Backtrack Linux Kullanımı

Bilgi Güvenliği AKADEMİSİ

Backtrack Linux Dağıtımı

- Backtrack, eski sürümleri Slackware üzerine kurulu SLAX Linux dağıtımını, yeni sürümleri (Backtrack 4 ile birlikte)Debian Linux dağıtımını temel almış güvenlik testleri amaçlı bir dağıtımdır.

- Eğitim boyunca en sık kullanacağımız sistem Backtrack Linux dağıtımı olacaktır.

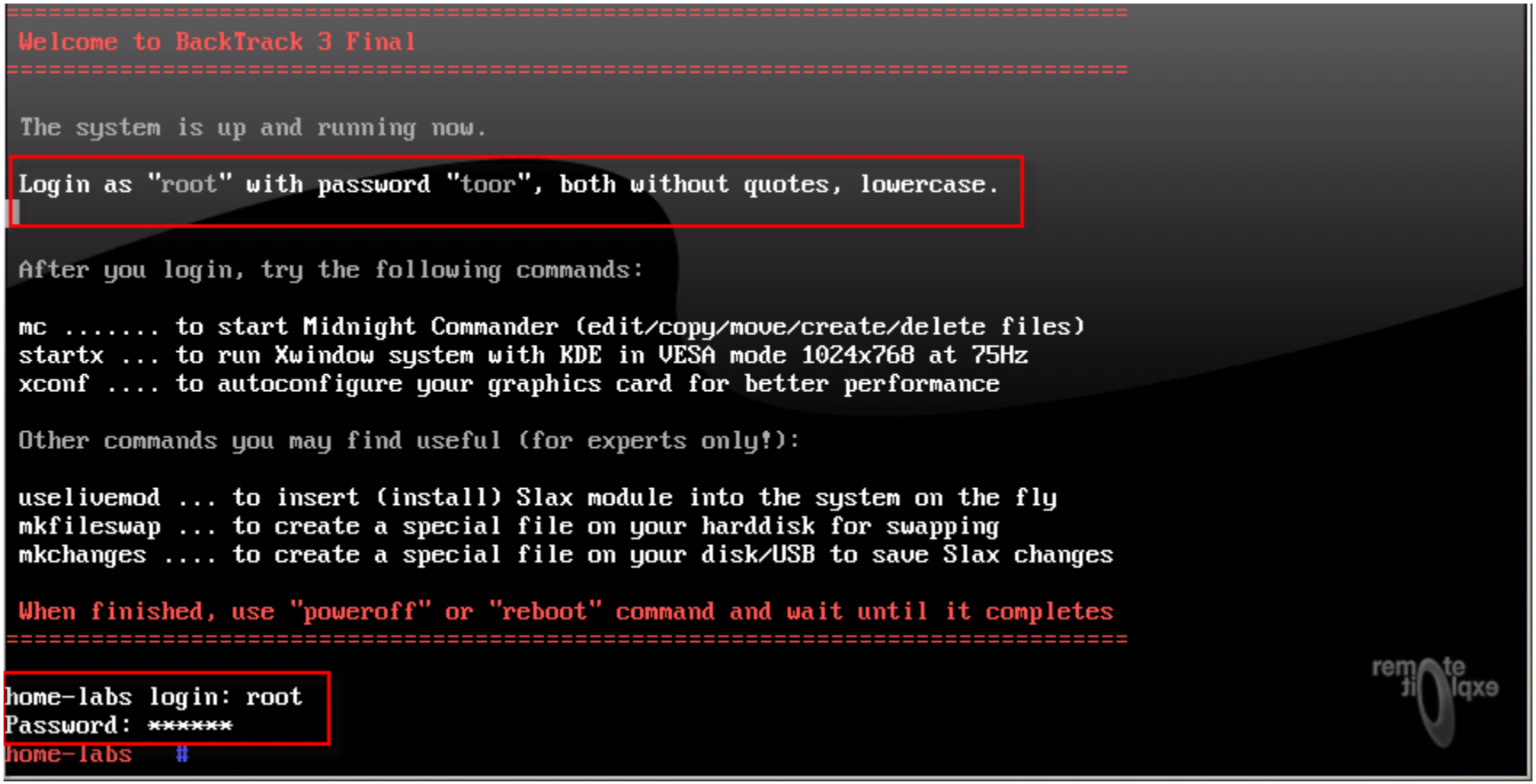
Backtrack Linux kullanımı

- Backtrack Linux iki farklı şekilde kullanılabilir;
  - Hazır CD den çalıştırma yoluyla
  - Diske kurulum yöntemi ya da Vmware aracılığıyla.
- CDden çalıştırma yönteminin performansı cd okuyucunun kalitesine ve hızına bağlı olarak değişebilir.
- Tavsiye edilen yöntem Backtrack'i Vmware ya da VirtualBox üzerinden çalıştırmaktır.

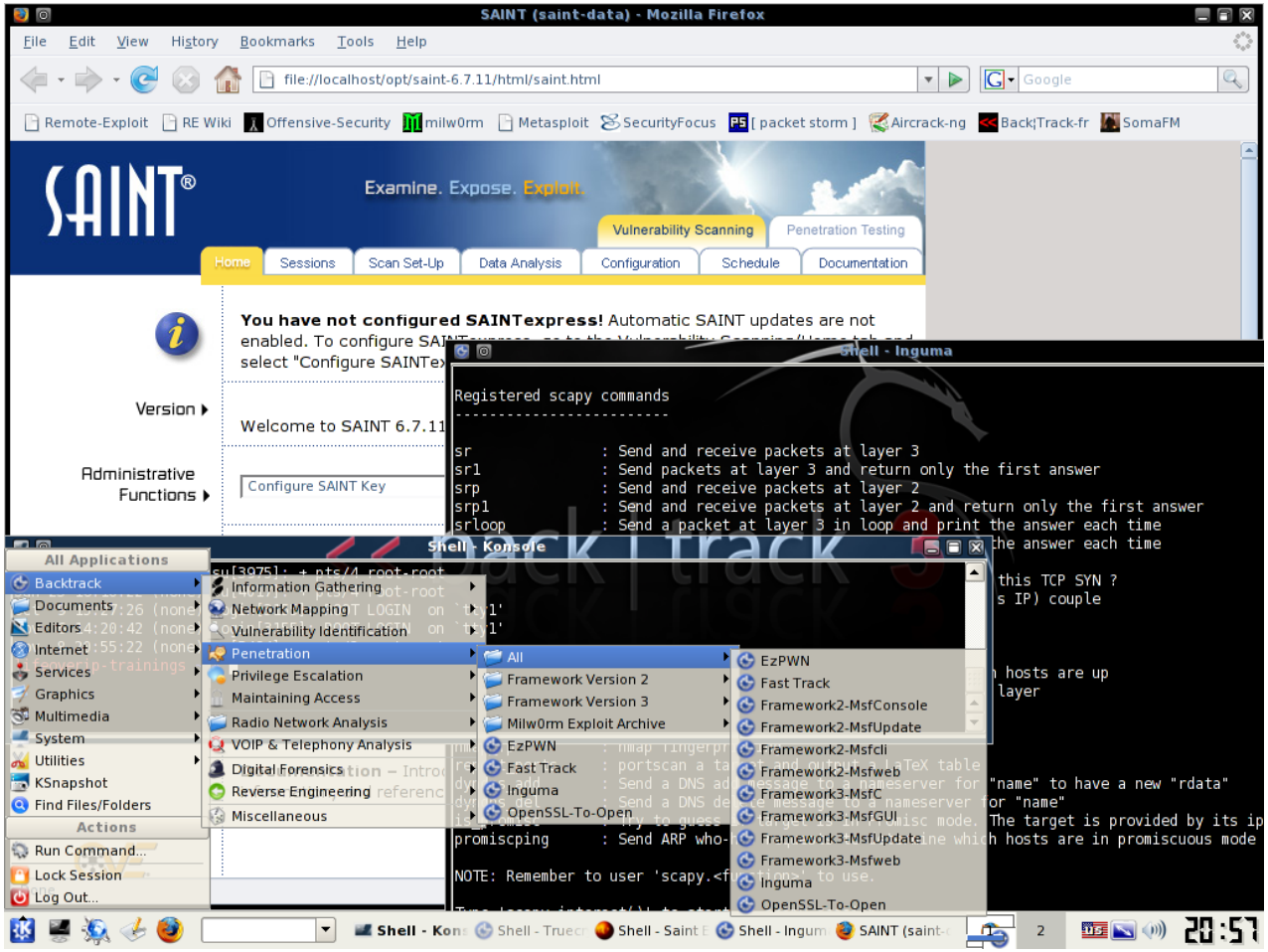
Backtrack Linux Kullanımı

- Linux üzerinde KDE ya da benzeri masaüstü kullandıysanız backtrack'i kullanırken zorluk cekmezsiniz ama Backtrack'in asıl gücü masaüstünde değil komut satırındadır
- Masaüstü kullanarak erişilebilecek programların çoğu aslında komut satırından çalışan program/scriptlerin düzenli menüler haline getirilmişidir.

Sisteme Giriş



Grafik Arabirim



Sistemi Tanıma

- Dağıtımın kök dizini incelenecek olursa diğer dağıtımlardan farklı olarak /pentest dizini göze çarpacaktır

```
lifeoverip ~ # cd /
lifeoverip / # ls -l
total 21
drwxr-xr-x  2 root root  3776 Mar  6  2007 bin/
drwxr-xr-x  2 root root    48 Aug 18  2007 boot/
drwxr-xr-x 21 root root 14720 Mar 15 09:05 dev/
drwxr-xr-x 49 root root  4520 Mar 15 07:05 etc/
drwxr-xr-x  3 root root    72 Mar  6  2007 home/
drwxr-xr-x  6 root root  3712 Mar  9  2007 lib/
drwxr-xr-x  8 root root   216 Feb 27 15:05 mnt/
drwxr-xr-x 15 root root   360 Mar 10  2007 opt/
drwxr-xr-x 23 root root   608 Nov 30 05:27 pentest/
dr-xr-xr-x 102 root root     0 Mar 15 02:05 proc/
drwxr-xr-x 34 root root  1760 Mar 15 09:21 root/
drwxr-xr-x  2 root bin   6496 Mar  6  2007 sbin/
```

/pentest dizini

- Bu dizin sistemde bulunan çoğu programın düzenli bir şekilde yer aldığı ana dizindir.

```
lifeoverip pentest # cd /pentest/

lifeoverip pentest # ls -l

total 1
drwxr-xr-x  3 root root   72 Nov 23  2006 anon/
drwxr-xr-x  5 root root  128 Mar  5  2007 bluetooth/
drwxr-xr-x 13 root root  456 Oct  7  2006 cisco/
drwxr-xr-x  5 root root  144 Feb 13  2007 database/
drwxr-xr-x 19 root root  512 Sep 17  2006 enumeration/
drwxr-xr-x  5 root root  168 Aug 18  2007 exploits/
drwxr-xr-x 12 root root  304 Mar  6  2007 fuzzers/
drwxr-xr-x  3 root root   80 Oct  2  2006 home-labs/
drwxr-xr-x  3 root root  232 Oct  7  2006 housekeeping/
drwxr-xr-x  2 root root   72 Mar  6  2007 misc/
drwxr-xr-x 12 1001 users 408 Oct  5  2006 password/
drwxr-xr-x  2 root root  136 Oct  7  2006 printer/
drwxr-xr-x  3 root root   72 Oct  2  2006 reversing/
drwxr-xr-x  7 1001 users 184 Mar  5  2007 scanners/
drwxr-xr-x  7 root root  184 Oct  9  2006 sniffers/
drwxr-xr-x  3 root root   72 Mar  6  2007 spoofing/
drwxr-xr-x  5 root root  144 Oct  7  2006 tunneling/
drwxr-xr-x  3 root root   72 Oct  8  2006 vpn/
drwxr-xr-x 11 root root  464 Nov 23  2006 web/
drwxr-xr-x  8 root root  208 Nov  4  2006 windows-binaries/
drwxr-xr-x 15 root root  480 Mar  6  2007 wireless/
```

Komut satırı araçlarının kullanımı

- Backtrack'i arabirimden kullanabileceğiniz gibi her programı kendi dizinine geçerek de kullanabilirsiniz.
- Mesela Wireless kategorisindeki aircrack-ng programını çalıştırmak için;
  - **# cd /pentest/wireless/aircrack-ng/**
  - **# ./aircrack-ng**

İsme Göre Araç Arama

- Herhangi bir programın nerede olduğu konusunda ön bilgi yoksa ve komut satırından doğrudan çalıştırılamıyorsa “find” ya da “locate” komutlarını kullanarak ilgili programın bulunduğu dizin öğrenilebilir

locate dnsenum

/pentest/enumeration/dnsenum

Backtrack'de bulunan bazı ek servisler ve kullanımı

- Backtrack bir güvenlik dağıtımı olmasına rağmen üzerinde klasik Linux dağıtımlarında bulunabilecek bazı servisleri içermektedir.
- Bunların amacı çeşitli güvenlik testlerinde ek bileşen olarak kullanılmaktır.
  - Mesela bir sisteme sızma denemesi gerçekleştirildi ve başarıldı, sızılan sistemden tftp ile veri alınması gerekiyor. Bu durumda Bakctrack üzerinde tftp servisi çalıştırılarak gerekli bilgiler sunucudan kolaylıkla transfer edilebilir.

Tftp Servisinin Başlatılması

- Tftp servisini başlatmak için aşağıdaki komut yeterli olacaktır.

lifeoverip # atftpd --daemon /tmp

- tftp servisi gelen verileri /tmp dizinine atacak(ya da bu dizinden alacak) şekilde başlatılmış oldu. Servisin durum kontrolü için lsof komutu kullanılabilir.
- **# lsof -i udp**
  - atftpd 12986 nobody 0u IPv4 215861 UDP *:tftp

SSH Servisisinin Başlatılması

- İlk olarak
  - #sshd-generate
- ardından
  - #/usr/sbin/sshd

komutları çalıştırılmalıdır. Bu işlemler grafik arabirimdeki menüler aracılığı ile de yapılabilir.

Network Ayarları

- İfconfig eth0 up
- Dhcpcd –nd eth0
- #ping www.google.com

Backtrack4 Sorun Giderme

- Backtrack4 Henüz Beta bir sistem ve çeşitli eksiklikleri var
- Öncelikle her zaman güncel sistem kullanabilmek için

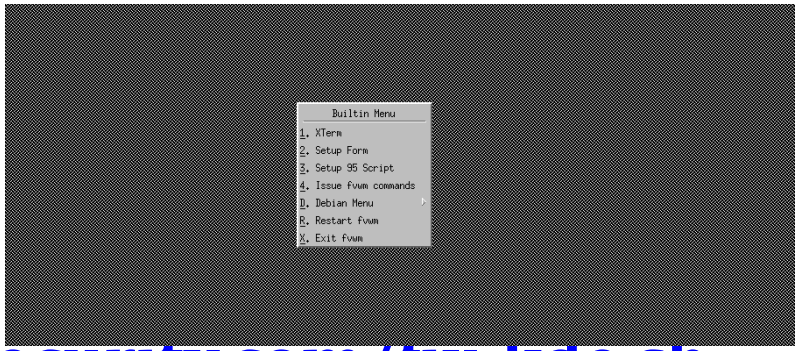
  #apt-get update

  #apt-get upgrade

  Komutlarıyla sistem güncel tutulmalı
- Çalışma ortamlarına bağımlı çeşitli problemler çıkabilir(Vmware, USB, LiveCD)

apt-get upgrade komutu sonrası KDE'nin açılmaması problemi

- apt-get upgrade komutu ile sistemi güncellemek isterseniz bu işlem sonrasında grafik arabirim bozulacaktır.



- Düzeltmek için
  - **wget www.offensive-security.com/fix-kde.sh**
  - **root@home-labs:~# bash fix-kde.sh**
  - **startx**

Klavye Ayarları Değiştirme

- Klavye ve dil seçimi için aşağıdaki komut çalıştırılmalı ve yönergeler izlenerek uygun klavye modeli ve dil seçeneği belirlenmeli.
- # dpkg-reconfigure console-setup

SSH Servisi Başlatma Sorunu

- /etc/init.d/ssh start

Could not load host key: /etc/ssh/ssh_host_dsa_key

Could not load host key: /etc/ssh/ssh_host_rsa_key

- **ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key**
- **ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key**

Ek program Kurma

- Bazı bilinen programlar eksiktir
- Bazı programların GUI üsümleri eksiktir.
- Debian/Ubuntu paket yönetim sistemi
- Apt-get install yazilim_ismi
- Apt-cache search yazilim_ismi

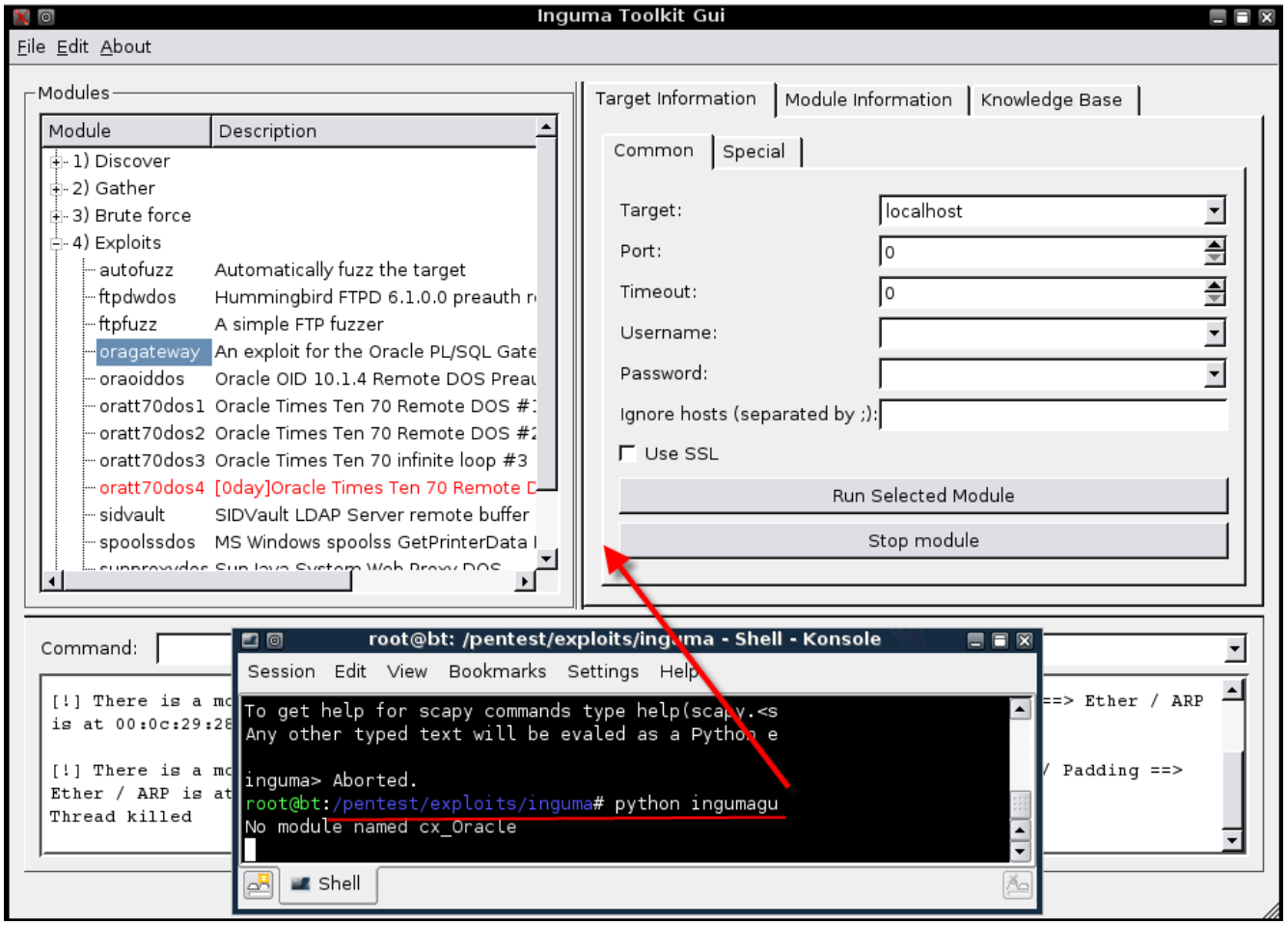
Ettercap GUI Kurulumu

- Backtrack4 ile birlikte gelen Ettercap sürümü GUI modu eksiktir
- Ettercap GUI Kurulumu
  - root@bt:~/progs# apt-get install ettercap-gtk

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  subversion libct4 freetds-dev
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
  ettercap ettercap-menu fasttrack
The following NEW packages will be installed:
  ettercap-gtk
0 upgraded, 1 newly installed, 3 to remove and 150 not
Need to get 233kB of archives.
After this operation, 3355kB disk space will be freed.
Do you want to continue [Y/n]? Y
```

Inguma GUI Kurulumu

apt-get install python-qt3



Yersinia GUI Kurulumu

Nessus Kurulumu

- Nessus lisansı dolayısıyla Linux dağıtımlarında yer almaz
- Nessus Kurulumu:
  - Nessus paketleri nessus.org'dan indirilir
  - Ön gereksinimler kurulur
  - Nessus Sunucu ve istemci paketleri sırayla kurulur

Kurulu Uygulamaları Güncelleme

- Fasttrack kullanarak...
- Apt-get update
- Apt-get upgrade
- Apt-get dist-upgrade

Sistem/Ağ Güvenliği Komutları

- Sisteme Kimler Bağlı/bağlanmış?
- Who, w, last komutları

```
netsec-egitim ~ # who
root     tty1         Jul 10 21:45
root     pts/4        Jul 11 14:27 (192.168.1.11)
root     pts/5        Jul 11 14:32 (192.168.1.11)
```

```
netsec-egitim ~ # who -l -i -H
who: Warning: -i will be removed in a future release;  use -u instead
NAME     LINE         TIME         IDLE          PID COMMENT
root     tty1         Jul 10 21:45 16:46         4173
LOGIN    tty2         Jul 10 21:43               4174 id=c2
LOGIN    tty3         Jul 10 21:43               4175 id=c3
LOGIN    tty4         Jul 10 21:43               4176 id=c4
LOGIN    tty5         Jul 10 21:43               4177 id=c5
LOGIN    tty6         Jul 10 21:43               4178 id=c6
```

```
netsec-egitim ~ # last

huzeyfe      ttyp0    88.233.47.18     Tue Jul 24 23:27   still logged in
huzeyfe      ttyp0    212.65.136.101   Tue Jul 24 16:23 - 16:53  (00:30)
huzeyfe      ttyp0    212.65.136.101   Tue Jul 24 09:40 - 15:18  (05:38)
Lifeoverip   ttyp2    88.235.78.143    Mon Jul 23 20:57 - 23:11  (02:13)
huzeyfe      ttyp1    88.235.78.143    Mon Jul 23 20:32 - 22:43  (02:11)
adnan        ttyp0    88.235.47.135    Mon Jul 23 19:41 - 21:50  (02:09)
huzeyfe      ttyp0    88.233.217.135   Sun Jul 22 15:37 - 16:02  (00:25)
```