Metasploit 渗透测试指南读书笔记一到四章

第一章渗透测试技术基础

第二章Metasploit 基础

Armitage 是 metasploit 的图形界面

注：1.2 两章没什么好写的，此处省略。

千里之堤，毁于蚁穴，千里长的堤坝就因为一个小小的蚁穴而毁了，可见小小的蚁穴是多么的重要。在网络世界也是同样的，看似安全的网络，一旦被别人发现小小的蚁穴，那就意味这个网络没有什么安全可言了。那要怎么才能找到这个蚁穴了？？因此接下来的两章显的尤为重要。（情报收集和漏洞扫描）

第三章情报收集

3.1 被动信息收集（间接的信息收集）

3.1.1 whois 查询

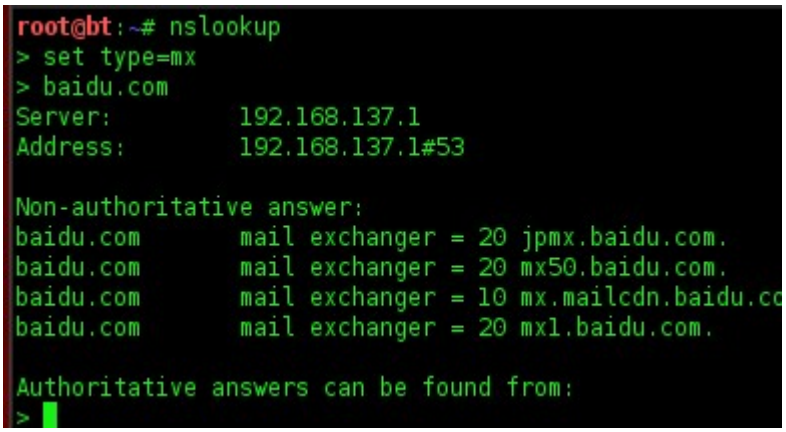
```
msf > whois baidu.com
[*] exec: whois baidu.com


Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Server Name: BAIDU.COM.ZZZZZZ.COM.MORE.INFO.AT.WWW.BEYONDWHOIS.COM
   IP Address: 203.36.226.2
   Registrar: INSTRA CORPORATION PTY, LTD.
   Whois Server: whois.instra.net
   Referral URL: http://www.instra.com

   Server Name: BAIDU.COM.ZZZZZ.GET.LAID.AT.WWW.SWINGINGCOMMUNITY.COM
   IP Address: 69.41.185.203
   Registrar: TUCOWS.COM CO.
   Whois Server: whois.tucows.com
   Referral URL: http://domainhelp.opensrs.net

   Server Name: BAIDU.COM.S18.4BO.CN
   Registrar: XIN NET TECHNOLOGY CORPORATION
   Whois Server: whois.paycenter.com.cn
   Referral URL: http://www.xinnet.com

   Server Name: BAIDU.COM.MORE.INFO.AT.WWW.BEYONDWHOIS.COM
   IP Address: 203.36.226.2
```

3.1.2 Netcraft

Netcraft 是一个网页界面的工具（http://searchdns.netcraft.com/）

Site	http://www.baidu.com	**Last reboot**	unknown Uptim
Domain	baidu.com	**Netblock owner**	CHINANET Beijing provin
IP address	220.181.111.147	**Site rank**	457
Country	CN	**Nameserver**	dns.baidu.com
Date first seen	November 1999	**DNS admin**	sa@baidu.com
Domain Registrar	markmonitor.com	**Reverse DNS**	unknown
Organisation	Beijing Baidu Netcom Science Technology Co., Ltd., 3F Baidu Campus No.10 Shangdi 10th Street Haidian District, Beijing, 100085, China	**Nameserver Organisation**	Beijing Baidu Netcom Sci Campus No.10 Shangdi 100085, China
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

3.1.3Nslookup



查询邮件服务器

注：mx 记录：邮件服务器记录

A 记录：正向解析

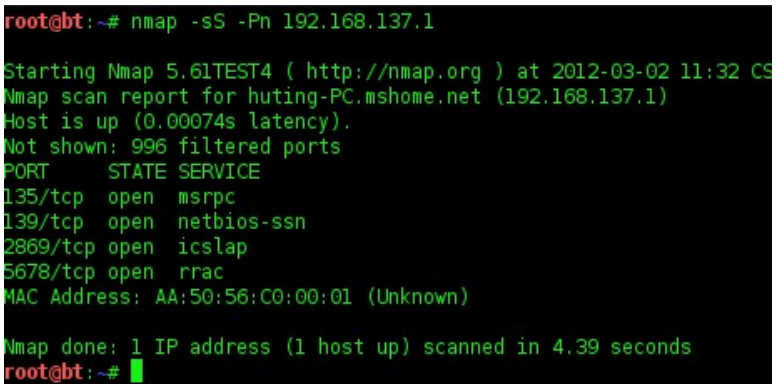
3.2 主动信息收集

3.2.1 使用 nmap 进行端口扫描

-A 尝试进行深入的服务枚举和旗标获取

-sS 使用它来执行一次隐秘的 tcp 扫描

-Pn 不要使用 ping 预测主机的存活



```
root@bt:~# nmap -Pn -sS -A 192.168.137.1

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-02 13:20 CST
Nmap scan report for huting-PC.mshome.net (192.168.137.1)
Host is up (0.00049s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE     VERSION
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn
2869/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5678/tcp open  rrac?
MAC Address: AA:50:56:C0:00:01 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista cpe:
/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Wi
ndows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server 2
008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.49 ms huting-PC.mshome.net (192.168.137.1)

OS and Service detection performed. Please report any incorrect results at http://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.87 seconds
root@bt:~#
```

3.2.2 在 Metasploit 中使用数据库

这里有点小疑问，书上讲，首先要启动 postgresql 数据库，再进入 msf 里面来连接 postgresql 数据库，但我的 bt5 里进入 msf 就默认连接了 postgresql 数据库。怪的就是我想去启动 postgresql 数据库时根本就没有那玩意。

```
root@bt:~# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.3.0-dev [core:4
+ -- --=[ 806 exploits - 451 auxiliary
+ -- --=[ 246 payloads - 27 encoders -
       =[ svn r14815 updated 4 days ago

msf > db_
db_connect     db_export      db_nmap
db_disconnect  db_import      db_status
msf > db_status
[*] postgresql connected to msf3
msf >
```

看见了吧！进去就显示连接上了这个数据库。

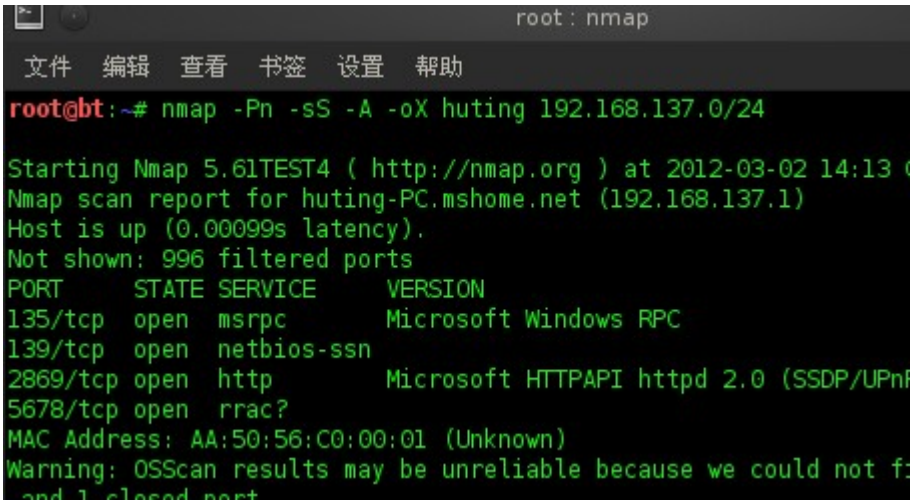
下面是书上的原文：

root@bt:~# /etc/init.d/postgresql-8.3 start （启动 postgresql 数据库）

msf > db_connect postgres:toor@127.0.0.1/msfbook （连接 postgresql 数据库）

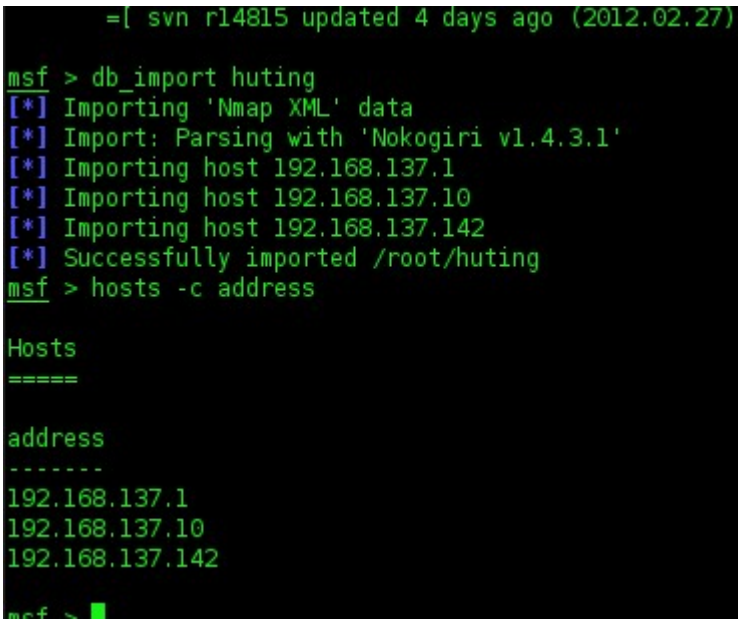
1.将 nmap 输出的结果导入 metasploit

使用-oX 选项进行扫描生 huting.xml 的文件



注：这是对 137 网段进行扫描

Xml 文件生成后，我们用 db_import 命令将文件导入到数据库中



注;以前的版本里面是 db_hosts,我这里的是 hosts，hosts -c address 这是查看主机。

这里我补充一点，自动攻击，明教教主的视频里讲过了的。

还有就是你的 msf 可能没有 db_autopwn ， 怎么办了？、

呵呵！不怕这里有详细的办法：
http://hi.baidu.com/%D5%F1%CF%A3/blog/item/92c32a4816fc759db3b7dc76.html

只要按照上面做就 ok 了。

```
msf > hosts

Hosts
=====

address          mac                name                os_name           os_
vor  os_sp  purpose  info  comments
-------          ---                ----                -------           ---
---  -----  -------  ----  --------
192.168.137.1    AA:50:56:C0:00:01  huting-PC.mshome.net  Microsoft Windows  Vis
           device
192.168.137.10   00:0C:29:A1:46:EE                      Linux              2.4
           device
192.168.137.142  00:0C:29:89:E9:5E  ttpp.mshome.net       Microsoft Windows  XP
           device

msf >
msf >
msf >
msf > db_autopwn -p -t -e
```

注：就是 msf > db_autopwn -p -t -e
它会根据扫描结果自动选择模块来攻击

2.高级 nmap 扫描技巧：tcp 空闲扫描
这种扫描能让我们冒充另一台主机的 ip 地址，对目标进行更为隐秘的扫描。
第一步：寻找满足 tcp 空闲扫描要求的空闲主机

```
msf > 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 inte
   RHOSTS                      yes       The target address r
r
   RPORT      80               yes       The target port
   SNAPLEN    65535            yes       The number of bytes
   THREADS    1                yes       The number of concur
   TIMEOUT    500              yes       The reply read timed

msf  auxiliary(ipidseq) >
```

选取模块

```
msf  auxiliary(ipidseq) > set RHOSTS 192.168.137.0/24
RHOSTS => 192.168.137.0/24
msf  auxiliary(ipidseq) > set THREADS 50
THREADS => 50
msf  auxiliary(ipidseq) > run
```

设置模块

注：RHOSTS 是目标，可以是一台主机，也可以是一个网段，
这里是一个网段。THREADS 是线程，这里设置为 50.

```
msf  auxiliary(ipidseq) > run

[*] Error: 192.168.137.27: #<Class:0xdac89f8> execution expirec
[*] Error: 192.168.137.38: #<Class:0xac7e50c> execution expirec
[*] Scanned 035 of 256 hosts (013% complete)
[*] Scanned 071 of 256 hosts (027% complete)
[*] Scanned 082 of 256 hosts (032% complete)
[*] 192.168.137.142's IPID sequence class: Incremental!
[*] Scanned 115 of 256 hosts (044% complete)
[*] Scanned 131 of 256 hosts (051% complete)
[*] Scanned 178 of 256 hosts (069% complete)
[*] Scanned 196 of 256 hosts (076% complete)
[*] Scanned 225 of 256 hosts (087% complete)
[*] Scanned 246 of 256 hosts (096% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(ipidseq) >
```

扫描结果

得知 192.168.137.142 这台主机符合，可用其作为空闲主机对目标主机进行扫描

```
msf  auxiliary(ipidseq) > nmap -PN -sI 192.168.137.142 192.168.137.1
[*] exec: nmap -PN -sI 192.168.137.142 192.168.137.1


Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-02 15:07 CST
Idle scan using zombie 192.168.137.142 (192.168.137.142:80); Class: Incremental
Nmap scan report for huting-PC.mshome.net (192.168.137.1)
Host is up (0.049s latency).
Not shown: 996 closed|filtered ports
PORT     STATE SERVICE
```

3 在 msf 终端中运行 nmap

```
msf > db_nmap -sS -A 192.168.137.0/24
[*] Nmap: Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-
[*] Nmap: Nmap scan report for huting-PC.mshome.net (192.168.13
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: Not shown: 996 filtered ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 135/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 2869/tcp open  http        Microsoft HTTPAPI httpd 2.
[*] Nmap: 5678/tcp open  rrac?
[*] Nmap: MAC Address: AA:50:56:C0:00:01 (Unknown)
[*] Nmap: Warning: OSScan results may be unreliable because we
ast 1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 2008|7|Vista
[*] Nmap: OS details: Microsoft Windows Server 2008, Microsoft
al, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
```

```
msf > hosts

Hosts
=====

address          mac                name                 os_name           os_fl
vor  os_sp  purpose  info  comments
-------          ---                ----                 -------           -----
---  -----  -------  ----  --------
192.168.137.1    AA:50:56:C0:00:01  huting-PC.mshome.net  Microsoft Windows  2008
           device
192.168.137.10   00:0C:29:A1:46:EE                       Linux              2.4.X
           device
192.168.137.142  00:0C:29:89:E9:5E  ttpp.mshome.net       Microsoft Windows  XP
           device
```

查看扫描到的主机信息

```
msf > services

Services
========

host             port   proto  name         state  info
----             ----   -----  ----         -----  ----
192.168.137.1    135    tcp    msrpc        open   Microsoft Windows RPC
192.168.137.1    139    tcp    netbios-ssn  open
192.168.137.1    5678   tcp    rrac         open
192.168.137.1    2869   tcp    http         open   Microsoft HTTPAPI httpd 2.0 SSD
/UPnP
192.168.137.10   32768  tcp    status       open   1 rpc #100024
192.168.137.10   22     tcp    ssh          open   OpenSSH 3.5p1 protocol 1.99
192.168.137.142  135    tcp    msrpc        open   Microsoft Windows RPC
192.168.137.142  139    tcp    netbios-ssn  open
192.168.137.142  2869   tcp    http         open   Microsoft HTTPAPI httpd 1.0 SSD
/UPnP

msf >
```

查看扫描到的主机的服务

3.2.3 使用 metasploit 进行端口扫描

```
msf > search portscan

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

   Name                                    Disclosure Date  Rank    Description
   ----                                    ---------------  ----    -----------
   auxiliary/scanner/natpmp/natpmp_portscan                 normal  NAT-PMP External Port Scanner
   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
```

这些都是 metasploit 框架提供的端口扫描工具

实例：使用 metasploit 的 SYN 的端口扫描器对单个主机进行一次简单的扫描

```
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. 22-25,80,110-90
   RHOSTS                      yes       The target address range or CIDR id
   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 milliseco
```

选取扫描模块，查看参数设置

```
msf  auxiliary(syn) > set RHOSTS 192.168.137.1
RHOSTS => 192.168.137.1
msf  auxiliary(syn) > set THREADS 50
THREADS => 50
msf  auxiliary(syn) > run

[*]  TCP OPEN 192.168.137.1:135
[*]  TCP OPEN 192.168.137.1:139
```

设置参数，运行扫描。

3.3 针对性的扫描

3.3.1 服务器消息块协议（smb）扫描

Msf 利用 smb_version 模块来遍历网络并获取 window 系统的版本号。

```
msf > use auxiliary/scanner/smb/smb_version
msf  auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identi
fier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentic
ation
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf  auxiliary(smb_version) >
```

```
msf  auxiliary(smb_version) > set RHOSTS 192.168.137.1
RHOSTS => 192.168.137.1
msf  auxiliary(smb_version) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(smb_version) >
```

设置参数，运行。（注：线程参数 THREADS 可以设置的，默认是 1，设置越大扫描越快。）

```
msf  auxiliary(smb_version) > hosts

Hosts
=====

address  mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------  ---  ----  -------  ---------  -----  -------  ----  --------

msf  auxiliary(smb_version) >
```

这里有疑问，我这里怎么没有扫描出来了？？？？？

3.3.2 搜索配置不当的 microsoft SQL Server

```
msf > use auxiliary/scanner/mssql/mssql_ping
msf  auxiliary(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 specified username
   RHOSTS                                yes       The target address range or CIDR identifie
   THREADS              1                yes       The number of concurrent threads
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification

msf  auxiliary(mssql_ping) >
```

注：MS sql 安装后默认监听 tcp 的 1433 端口

```
msf  auxiliary(mssql_ping) > set RHOSTS www.[redacted].com/24
RHOSTS => www.hunangy.com/24
msf  auxiliary(mssql_ping) > set THREADS 255
THREADS => 255
msf  auxiliary(mssql_ping) > run
```

我这里由于网络环境的关系，没有成功，上面是参数的设置。

```
659 284.097377 192.168.137.60  58.20.53.252  UDP  43 Source port: 39287  Desti
660 284.097720 192.168.137.60  58.20.53.249  UDP  43 Source port: 47231  Desti
661 284.097929 192.168.137.60  58.20.53.253  UDP  43 Source port: 34954  Desti
662 284.098301 192.168.137.60  58.20.53.250  UDP  43 Source port: 34921  Desti
663 284.098538 192.168.137.60  58.20.53.237  UDP  43 Source port: 42543  Desti
```

这是我抓的包，只有出去的莫有回来的，所以啥都莫有。所以我觉得可能是网络环境的问题。

3.3.3 SSH 服务扫描

```
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 ide
   RPORT    22               yes       The target port
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  30               yes       Timeout for the SSH probe
```

使用模块，列出参数。

```
msf  auxiliary(ssh_version) > set THREADS 50
THREADS => 50
msf  auxiliary(ssh_version) > set RHOSTS 192.168.137.10
RHOSTS => 192.168.137.10
msf  auxiliary(ssh_version) > run

[*] 192.168.137.10:22, SSH server version: SSH-1.99-OpenSSH_3.5p1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(ssh_version) >
```

设置参数，运行扫描。

```
[*] 192.168.137.10:22, SSH server version: SSH-1.99-OpenSSH_3.5p1
```

这就是结果，呵呵！个人觉得没撒啥用

书上原文：这个输出结果告诉我们，一些不同的服务器安装了不同的补丁等级版本，如果你想要攻击一个特定版本的 openssh 服务程序，那么这些使用 ssh_version 扫描得到的结果可能对你非常有价值。

3.3.4FTP 扫描

```
msf > use auxiliary/scanner/ftp/ftp_version
msf  auxiliary(ftp_version) > show options

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

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
   FTPPASS  mozilla@example.com  no        The password for the specified username
   FTPUSER  anonymous            no        The username to authenticate as
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT    21                   yes       The target port
   THREADS  1                    yes       The number of concurrent threads
```

```
msf  auxiliary(ftp_version) > set RHOSTS 192.168.137.0/24
RHOSTS => 192.168.137.0/24
msf  auxiliary(ftp_version) > set THREADS 50
THREADS => 50
msf  auxiliary(ftp_version) > run

[*] 192.168.137.50:21 FTP Banner: '220-Microsoft FTP Service\x0d\x0a220 http://hi.baidu.com/\xd
5\xf1\xcf\xa3/blog \x0d\x0a'
```

这里说明：扫描 ftp 他只能对匿名用户进行连接，这里表达的不好，我们看第一张截图，有个 ftppass 和 ftpuser，这就是它用来连接的用户名和密码。

3.3.5 简单网管协议（SNMP）扫描

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

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

   Name              Current Setting                                  Required  Descrip
   ----              ---------------                                  --------  ------
   BATCHSIZE         256                                              yes       The num
   BLANK_PASSWORDS   true                                             no        Try bla
   BRUTEFORCE_SPEED  5                                                yes       How fas
   CHOST                                                              no        The loc
   PASSWORD                                                           no        The pas
   PASS_FILE         /opt/framework/msf3/data/wordlists/snmp_default_pass.txt  no        File co
   RHOSTS                                                             yes       The tar
   RPORT             161                                              yes       The tar
   STOP_ON_SUCCESS   false                                            yes       Stop gu
host
   THREADS           1                                                yes       The num
```

```
msf  auxiliary(snmp_login) > set RHOSTS 10.2.27.254
RHOSTS => 10.2.27.254
msf  auxiliary(snmp_login) > run

[*] :161SNMP - [001/118] - 10.2.27.254:161 - SNMP - Trying public...
[+] SNMP: 10.2.27.254 community string: 'public' info: 'iSpirit5624GX'
[*] :161SNMP - [002/118] - 10.2.27.254:161 - SNMP - Trying private...
```

iSpirit5624GX 对这个百度或者谷歌一下，得知这是

天工iSpirit5624GX交换机 - 联想天工网络（深圳）有限公司
www.lenovonet.com/asp/productdetail.asp?productid=195 - 网页快照
联想天工iSpirit5624GX可利用双绞线端口为近距离的服务器或大流量数据用
入，又可以利用光纤的远距离传输特性构建千兆骨干网络，为远端的接入层

书上原文：SNMP 本是为系统管理员提供方便之举，但他却成了渗透测试者的金矿。 SNMP v1 和 v2 天生便有安全缺陷。（中间省略了一些废话）

v1 和 v2 具体有什么缺陷怎么利用，书上并没有讲，这里需要聪明的你去攻破了，呵呵！

3.4 编写自己的扫描器

由于本人编程水平有限，再加上 ruby 脚本语言并没有学过，也只有一页书，实在是难为我了。因此这里就先放着。

个人屁话：第三章讲的太那个了，太吊人胃口。扫描，扫完这里扫那里，扫个不停，也没见什么实质的东西是吧！写到后面我都有点不想了。要么扫到了，有没讲怎么去利用只是说有漏洞，是吧！也许这正是你现在心里所想。不要急，到第五章就有你激动的了。

第四章漏洞扫描

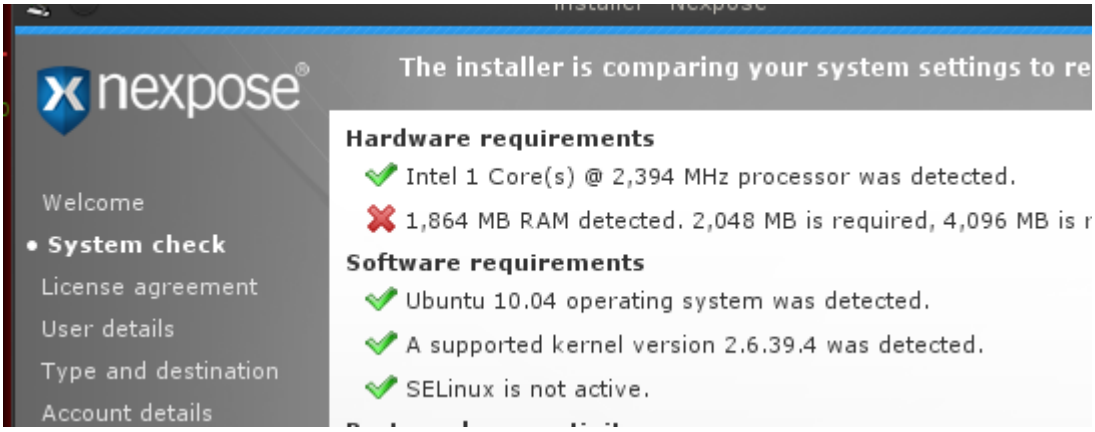
4.1 基本漏洞扫描

这里没什么好记录的

4.2 使用 NeXpose

这个东西要下载安装，在 BT5 里没有自带。当然这个好像也是免费的。
它有 window 版本和 linux 版本
这是下载地址，自己去看看吧！
http://www.rapid7.com/vulnerability-scanner.jsp

这里就有点悲剧了，看吧！



内存不足，安装不了呀！它要 4G 的内存，我电脑一共才 4G，一个虚拟机就要 4G，就叫我情何以堪嘛！这还怎么玩下去吗？？过了算了，只要你懂点英语这东西那这就可以用，有不明白的地方可以去百度或者谷歌，基本上是可以搞定的，这里就不多讲了。

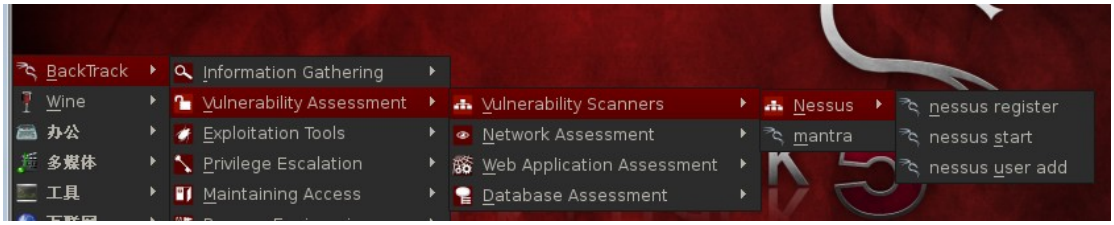
注明一点：安装完成后，你可能很郁闷不知道注明启动它，呵呵！它是网页工具和我们后面要介绍的工具差不多。安装完成后，你可以打开一个网页浏览器，输入如下网址：

https://<you ip address>:3780　　就进去了。

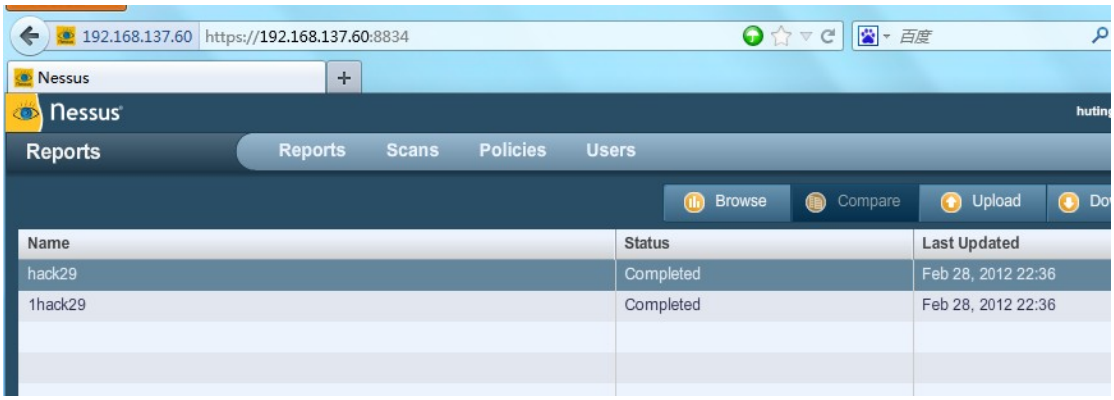
4.3 使用 Nessus 进行扫描

这个工具貌似 BT5 里自带，这个我们使用的是免费的家用版，但好像也要注册，但免费咯。它会以邮件的形似发注册码给你，第一次用的时候注册一下就 ok 了。

开始吧！首先要启动 http 服务即 apache start



第一次用要选择 register 注册，注完测后选择 user add 创建用户名和密码，在是启动 start。



这是我在本机上打开的，就几个简单的英文，这个网页工具也没什么好写的。学过点英语一看便知道了，如果你实在不知道可以去看看明教教主讲的视频。

4.35 将扫描结果导入 metasploit 框架中

先要扫描，下载扫描报告 Report，这个东西扫描好慢。

```
msf > db_status
[*] postgresql connected to msf3
msf >
msf >
msf >
msf > db_import /root/nessus_report_hunangy.com.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 58.20.53.163
[*] Successfully imported /root/nessus_report_hunangy.com.nessus
msf > hosts -c address,svcs,vulns

Hosts
=====

address         svcs  vulns
-------         ----  -----
10.1.0.254      1     0
10.2.27.254     1     0
58.20.53.163    1     25
192.168.137.10  1     0
192.168.137.50  1     0
```

msf > db_status

[*] postgresql connected to msf3

查看是否连接数据库，导入报告文件，查看目标的 ip 地址，探测到的服务数量以及 Nessus 在目标上发现的漏洞数量。

4.3.6 在 Metasploit 内部使用 Nessus 进行扫描

```
msf > load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[*] Successfully loaded plugin: nessus
msf >
```

执行 load nessus 命令载入 Nessus 插件，这里我觉得没必要这么做，所以接下这里来就不写了，其实效果和上面是一样的。

4.4 专用漏洞扫描器

4.4.1 验证 SMB 登陆

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

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank p
   BRUTEFORCE_SPEED  5                yes       How fast to
   PASS_FILE                          no        File contai
   PRESERVE_DOMAINS  true             no        Respect a u
   RECORD_GUEST      false            no        Record gues
   RHOSTS                             yes       The target
   RPORT             445              yes       Set the SME
```

这里是乱来了，也太假，这还要扫描么？？真想去问问这个作者怎么搞的。这里没有一点意义。

过

4.4.2 扫描开放的 VNC 空口令

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

Module options (auxiliary/scanner/vnc/vnc_none_auth):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf  auxiliary(vnc_none_auth) >
```

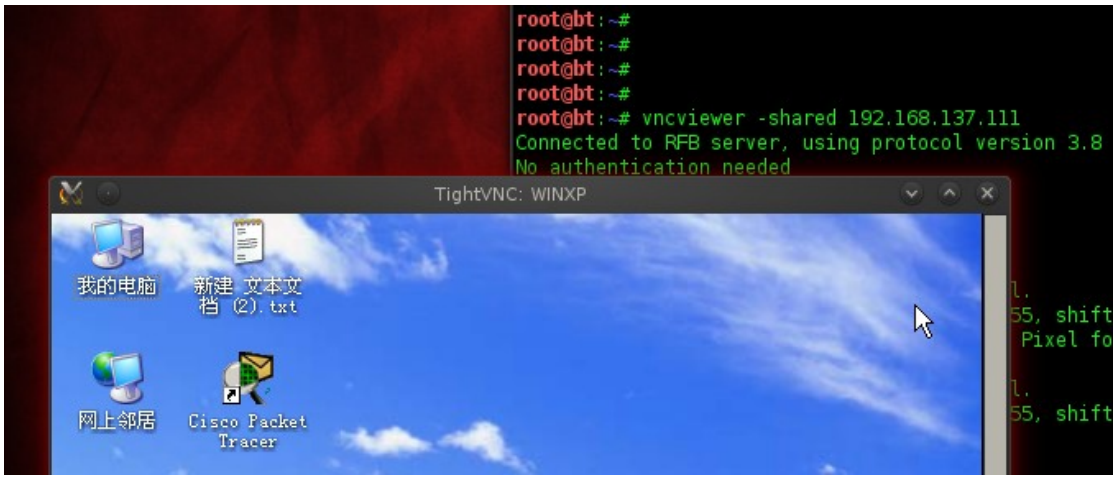
选择模块，以及查看参数。

```
msf  auxiliary(vnc_none_auth) > set RHOSTS 192.168.137.0/24
RHOSTS => 192.168.137.0/24
msf  auxiliary(vnc_none_auth) > set THREADS 50
THREADS => 50
msf  auxiliary(vnc_none_auth) > run
```

参数的设置，即运行。

```
msf  auxiliary(vnc_none_auth) > run

[*] Scanned 051 of 256 hosts (019% complete)
[*] Scanned 101 of 256 hosts (039% complete)
[*] 192.168.137.111:5900, VNC server protocol version : 3.8
[-] 192.168.137.111:5900, Auth negotiation failed: No supported authentication method found.
[*] Scanned 119 of 256 hosts (046% complete)
```

Ok 出来了，但他这个家伙还是感觉有点问题，明明是空口令，它却不成功，可能是这个 vnc 更新了吧！不过我们还是可以连接上的，呵呵！看看吧！

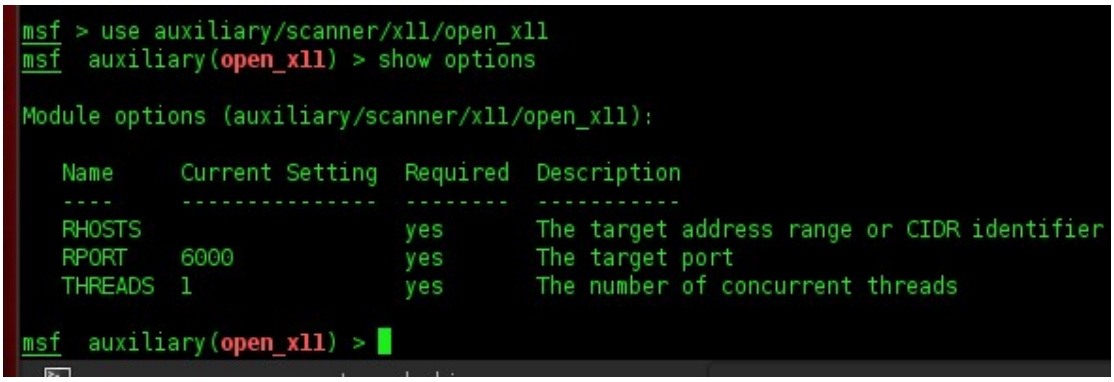


呵呵！是不是感觉很好啊！不过一切都没那么容易的。
不设密码的是极少数傻子才会干的，运气好可能你能够
碰到这样的傻子。

4.4.3 扫描开放的 X11 服务器

X11 这玩意听都木有听过，书上说:是古老的主机使用的，老旧的系统往往是网络上最脆弱的地方。

还是来看看吧！



这东西还是不好演示啊！这个 x11 服务器 ，我实在是没办法搭建，
百度上几乎找不到一点资料，谷歌还好点，找到了个像样点的，
大爷的，弄了两个小时了，还没找到软件包，不搞了。有兴趣的自己去玩玩
这里是我找到的有用的，唯一的一点资料：
http://www.freebsd.org/doc/zh_CN.GB2312/books/handbook/x-install.html

4.5 利用扫描结果进行自动化攻击

呵呵！这里前面我已经介绍了一点了，这里在详细的记录下。

书上原文：Metasploit 的 autopwn 工具能够自动选择目标，并利用已开放的端口或漏洞扫描结果，对目标进行自动化的渗透攻击。

使用 db_connect 创建一个新的数据库（注：这步可以省略，这是我的实践的到的经验）

使用 db_import 导入扫描报告。

这里重点是 db_autopwn 的开关参数

-e 对所有的目标发起攻击

-t 显示所有匹配的模块

-r 使用反弹 shell 的攻击载荷

-x 根据漏洞选择攻击模块

-p 根据开放端口选择攻击模块

第五章渗透攻击之旅

休息下，待续.....