ sudo mkdir -p /opt/metasploit4
$ sudo cp -a msf4/ /opt/metasploit3/msf4
$ sudo chown root:root -R /opt/metasploit4/msf4
$ sudo ln -sf /opt/metasploit3/msf3/msf* /usr/local/bin/
```

نکته مهم در نصب ابزار Metasploit بر روی توزیع‌های لینوکس این است که بهتر است ماژول‌هایی مانند NET::ssleay و GNU::TERM::readlin نیز برای ابزار نصب شود. این نوع ماژول‌ها در مسیر extra موجود می‌باشند.

فصل دوم

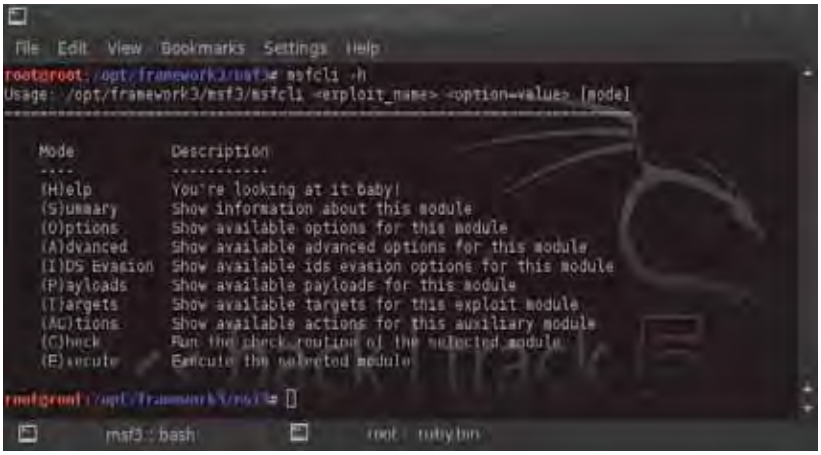
واسط‌های کاربری ابزار Metasploit

هم اینک واسط‌های کاربری گوناگونی برای ابزار Metasploit Framework موجود می‌باشند که هریک نقاط ضعف و قدرت ویژه خود را دارند. بنابراین واسط کاربری کاملی برای ابزار MSF وجود ندارد، اما از میان واسط‌های موجود بهترین و کاربردی‌ترین آن‌ها واسط کاربری msfconsole است که در این فصل زمان بیشتری برای این نوع واسط در نظر گرفته شده است. این واسط توانمندی ویژه‌ای برای دسترسی به ویژگی‌های ابزار MSF دارد و نسبت به واسط‌های دیگر حرفه‌ای‌تر و به‌مراتب کار با آن آسان‌تر می‌باشد. برخی از واسط‌های کاربری ابزار MSF به فرم گرافیکی و یا تحت وب ارائه شده‌اند، اما از دیدگاه نفوذگران، واسط کاربری msfconsole نسبت به واسط‌های دیگر کامل‌تر، کاربر پسندتر و حرفه‌ای‌تر می‌باشد. در ابتدای فصل به بررسی دیگر واسط‌های کاربری ابزار MSF می‌پردازیم و در پایان به بررسی کامل واسط کاربری msfconsole می‌پردازیم.

واسط کاربری msfcli

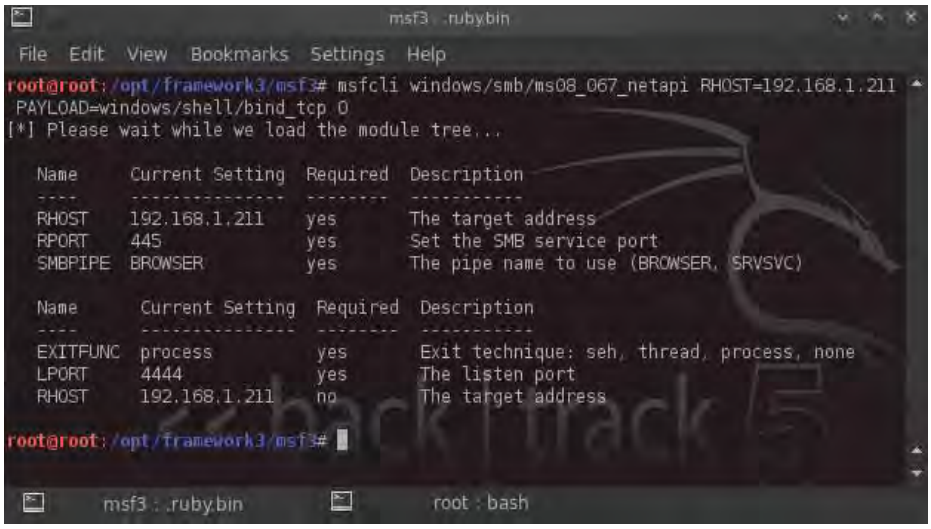
واسطی تقریبا کامل برای ابزار MSF است. از دیدگاه توانایی‌ها و قابلیت‌ها، واسط کاربری msfcli تا حدودی همانند msfconsole است، اما در برخی ساختارها و امکانات ضعف‌هایی در آن دیده می‌شود. در واقع تنظیمات مربوط به حمله در ابزار msfconsole را می‌توان در خط‌فرمان و در قالب یک دستور پیاده‌سازی کرد. خروجی دستور زیر در قالب خط‌فرمان به کاربر نمایش داده می‌شود. واسط کاربری msfcli، از بیشتر اسکریپت‌های ابزار MSF پشتیبانی می‌کند. همچنین بیشتر ماژول‌های ابزار MSF همانند exploit و auxiliary را می‌توان با این واسط اجرا کرد. نکته‌ی مهم در این نوع واسط کاربری این است که واسط گفته شده به استفاده از حروف کوچک و بزرگ در گزینه‌ها حساس است و باید متغیرهای اختصاص داده شده با استفاده از علامت مساوی (=) تعیین شوند.

چنانچه از دستور msfcli به‌صورت تکی در توزیع BackTrack استفاده شود، ابتدا ماژول‌های مورد نیاز ابزار MSF بارگذاری می‌شود و می‌توان از آن‌ها برای پیاده‌سازی حمله استفاده کرد. شمایی از سوئیچ‌های دستور msfcli در توزیع BackTrack در شکل (1-2) نشان داده شده است.



شکل (2-1) شمایی از سوئیچ‌های دستور msfcli در توزیع BackTrack

برای نمایش گزینه‌ها و متغیرهای مربوط به Options باید در انتهای دستور msfcli از سوئیچ O استفاده کرد. از این گزینه در مواردی که اطلاعات کافی از گزینه‌های موجود در بخش Options وجود ندارد استفاده می‌شود تا پس از مشاهده متغیرهای مورد نیاز بتوان مقادیر مورد نظر را تکمیل کرد. شمایی از چگونگی استفاده و خروجی این سوئیچ در شکل (2-2) نشان داده شده است.



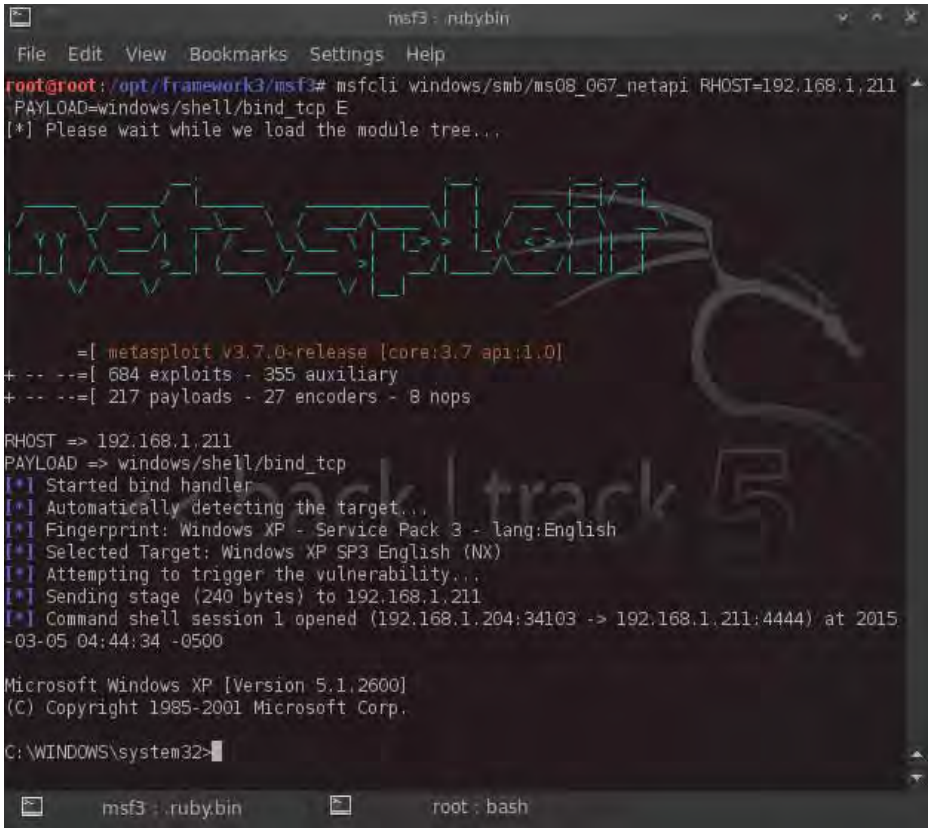
شکل (2-2) شمایی از چگونگی استفاده و خروجی سوئیچ O در دستور msfcli

همان‌گونه که در شکل (2-2) مشخص است، گزینه‌های دستور، دربردارنده‌ی پارامتر مربوط به Exploit و پارامتر مربوط به PAYLOAD و همچنین آدرس IP سیستم مقصد می‌باشد که باید متغیر RHOST مقداردهی شود.

یعنی باید مقدار متغیر RHOST[3] با آدرس IP سیستم هدف مقداردهی شود. گزینه‌های دیگری نیز در متغیرهای ویژه‌ی ماژول‌ها وجود دارند که دربردارنده‌ی LHOST[4]، RPORT[5] و LPORT[6] می‌باشند. از سوئیچ P نیز می‌توان برای نمایش Payloadهای موجود در ابزار استفاده کرد. این دستور به‌فرم زیر خواهد بود:

```
root@bt:/opt/framework3/msf3# msfcli windows/smb/ms08_067_netapi
RHOST=192.168.1.211 P
```

پس از اینکه نوع Payload مشخص شد می‌توان از دستور msfcli برای انجام حمله همانند شکل (3-2) اقدام کرد.



شکل (3-2) شمایی از چگونگی استفاده از واسط کاربری msfcli برای پیاده‌سازی مکانیزم حمله

3_Remote HOST

4_Local HOST

5_Remote PORT

6_Local PORT

واسط کاربری msfweb

واسط کاربری msfweb دارای رابطی بسیار ساده و کاربرپسند است که با رابط Ajax-y طراحی و پیاده‌سازی شده است. ابزار MSF یک سرور وب ویژه‌ی خود دارد و از آن برای فعال‌سازی واسط کاربری msfweb استفاده می‌کند. به‌طور معمول برای آزمایش‌های نفوذ در سطح وسیع، ابزار MSF را بر روی یک سرور با پهنای‌باند بالا نصب می‌کنند و در ادامه با واسط کاربری وب به آن متصل می‌شوند. نکته‌ی مهم آن است که برای سرویس‌دهنده‌ی وب این ابزار و مکانیزم اتصال به آن هیچ‌گونه تمهیدات امنیتی در نظر گرفته نشده است و هر کاربری می‌تواند در صورت فعال بودن سرویس مربوطه، به سرور مورد نظر متصل شود و از خدمات آن استفاده نماید. البته گفتنی است که اگر تنظیمات پیش‌فرض ابزار در نظر گرفته شود، تنها سیستم سرویس‌دهنده می‌تواند از خدمات ابزار استفاده کند که در این‌حالت باید با کمک سوئیچ a- ابزار و آدرس IP سیستم شبکه، به وسیله شبکه نیز به آن متصل شد. نمونه‌ای از چگونگی استفاده از این ابزار در سطح شبکه به‌فرم زیر می‌باشد:

```
root@bt:~# msfweb -a 192.168.1.211
```

این واسط کاربری هم اکنون از قالب ابزار Metasploit حذف شده است و استفاده از آن توصیه نمی‌شود، زیرا نسبت به حملات XSS آسیب‌پذیر می‌باشد و از لحاظ امنیتی، تمهیداتی برای آن در نظر گرفته نشده است. شمایی از محیط این واسط کاربری در توزیع BackTrack در شکل (4-2) نشان داده شده است.

شکل (4-2) شمایی از محیط واسط کاربری msfweb در توزیع BackTrack

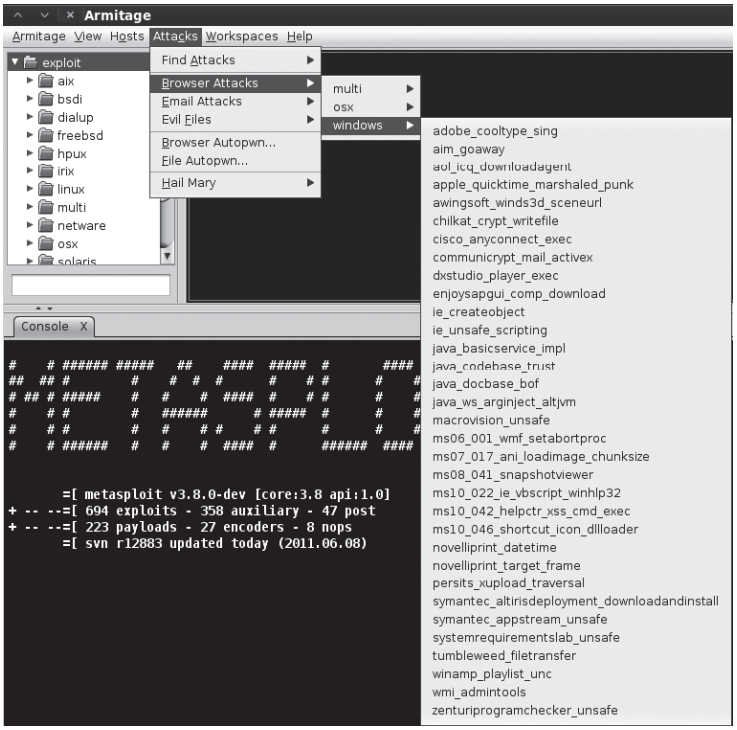
این واسط کاربری از کاربران، Payloadها، Encoderها و غیره پشتیبانی می‌کند و مبتنی بر زبان AJAX پیاده‌سازی شده است.

واسط کاربری Armitage

واسط کاربری Armitage، یکی از رابط‌های گرافیکی کاملا محاوره‌ای و فعال برای اتصال به ابزار Metasploit می‌باشد که توسط Raphael Mudge نوشته شده است. این واسط کاربری بسیار شگفت‌انگیز است و دارای ویژگی‌های متعددی می‌باشد و به‌صورت رایگان ارائه می‌شود. این ابزار دارای قابلیت‌های گرافیکی جذابی می‌باشد که می‌توان از آن‌ها برای اهداف حمله استفاده کرد. نمونه‌ای از چگونگی اجرای این واسط کاربری به‌فرم زیر می‌باشد:

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

شمایی از محیط گرافیکی ابزار armitage در شکل (2-5) نشان داده شده است.



شکل (2-5) شمایی از محیط گرافیکی ابزار armitage

واسط کاربری msfgui

واسط کاربری گرافیکی دیگری نیز برای ابزار Metasploit وجود دارد که با نام msfgui شناخته می‌شود. از این ابزار معمولا در سیستم‌های کلاینت و به‌منظور مدیریت ابزار MSF استفاده می‌شود. از واسط کاربری گفته شده برای پیاده‌سازی و استفاده از کدهای Exploit در محیط گرافیکی استفاده می‌شود. واسط گفته شده از رابط msfconsole نیز پشتیبانی می‌کند و برای دسترسی به آن با محیط واسط کاربری msfgui، می‌توان از منوی

Console موجود در واسط msfgui استفاده کرد. این ابزار قابلیت‌های بسیاری دارد، اما در برخی موارد توانایی رقابت با واسط کاربری msfconsole را ندارد. در نسخه‌های جدید ابزار Metasploit، نسخه جدید این رابط کاربری ارائه شده است که به‌وسیله ScriptJunkie در مخازن SVN ابزار Metasploit پیاده‌سازی شده است. این واسط کاربری دارای چندین سکو است و مبتنی بر جاوا می‌باشد. این واسط کاربری جدید را می‌توان با استناد به اسکریپت msfgui در دایرکتوری اصلی ابزار Metasploit اجرا کرد. برای اجرای این ابزار همانند اجرای واسط کاربری msfgui از دستور زیر استفاده می‌شود:

```
root@bt:~# ./msfgui
```

این اسکریپت پس از اجرا دستور زیر را اجرا می‌کند:

```
java -jar 'dirname $0'/data/gui/msfgui.jar
```

پس از اینکه ساختار گرافیکی جاوا بر روی سیستم نصب و راه‌اندازی شد، باید شمایی از محیط گرافیکی واسط کاربری جدید msfgui همانند شکل (6-2) نشان داده شود.

شکل (6-2) شمایی از محیط گرافیکی واسط کاربری جدید msfgui

همچنین می‌توان با دایمون msfrpcd و با کمک واسط کاربری msfgui به سیستمی که ابزار Metasploit بر روی آن نصب است، متصل شد. برای این منظور ابتدا باید دایمون msfrpcd را بر روی سیستم مورد نظر راه‌اندازی کرد. این‌کار به‌فرم زیر انجام می‌شود:

```
root@test:~# ./msfrpcd -S -U MetaUser -P Securepass -p 1337
```

در این‌حالت دایمون msfrpcd درحالتی‌که SSL غیرفعال است، شروع به‌کار می‌کند. در این دستور با سوئیچ U- نام‌کاربری و با سوئیچ P- گذرواژه و با استفاده از سوئیچ p- شماره پورت برای اتصالات ورودی مشخص می‌شود. در این ساختار سرویس بر روی آدرس 0.0.0.0 راه‌اندازی می‌شود، درنتیجه دایمون گفته شده بر روی همه‌ی واسط‌های شبکه فعال می‌شود. اگر بخواهید دایمون بر روی واسط شبکه ویژه‌ای فعال شود، باید آدرس IP واسط

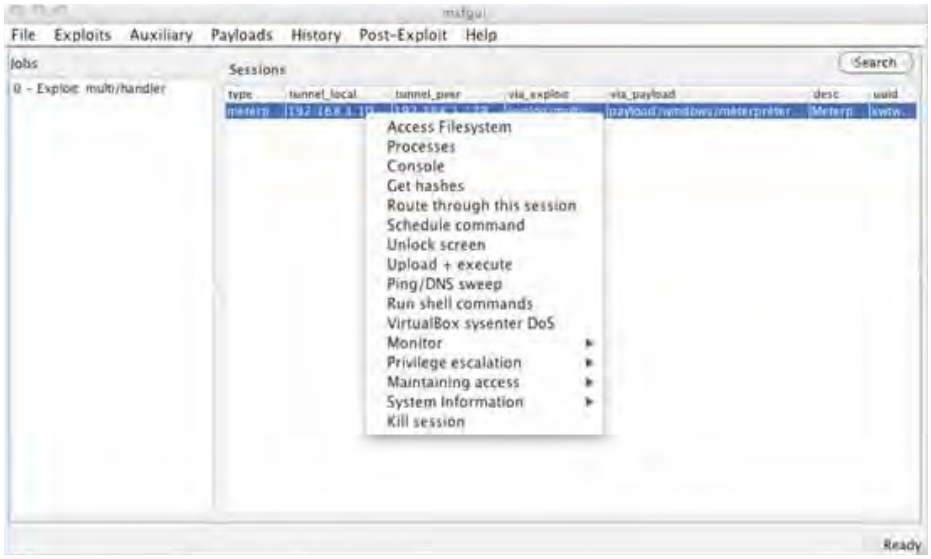
شبکه گفته شده را با کمک سوئیچ a- به دستور اعلام کنید. درحالت کلی زمانی‌که دستور گفته شده بر روی سیستم اجرا می‌شود، خروجی همانند حالت زیر نمایش داده خواهد شد:

```
t:msf3 test$ ./msfrpcd -S -U MetaUser -P Securepass -p 1337
[*] XMLRPC starting on 0.0.0.0:1337 (NO SSL):Basic...
[*] XMLRPC initializing...
[*] XMLRPC backgrounding...
```

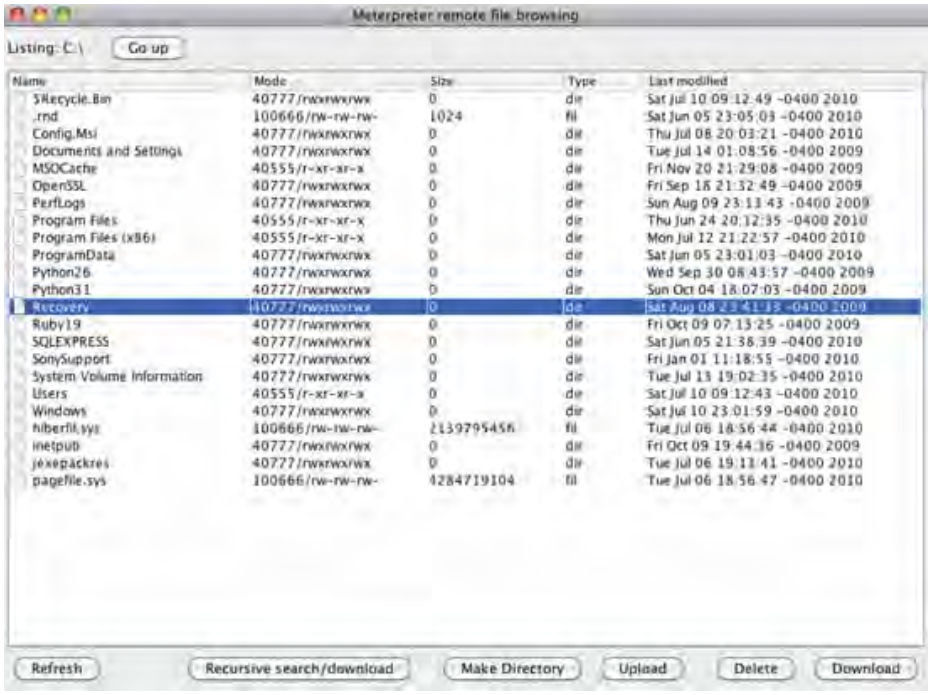
پس از فعال شدن msfrpcd بر روی پورت شماره 1337، می‌توان از ابزار msfgui برای اتصال به پورت گفته شده استفاده کرد. برای انجام این‌کار از گزینه File→Connect to msfrpcd در ابزار msfgui برای اتصال به گزینه‌های msfrpcd استفاده می‌شود. در پنجره‌ی باز شده، از نام‌کاربری و گذرواژه تعریف شده در دایمون msfrpcd استفاده می‌شود. شمایی از منوهای فعال شده‌ی واسط کاربری پس از اتصال به دایمون msfrpcd در شکل (2-7) نشان داده شده است.

شکل (2-7) **شمایی از منوهای فعال شده‌ی واسط کاربری پس از اتصال به دایمون msfrpcd**

همچنین نمونه‌ای از چگونگی استفاده از واسط کاربری msfgui و نفوذ به سیستم هدف در شکل‌های (2-8) و (2-9) نشان داده شده است.



شکل (2-8) شمایی از چگونگی استفاده از واسط کاربری msfgui و نفوذ به سیستم هدف



شکل (2-9) از چگونگی استفاده از واسط کاربری msfgui و نفوذ به سیستم هدف

واسط کاربری msfconsole

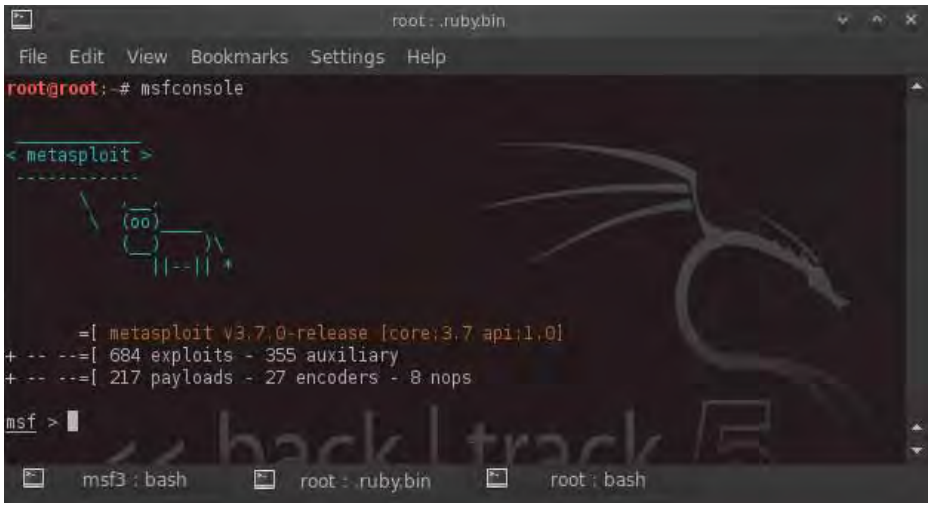
با استفاده از این واسط کاربری می‌توان به همه‌ی ویژگی‌ها و امکان‌های ابزار قدرتمند Metasploit دسترسی پیدا کرد. این واسط کاربری کاملا انعطاف‌پذیر است و به آسانی می‌توان از امکان‌های ابزار گفته شده استفاده کرد. در این واسط کاربری، نفوذگر یا کارشناس امنیت، به همه‌ی ماژول‌ها، پلاگین‌ها و پایگاه‌های‌داده‌ی ابزار Metasploit دسترسی خواهد داشت و می‌تواند از هر کدام از این ویژگی‌ها که دارای امکان‌های گوناگونی هستند، برای پیاده‌سازی آزمایش‌ها و حملات استفاده کند. در واقع همه‌ی این امکان‌ها در یک واسط متمرکز شده است و هم اینک جزو بهترین و محبوب‌ترین واسط‌های کاربری برای استفاده از ابزار Metasploit به‌شمار می‌آید. چنانچه با دستورهای این واسط کاربری آشنا شوید، محیط این رابط برای شما بسیار لذت‌بخش خواهد شد. می‌توان گفت واسط کاربری msfconsole هم اینک پایدارترین رابط ابزار MSF است که پشتیبانی کاملی از مکانیزم‌های readline و tabbing دارد. نکته‌ی مهم در این باره این است که در قالب این واسط کاربری می‌توان دستورهای خارجی و ویژه‌ی خطفرمان لینوکس را اجرا کرد. برای دسترسی به این واسط کاربری با خطفرمان در توزیع حرفه‌ای BackTrack می‌توان به مسیرهای زیر مراجعه کرد. شمایی از محیط اصلی واسط کاربری msfconsole در شکل (10-2) نشان داده شده است.

root@bt:~# /opt/framework3/msf3/msfconsole

root@bt:~# /pentest/exploits/framework3/msfconsole

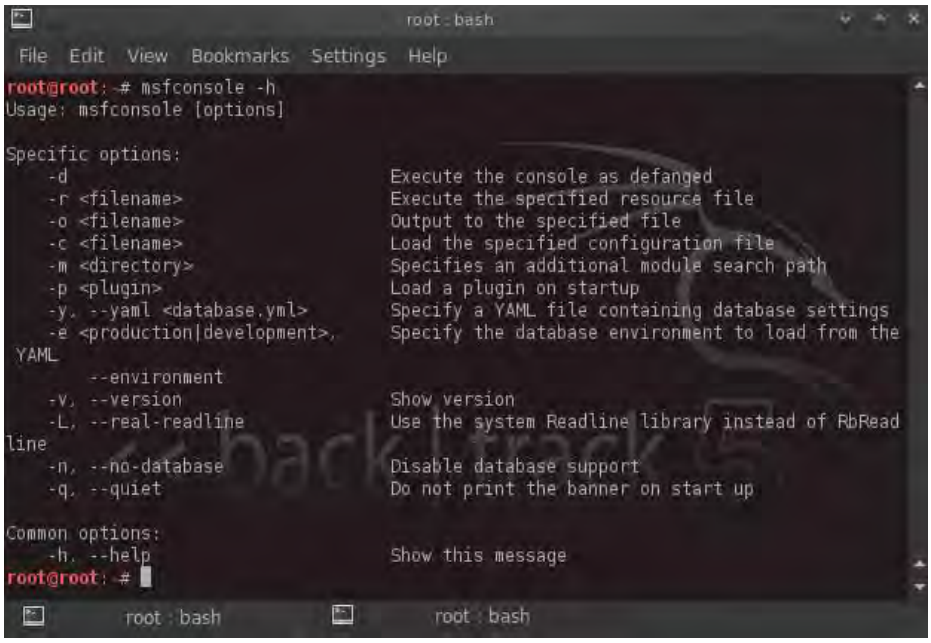
همچنین برای دسترسی به این واسط کاربری، در منوی گرافیکی توزیع BackTrack از مسیر زیر اقدام می‌کنیم:

Applications→Exploitation tools→Network exploitation tools→Metasploit framework→msfconsole



شکل (10-2) شمایی از محیط اصلی واسط کاربری msfconsole

همچنین می‌توان با کمک سوئیچ h- این واسط کاربری در بیرون از محیط اصلی از گزینه‌ها و سوئیچ‌های دیگر این ابزار آگاهی یافت. شمایی از سوئیچ‌های این واسط کاربری در شکل (11-2) نشان داده شده است.

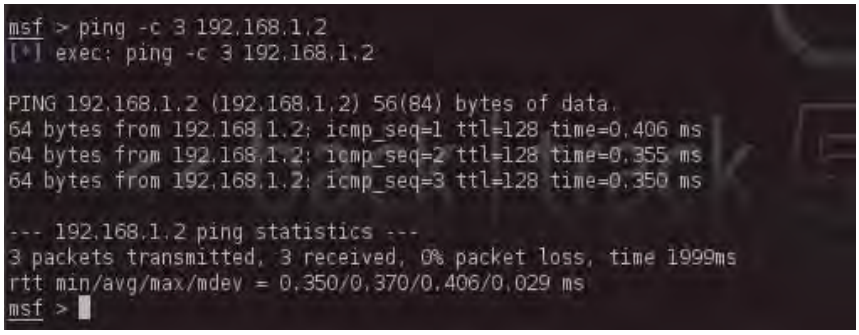


شکل (11-2) شمایی از سوئیچ‌های واسط کاربری msfconsole

پس ورود به محیط واسط کاربری msfconsole می‌توان با کمک دستور help یا علامت ؟، از دستورهای دیگر واسط کاربری گفته شده آگاه شد. شمایی از بخشی از دستورهای واسط کاربری msfconsole در شکل (12-2) نشان داده شده است.

شکل (2-12) **شمایی از بخشی از دستورهای واسط کاربری msfconsole**

همان‌گونه که گفته شد، افزون بر دستورهای اصلی واسط کاربری msfconsole، می‌توان در این محیط از دستورهای خطفرمان لینوکس که در این‌جا به آن‌ها دستورهای خارجی می‌گوییم، استفاده کرد. نمونه‌ای از چگونگی استفاده از دستور ping در محیط واسط کاربری msfconsole در شکل (2-13) نشان داده شده است.



شکل (2-13) **نمونه‌ای از چگونگی استفاده از دستور ping در محیط واسط کاربری msfconsole**

همچنین از دستور ls برای مشاهده فایل و دایرکتوری‌های مسیر جاری که واسط کاربری msfconsole از آن مسیر اجرا شده است، استفاده می‌شود. از دستور msfupdate نیز به‌منظور به‌روزرسانی ابزار Metasploit به‌همراه ماژول‌ها، کدهای Exploit، کتابخانه‌ها و عناصر دیگر این ابزار استفاده می‌شود. در حالت کلی دستورهای استاندارد واسط کاربری msfconsole در دو طبقه‌بندی دستورهای هسته (مفید) و دستورهای پایگاه‌داده قرار می‌گیرند. این طبقه‌بندی در هنگام استفاده از دستور help نیز قابل مشاهده است. گفتنی است که در این محیط هنگام استفاده از دستورها، ماژول‌ها، Exploitها و عناصر دیگر، قابلیت استفاده از کلید Tab همانند محیط خط‌فرمان سیستم‌عامل لینوکس، فعال می‌باشد و این نکته می‌تواند کمک به‌سزایی در یافتن عنصر مورد نظر کند. از دستور help برای آشنایی بیشتر در مورد چگونگی عملکرد هر یک از دستورهای واسط کاربری نیز می‌توان استفاده کرد. برای نمونه می‌توان دستور help را در محیط واسط کاربری گفته شده وارد کرد و در ادامه با دوبار زدن کلید Tab، لیست دستورها و پایگاه‌های‌داده‌ای که دستور help در مورد آن‌ها اطلاعاتی در اختیار دارد، را مشاهده کرد. نمونه‌ای از این‌حالت به‌فرم زیر می‌باشد:

```
msf> help connect
```

در این فصل به بررسی دستورهای هسته یا همان دستورهای مفید واسط کاربری msfconsole می‌پردازیم و دستورهای مبتنی بر پایگاه‌های‌داده را در فصل بعدی معرفی و بررسی خواهیم کرد. دستور help در واسط کاربری گفته شده در هر بخشی قابل استفاده می‌باشد. برای نمونه اگر در شاخه یک ماژول ویژه استفاده شود، دستورهایی که می‌توان در قالب آن ماژول از آن‌ها استفاده کرد، نمایش داده می‌شود. اینک در ادامه‌ی این بخش به بررسی و معرفی دستورهای هسته‌ی واسط کاربری msfconsole می‌پردازیم. گفتنی است که بیشتر دستورهای موجود در واسط کاربری msfconsole دارای گزینه help برای یادگیری بیشتر می‌باشند که با کمک سوئیچ h- آن دستور قابل نمایش می‌باشند:

دستور back: از این دستور برای بازگشت از محیط جاری مربوط به یک ماژول به اعلان اصلی واسط کاربری استفاده می‌شود. این حالت در شکل (14-2) نشان داده شده است.

```
msf exploit(symantec_rtvscan) > back
msf >
```

شکل (14-2) شمایی از چگونگی استفاده از دستور back

دستور banner: از این دستور برای نمایش بنر نخستین واسط کاربری msfconsole استفاده می‌شود. در این بنر اطلاعاتی در مورد ماژول‌ها و نسخه ابزار Metasploit ارائه می‌شود. شمایی از محیط بنر واسط کاربری msfconsole در شکل (15-2) نشان داده شده است.