



Building the Perfect Backtrack 4 USB Thumb Drive

Why?

What
makes it
perfect?





Persistence

Nessus

Encrypted

Current

What you
will need

Two USB Thumb drives
One at least 2GB
One at least 4GB



OR

One DVD

One Thumb Drive at least 4GB



A copy of the Backtrack 4 Pre-Release ISO

http://www.remote-exploit.org/backtrack_download.html

BackTrack Downloads

We provide BackTrack to the community using various mirrors all over the world. We would like to thank the different companies / persons for the help in redistributing.

BackTrack 4 Pre Release

Last Update: 19.06.2009

NOTE: Due to massive downloads and missing bandwidth, some servers might be unreachable and you need to hit either reload or click again on the download link.

Description: DVD Image
Name:: bt4-pre-final.iso
Size: 1390 MB
MD5: b0485da6194d75b30cda282ceb629654
Download: [Click here](#)

Disklabel: bt4-label.png

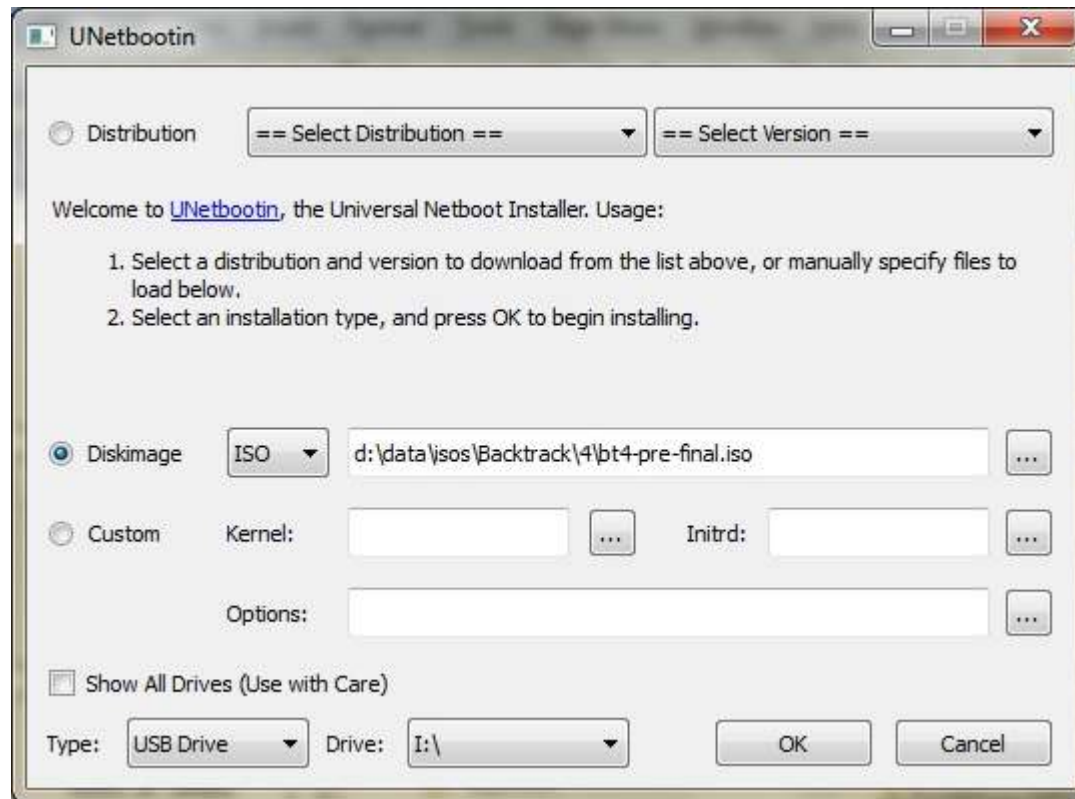
What are
We Going
to Do?

Partition the Thumb Drive
Install Backtrack
Setup Persistence
Install Nessus
Configure Encryption
Tweak a Few Things
Profit

Let's Get
Started

Create A Bootable Backtrack 4 Device

<http://unetbootin.sourceforge.net/>



OR

Burn a DVD

Partition the Thumb Drive

<< back | track 龍

```
root@bt:~# dmesg | egrep hd.\isd.
hdc: VBOX CD-ROM, ATAPI CD/DVD-ROM drive
hdc: host max PIO4 wanted PIO255(auto-tune) selected PIO4
hdc: UDMA/33 mode selected
ide-cd: hdc: ATAPI 32X DVD-ROM drive, 128kB Cache
Driver 'sd' needs updating - please use bus_type methods
sd 2:0:0:0: [sda] 8388608 512-byte hardware sectors: (4.29 GB/4.00 GiB)
sd 2:0:0:0: [sda] Write Protect is off
sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
sd 2:0:0:0: [sda] 8388608 512-byte hardware sectors: (4.29 GB/4.00 GiB)
sd 2:0:0:0: [sda] Write Protect is off
sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
sda: unknown partition table
sd 2:0:0:0: [sda] Attached SCSI disk
sd 2:0:0:0: Attached scsi generic sg0 type 0
root@bt:~# _
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

```
root@bt: # fdisk /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xd48bbdb4.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-522, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-522, default 522): +1500M
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 1

First cylinder (1-522, default 1):

Using default value 1

Last cylinder, +cylinders or +size{K,M,G} (1-522, default 522): +1500M

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 2

First cylinder (193-522, default 193):

Using default value 193

Last cylinder, +cylinders or +size{K,M,G} (193-522, default 522):

Using default value 522

Command (m for help): _



"The quieter you become, the more you are able to hear."

<< back | track 龍

```
Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-522, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-522, default 522): +1500M

Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (193-522, default 193):
Using default value 193
Last cylinder, +cylinders or +size{K,M,G} (193-522, default 522):
Using default value 522

Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): _
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

0 Empty	1e Hidden W95 FAT1	80 Old Minix	bf Solaris
1 FAT12	24 NEC DOS	81 Minix / old Lin	c1 DRDOS/sec (FAT-
2 XENIX root	39 Plan 9	82 Linux swap / So	c4 DRDOS/sec (FAT-
3 XENIX usr	3c PartitionMagic	83 Linux	c6 DRDOS/sec (FAT-
4 FAT16 <32M	40 Venix 80286	84 OS/2 hidden C:	c7 Syrinx
5 Extended	41 PPC PReP Boot	85 Linux extended	da Non-FS data
6 FAT16	42 SFS	86 NTFS volume set	db CP/M / CTOS / .
7 HPFS/NTFS	4d QNX4.x	87 NTFS volume set	de Dell Utility
8 AIX	4e QNX4.x 2nd part	88 Linux plaintext	df BootIt
9 AIX bootable	4f QNX4.x 3rd part	8e Linux LVM	e1 DOS access
a OS/2 Boot Manag	50 OnTrack DM	93 Amoeba	e3 DOS R/O
b W95 FAT32	51 OnTrack DM6 Aux	94 Amoeba BBT	e4 SpeedStor
c W95 FAT32 (LBA)	52 CP/M	9f BSD/OS	eb BeOS fs
e W95 FAT16 (LBA)	53 OnTrack DM6 Aux	a0 IBM Thinkpad hi	ee GPT
f W95 Ext'd (LBA)	54 OnTrackDM6	a5 FreeBSD	ef EFI (FAT-12/16/
10 OPUS	55 EZ-Drive	a6 OpenBSD	f0 Linux/PA-RISC b
11 Hidden FAT12	56 Golden Bow	a7 NeXTSTEP	f1 SpeedStor
12 Compaq diagnost	5c Priam Edisk	a8 Darwin UFS	f4 SpeedStor
14 Hidden FAT16 <3	61 SpeedStor	a9 NetBSD	f2 DOS secondary
16 Hidden FAT16	63 GNU HURD or Sys	ab Darwin boot	fb VMware VMFS
17 Hidden HPFS/NTF	64 Novell Netware	b7 BSDI fs	fc VMware VMKCORE
18 AST SmartSleep	65 Novell Netware	b8 BSDI swap	fd Linux raid auto
1b Hidden W95 FAT3	70 DiskSecure Mult	bb Boot Wizard hid	fe LANstep
1c Hidden W95 FAT3	75 PC/IX	be Solaris boot	ff BBT

Hex code (type L to list codes): _



"The quieter you become, the more you are able to hear."

<< back | track 龍

5	Extended	41	PPC PReP Boot	85	Linux extended	da	Non-FS data
6	FAT16	42	SFS	86	NTFS volume set	db	CP/M / CTOS / .
7	HPFS/NTFS	4d	QNX4.x	87	NTFS volume set	de	Dell Utility
8	AIX	4e	QNX4.x 2nd part	88	Linux plaintext	df	BootIt
9	AIX bootable	4f	QNX4.x 3rd part	8e	Linux LVM	e1	DOS access
a	OS/2 Boot Manag	50	OnTrack DM	93	Amoeba	e3	DOS R/O
b	W95 FAT32	51	OnTrack DM6 Aux	94	Amoeba BBT	e4	SpeedStor
c	W95 FAT32 (LBA)	52	CP/M	9f	BSD/OS	eb	BeOS fs
e	W95 FAT16 (LBA)	53	OnTrack DM6 Aux	a0	IBM Thinkpad hi	ee	GPT
f	W95 Ext'd (LBA)	54	OnTrackDM6	a5	FreeBSD	ef	EFI (FAT-12/16/
10	OPUS	55	EZ-Drive	a6	OpenBSD	f0	Linux/PA-RISC b
11	Hidden FAT12	56	Golden Bow	a7	NeXTSTEP	f1	SpeedStor
12	Compaq diagnost	5c	Priam Edisk	a8	Darwin UFS	f4	SpeedStor
14	Hidden FAT16 <3	61	SpeedStor	a9	NetBSD	f2	DOS secondary
16	Hidden FAT16	63	GNU HURD or Sys	ab	Darwin boot	fb	VMware VMFS
17	Hidden HPFS/NTF	64	Novell Netware	b7	BSDI fs	fc	VMware VMKCORE
18	AST SmartSleep	65	Novell Netware	b8	BSDI swap	fd	Linux raid auto
1b	Hidden W95 FAT3	70	DiskSecure Mult	bb	Boot Wizard hid	fe	LANstep
1c	Hidden W95 FAT3	75	PC/IX	be	Solaris boot	ff	BBT

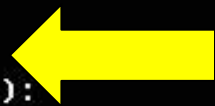
Hex code (type L to list codes): b

Changed system type of partition 1 to b (W95 FAT32)

Command (m for help): t

Partition number (1-4): 2

Hex code (type L to list codes):



"The quieter you become, the more you are able to hear."

<< back | track 龍

0 Empty	1e Hidden W95 FAT1	80 Old Minix	bf Solaris
1 FAT12	24 NEC DOS	81 Minix / old Lin	c1 DRDOS/sec (FAT-
2 XENIX root	39 Plan 9	82 Linux swap / So	c4 DRDOS/sec (FAT-
3 XENIX usr	3c PartitionMagic	83 Linux	c7 DOS/sec (FAT-
4 FAT16 <32M	40 Venix 80286	84 OS/2 hidden C:	da Syrinx
5 Extended	41 PPC PReP Boot	85 Linux extended	db Non-FS data
6 FAT16	42 SFS	86 NTFS volume set	de CP/M / CTOS / .
7 HPFS/NTFS	4d QNX4.x	87 NTFS volume set	df Dell Utility
8 AIX	4e QNX4.x 2nd part	88 Linux plaintext	e1 BootIt
9 AIX bootable	4f QNX4.x 3rd part	8e Linux LVM	e3 DOS access
a OS/2 Boot Manag	50 OnTrack DM	93 Amoeba	e4 DOS R/O
b W95 FAT32	51 OnTrack DM6 Aux	94 Amoeba BBT	eb SpeedStor
c W95 FAT32 (LBA)	52 CP/M	9f BSD/OS	ee BeOS fs
e W95 FAT16 (LBA)	53 OnTrack DM6 Aux	a0 IBM Thinkpad hi	ef GPT
f W95 Ext'd (LBA)	54 OnTrackDM6	a5 FreeBSD	ef EFI (FAT-12/16/
10 OPUS	55 EZ-Drive	a6 OpenBSD	f0 Linux/PA-RISC b
11 Hidden FAT12	56 Golden Bow	a7 NeXTSTEP	f1 SpeedStor
12 Compaq diagnost	5c Priam Edisk	a8 Darwin UFS	f4 SpeedStor
14 Hidden FAT16 <3	61 SpeedStor	a9 NetBSD	f2 DOS secondary
16 Hidden FAT16	63 GNU HURD or Sys	ab Darwin boot	fb VMware VMFS
17 Hidden HPFS/NTF	64 Novell Netware	b7 BSDI fs	fc VMware VMKCORE
18 AST SmartSleep	65 Novell Netware	b8 BSDI swap	fd Linux raid auto
1b Hidden W95 FAT3	70 DiskSecure Mult	bb Boot Wizard hid	fe LANstep
1c Hidden W95 FAT3	75 PC/IX	be Solaris boot	ff BBT

Hex code (type L to list codes):



"The quieter you become, the more you are able to hear."

<< back | track 龍

f	W95 Ext'd (LBA)	54	OnTrackDM6	a5	FreeBSD	ef	EFI (FAT-12/16/
10	OPUS	55	EZ-Drive	a6	OpenBSD	f0	Linux/PA-RISC b
11	Hidden FAT12	56	Golden Bow	a7	NeXTSTEP	f1	SpeedStor
12	Compaq diagnost	5c	Priam Edisk	a8	Darwin UFS	f4	SpeedStor
14	Hidden FAT16 <3	61	SpeedStor	a9	NetBSD	f2	DOS secondary
16	Hidden FAT16	63	GNU HURD or Sys	ab	Darwin boot	fb	VMware VMFS
17	Hidden HPFS/NTF	64	Novell Netware	b7	BSDI fs	fc	VMware VMKCORE
18	AST SmartSleep	65	Novell Netware	b8	BSDI swap	fd	Linux raid auto
1b	Hidden W95 FAT3	70	DiskSecure Mult	bb	Boot Wizard hid	fe	LANstep
1c	Hidden W95 FAT3	75	PC/IX	be	Solaris boot	ff	BBT

Hex code (type L to list codes): 83

Command (m for help): a
Partition number (1-4): 1

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: If you have created or modified any DOS 6.x
partitions, please see the fdisk manual page for additional
information.

Syncing disks.

root@bt:~# clear



"The quieter you become, the more you are able to hear."

<< back | track 龍


```
root@bt: # mkfs.vfat /dev/sda1  
mkfs.vfat 2.11 (12 Mar 2005)  
root@bt: # _
```



remote
jilqx9

"The quieter you become, the more you are able to hear."

<< back | track 龍



```
root@bt:~# mkfs.ext3 -b 4096 -L casper-rw /dev/sda2
mke2fs 1.41.3 (12-Oct-2008)
Filesystem label=casper-rw
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
165984 inodes, 662681 blocks
33134 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=679477248
21 block groups
32768 blocks per group, 32768 fragments per group
7904 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 28 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
root@bt:~# _
```



"The quieter you become, the more you are able to hear."

Install Backtrack

<< back | track 龍

```
root@bt:~# mkdir /mnt/sda1
root@bt:~# mount /dev/sda1 /mnt/sda1
root@bt:~# cd /mnt/sda1
root@bt:/mnt/sda1# rsync -r /media/cdrom0/* . _
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

```
root@bt:/mnt/sda1/boot/grub# cd /mnt/sda1
root@bt:/mnt/sda1# grub-install --no-floppy --root-directory=/mnt/sda1 /dev/sda
Probing devices to guess BIOS drives. This may take a long time.
Due to a bug in xfs_freeze, the following command might produce a segmentation
fault when /mnt/sda1/boot/grub is not in an XFS filesystem. This error is harmless
and
can be ignored.
xfs_freeze: specified file ["/mnt/sda1/boot/grub"] is not on an XFS filesystem
Installing GRUB to /dev/sda as (hd0)...
Installation finished. No error reported.
This is the contents of the device map /mnt/sda1/boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script 'grub-install'.

(hd0)    /dev/sda
root@bt:/mnt/sda1#
```



"The quieter you become, the more you are able to hear."

Setup Persistence

<< back | track 龍

```
root@bt:/mnt/sda1# cd boot/grub
root@bt:/mnt/sda1/boot/grub# vi menu.lst_
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

```
# By default boot the first entry.  
default 4
```

```
# Boot automatically after 30 secs.  
timeout 30
```

```
splashimage=/boot/grub/bt4.xpm.gz
```

```
title          Start BackTrack FrameBuffer (1024x768)  
kernel         /boot/vmlinuz BOOT=casper boot=casper nopersistent rw quiet v  
ga=0x317  
initrd         /boot/initrd.gz
```

```
title          Start BackTrack FrameBuffer (800x600)  
kernel         /boot/vmlinuz BOOT=casper boot=casper nopersistent rw quiet v  
ga=0x314  
initrd         /boot/initrd800.gz
```

```
title          Start BackTrack Forensics (no swap)  
kernel         /boot/vmlinuz BOOT=casper boot=casper nopersistent rw vga=0x3  
17  
initrd         /boot/initrdrfr.gz
```

```
"menu.lst" 43 lines, 1578 characters
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

```
title          Start BackTrack FrameBuffer (1024x768)
kernel        /boot/vmlinuz BOOT=casper boot=casper nopersistent rw quiet v
ga=0x317
initrd        /boot/initrd.gz

title          Start BackTrack FrameBuffer (800x600)
kernel        /boot/vmlinuz BOOT=casper boot=casper nopersistent rw quiet v
ga=0x314
initrd        /boot/initrd800.gz

title          Start BackTrack Forensics (no swap)
kernel        /boot/vmlinuz BOOT=casper 1 → nopersistent rw vga=0x3
17
initrd        /boot/initrdfs.gz

title          Start BackTrack in Safe Graphical Mode
kernel        /boot/vmlinuz BOOT=casper boot=casper xforcevesa rw quiet
initrd        /boot/initrd.gz

title          Start Persistent Live CD
kernel        /boot/vmlinuz BOOT=casper boot=casper persistent rw quiet vga
0x314 ←
initrd        /boot/initrd.gz
"menu.lst" 43 lines, 1586 characters written
root@bt:/mnt/sda1/boot/grub# _
```



"The quieter you become, the more you are able to hear."

<< back | track 龍

root@bt:/mnt/sda1# reboot

Broadcast message from root@bt
(/dev/tty1) at 7:19 ...

The system is going down for reboot NOW!

root@bt:/mnt/sda1# _



"The quieter you become, the more you are able to hear."

Start BackTrack FrameBuffer (1024x768)
Start BackTrack FrameBuffer (800x600)
Start BackTrack Forensics (no swap)
Start BackTrack in Safe Graphical Mode
Start Persistent Live CD
Start BackTrack in Text Mode
Start BackTrack Graphical Mode from RAM
Memory Test
Boot the First Hard Disk




Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 19 seconds.

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# touch test
root@bt:~# ls
install.sh  test
root@bt:~# reboot
```



back | track4

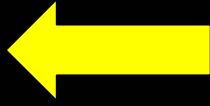
Shell



install.sh



test



<< back | track4



1 2

07:26

Install Nessus

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# /etc/init.d/networking start
Configuring network interfaces...Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/08:00:27:75:17:79
Sending on   LPF/eth0/08:00:27:75:17:79
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.1.105 from 192.168.1.1
DHCPREQUEST of 192.168.1.105 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.1.105 from 192.168.1.1
bound to 192.168.1.105 -- renewal in 43051 seconds.
if-up.d/mountnfs[eth0]: waiting for interface eth1 before doing NFS mounts
if-up.d/mountnfs[eth0]: waiting for interface eth2 before doing NFS mounts
if-up.d/mountnfs[eth0]: waiting for interface ath0 before doing NFS mounts
if-up.d/mountnfs[eth0]: waiting for interface wlan0 before doing NFS mounts
█
```

Shell

Tenable Network Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

← → ▾ ↺ ⓧ 🏠

http://www.nessus.org/download/

▾ Google

Remote-Exploit Offensive Security RE Forums milw0rm Metasploit Aircrack-ng BT-FR BT-IT >>

Download
Download Nessus now!

Documentation
Documentation about Nessus

ProfessionalFeed
Scan at your workplace and improve your policy compliance scanning abilities

Plugins
See all the security checks performed by Nessus

Enterprise Products
Our line of enterprise products

Features
Nessus main features

Select a product to download: ▾

Download

Select a product to download:

Nessus 4.0.1 for Microsoft Windows

Nessus 4.0.1 for Linux

Nessus 4.0.1 for Mac OS X 10.4 and 10.5

Nessus 4.0.1 for FreeBSD

NessusClient 4.0.1 (the Linux graphical interface for nessusd)

Nessus 3.2.1

Nessus 2.2.11 source code

ntOS 4 & 5, SuSE 9.3 & 10, Debian 5 (i386, amd64), Ubuntu

a, Iran, North Korea, Sudan, and Syria

Support Portal | Blog | RSS feeds | Contact us | Legal | Privacy

Done

root@bt: ~ - Sh Tenable Netw

1 2 00:55

Tenable Network Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nessus.org/download/nessus_download.p Google

Remote-Exploit Offensive Security RE Forums milw0rm Metasploit Aircrack-ng BT-FR BT-IT

Fedora 10 (64 bits)	Nessus-4.0.1-fc10.x86_64.rpm	3243 KB
SuSE 10	Nessus-4.0.1-suse10.0.i586.rpm	2453 KB
Fedora 10 (32 bits)	Nessus-4.0.1-fc10.i386.rpm	2895 KB
Fedora 11 (64 bits)	Nessus-4.0.1-fc11.x86_64.rpm	3275 KB
Generic Linux binary (intel/64 bits)	Nessus-4.0.1-linux-generic64.tar.gz	8815 KB
Fedora 11 (32 bits)	Nessus-4.0.1-fc11.i586.rpm	2935 KB
Generic Linux binary (intel/32 bits)	Nessus-4.0.1-linux-generic32.tar.gz	8005 KB
Debian 5.0 (64 bits)	Nessus-4.0.1-debian5_amd64.deb	3251 KB
Red Hat ES 5 / CentOS 5	Nessus-4.0.1-es5.i386.rpm	2894 KB
Ubuntu 8.04 (64 bits)	Nessus-4.0.1-ubuntu804_amd64.deb	3221 KB
Debian 5.0 (32 bits)	Nessus-4.0.1-debian5_i386.deb	2899 KB
Red Hat ES 5 (64 bits) / CentOS 5	Nessus-4.0.1-es5.x86_64.rpm	3204 KB
Red Hat ES 4 / CentOS 4	Nessus-4.0.1-es4.i386.rpm	2842 KB
Ubuntu 8.10 and 9.04 (64 bits)	Nessus-4.0.1-ubuntu810_amd64.deb	3261 KB
Ubuntu 8.04 (32 bits)	Nessus-4.0.1-ubuntu804_i386.deb	2916 KB
Ubuntu 8.10 and 9.04 (32 bits)	Nessus-4.0.1-ubuntu810_i386.deb	2625 KB
SuSE 9.3	Nessus-4.0.1-suse9.3.i586.rpm	

• [GPG Signed MD5s of these packages](#)

Done

root@bt: ~ - Sh Tenable Netw 1 2 00:55

Tenable Network Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nessus.org/download/

Remote-Exploit Offensive Security RE Forums milw0rm Metasploit Aircrack-ng BT-FR BT-IT

Download
Download Nessus now!

Documentation
Documentation about Nessus

ProfessionalFeed
Scan at your workplace and improve your policy compliance scanning abilities

Plugins
See all the security checks performed by Nessus

Enterprise Products
Our line of enterprise products

Features
Nessus main features

Select a product to download: [v] Download

- Select a product to download:
- Nessus 4.0.1 for Microsoft Windows
- Nessus 4.0.1 for Linux
- Nessus 4.0.1 for Mac OS X 10.4 and 10.5
- Nessus 4.0.1 for FreeBSD
-
- NessusClient 4.0.1 (the Linux graphical interface for nessusd)**
-
- Nessus 3.2.1
-
- Nessus 2.2.11 source code

Download

ntOS 4 & 5, SuSE 9.3 & 10, Debian 5 (i386, amd64), Ubuntu

a, Iran, North Korea, Sudan, and Syria

Tenable Netw [US] [FR] 1 2 00:56

Tenable Network Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nessus.org/download/index.php

Remote-Exploit Offensive Security RE Forums milw0rm Metasploit Aircrack-ng BT-FR BT-IT

Download
Download Nessus now!

Documentation
Documentation about Nessus

ProfessionalFeed
Scan at your workplace and improve your policy compliance scanning abilities

Plugins
See all the security checks performed by Nessus

Enterprise Products
Our line of enterprise products

Features
Nessus main features

Download :

- [NessusClient-4.0.1-fc10.x86_64.rpm](#) (Fedora 10 (64 bits)) (502 KB)
- [NessusClient-4.0.1-ubuntu810_amd64.deb](#) (Ubuntu 8.10 and 9.04 (64 bits)) (500 KB)
- [NessusClient-4.0.1-fc11.x86_64.rpm](#) (Fedora 11 (64 bits)) (504 KB)
- [NessusClient-4.0.1-ubuntu804_amd64.deb](#) (Ubuntu 8.04 (64 bits)) (486 KB)
- [NessusClient-4.0.1-debian5_amd64.deb](#) (Debian 5.0 (64 bits)) (500 KB)
- [NessusClient-4.0.1-ubuntu810_i386.deb](#) (Ubuntu 8.10 and 9.04 (32 bits)) (488 KB)
- [NessusClient-4.0.1-ubuntu804_i386.deb](#) (Ubuntu 8.04 (32 bits)) (468 KB)
- [NessusClient-4.0.1-fc10.i386.rpm](#) (Fedora 10 (32 bits)) (494 KB)
- [NessusClient-4.0.1-es5.i386.rpm](#) (Red Hat ES 5 / CentOS 5) (4913 KB)
- [NessusClient-4.0.1-debian5_i386.deb](#) (Debian 5.0 (32 bits)) (489 KB)
- [NessusClient-4.0.1-fc11.i586.rpm](#) (Fedora 11 (32 bits)) (498 KB)
- [NessusClient-4.0.1-es4.i386.rpm](#) (Red Hat ES 4 / CentOS 4) (7893 KB)
- [NessusClient-4.0.1-es5.x86_64.rpm](#) (Red Hat ES 5 (64 bits) / CentOS 5) (4856 KB)
- [GPG Signed MD5s of these packages](#)

Done

root@bt: ~ - Sh Tenable Netw 1 2 00:56

Tenable Network Security - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.nessus.org/plugins/

Remote-Exploit Offensive Security RE Forums milw0rm Metasploit Aircrack-ng BT-FR BT-IT

Download
Plugins
Newest Plugins
Obtain an activation code
View all plugins
Search
Documentation
Register
Buy Now
ProfessionalFeed Support
Bugs
All the Tenable Products

What is a Plugin?

Every audit in Nessus is coded as a **plugin**: a simple program which checks for a given flaw. There are 1046 different plugins used by Nessus, covering local and remote flaws.

Staying Up-To-Date

New vulnerabilities are discovered and published every day. As a result, staying up-to-date is a must if you want to perform a security scan. Every week, several dozens of plugins are added in the **nessus plugin feed**. To make sure your plugins are up-to-date, make sure that your scanner has been registered properly on Nessus.org. Once your scanner is registered, it will fetch the newest plugins automatically every 24 hours, or you can use the command `nessus-update-plugins` to force an update of your plugins.

- How to configure Nessus to receive all the newest plugins every day
- Information about the Nessus plugin feed
- View the newest Nessus plugins
- View all the Nessus plugins
- Search the Nessus plugins
- Nessus 3 & 4 and Plugins Licensing FAQ

About us | Whitepapers | Training | Discussion Forums | Support Portal | Blog | RSS feeds | Contact us | Legal | Privacy

© Copyright 2002 - 2009 Tenable Network Security(R). All Rights Reserved.

This is the web site for the Nessus Vulnerability Scanner from Tenable Network Security. If you are looking for the probabilistic

http://www.nessus.org/plugins/index.php?view=register-info

root@bt: ~ - Sh Tenable Netw 1 2 00:56

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# firefox
root@bt:~# ls
install.sh                                NessusClient-4.0.1-ubuntu810_i386.deb
Nessus-4.0.1-ubuntu810_i386.deb test
root@bt:~# dpkg --install Nessus-4.0.1-ubuntu810_i386.deb
Selecting previously deselected package nessus.
(Reading database ... 183077 files and directories currently installed.)
Unpacking nessus (from Nessus-4.0.1-ubuntu810_i386.deb) ...
Setting up nessus (4.0.1) ...
nessusd (Nessus) 4.0.1. for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

- Please run /opt/nessus/sbin/nessus-adduser to add a user
- Register your Nessus scanner at http://www.nessus.org/register/ to obtain
  all the newest plugins
- You can start nessusd by typing /etc/init.d/nessusd start

root@bt:~#
```



root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# dpkg --install NessusClient-4.0.1-ubuntu810_i386.deb
Selecting previously deselected package nessusclient.
(Reading database ... 183134 files and directories currently installed.)
Unpacking nessusclient (from NessusClient-4.0.1-ubuntu810_i386.deb) ...
Setting up nessusclient (4.0.1) ...
root@bt:~#
```

back | track 4

Shell

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# /opt/nessus/sbin/nessus-mkcert
-----
                Creation of the Nessus SSL Certificate
-----

This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
Nessus daemon will be able to retrieve this information.

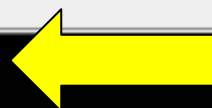
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [FR]: US
Your state or province name [none]:
Your location (e.g. town) [Paris]: USB
Your organization [Nessus Users United]:
```

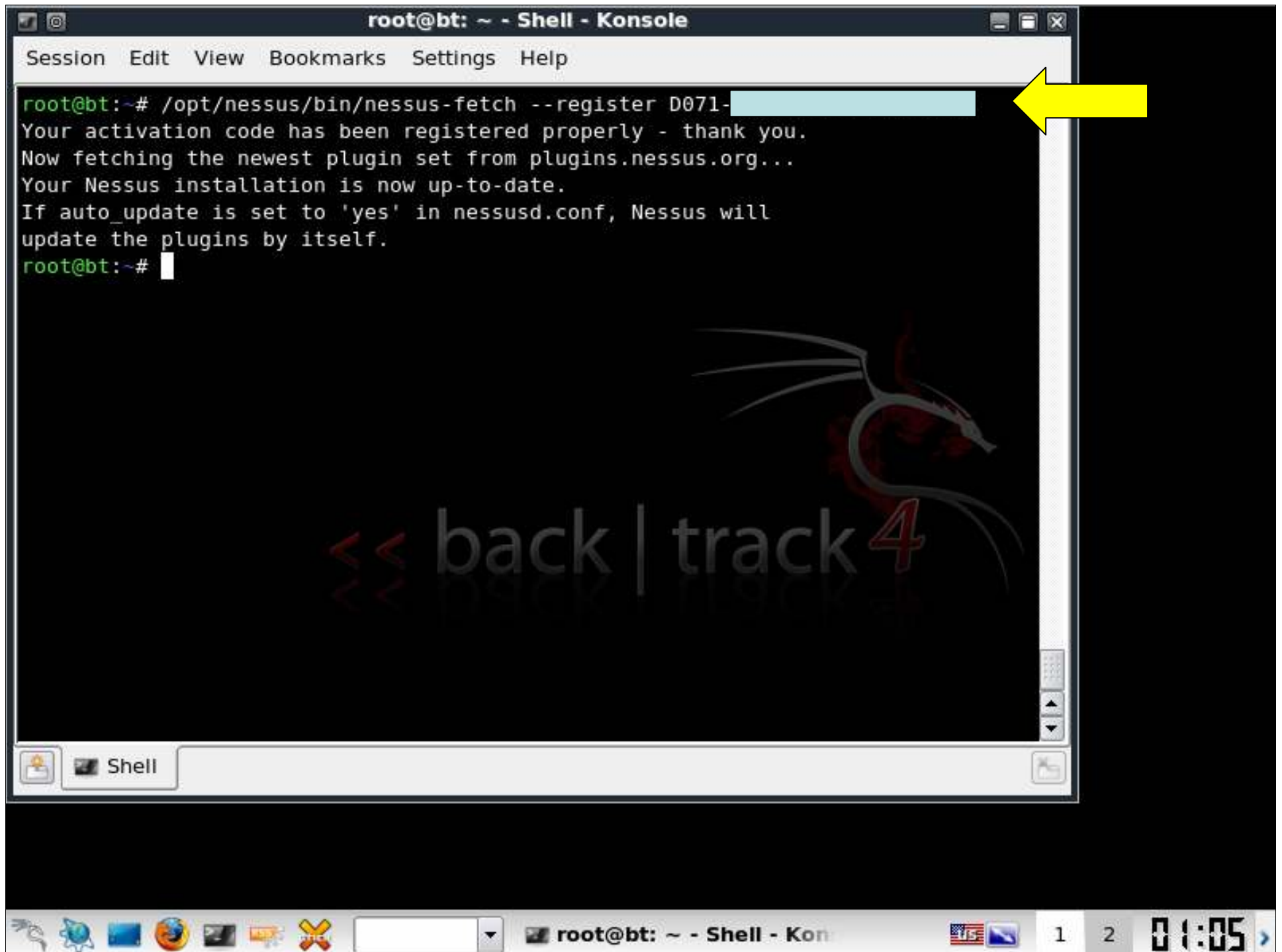
```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# /opt/nessus/sbin/nessus-adduser
Login : hacker_deluxe
Authentication (pass/cert) : [pass]
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that hacker_deluxe has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

```





```
root@bt: ~ - Shell - Konsole <2>  
Session Edit View Bookmarks Settings Help  
root@bt:~# update-rc.d -f nessusd remove  
Removing any system startup links for /etc/init.d/nessusd ...  
/etc/rc0.d/K20nessusd  
/etc/rc1.d/K20nessusd  
/etc/rc2.d/S20nessusd  
/etc/rc3.d/S20nessusd  
/etc/rc4.d/S20nessusd  
/etc/rc5.d/S20nessusd  
/etc/rc6.d/K20nessusd  
root@bt:~#
```



<< back | track 4

<< back | track 龍

```
X.Org X Server 1.5.2
Release Date: 10 October 2008
X Protocol Version 11, Revision 0
Build Operating System: Linux 2.6.24-19-server i686 Ubuntu
Current Operating System: Linux bt 2.6.29.4 #3 SMP Mon May 25 18:50:05 EDT 2009 i686
Build Date: 09 March 2009 10:48:54AM
xorg-server 2:1.5.2-2ubuntu3.1 (buildd@rothera.buildd)
    Before reporting problems, check http://wiki.x.org
    to make sure that you have the latest version.
Module Loader present
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Sat Aug 15 00:54:12 2009
(==) Using config file: "/etc/X11/xorg.conf"
(EE) AIGLX error: vboxvideo does not export required DRI extension
(EE) AIGLX: reverting to software rendering

Broadcast message from root@bt
        (/dev/pts/1) at 1:11 ...

The system is going down for reboot NOW!
```



"The quieter you become, the more you are able to hear."

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# /etc/init.d/nessusd start  
Starting Nessus : .  
root@bt:~#
```

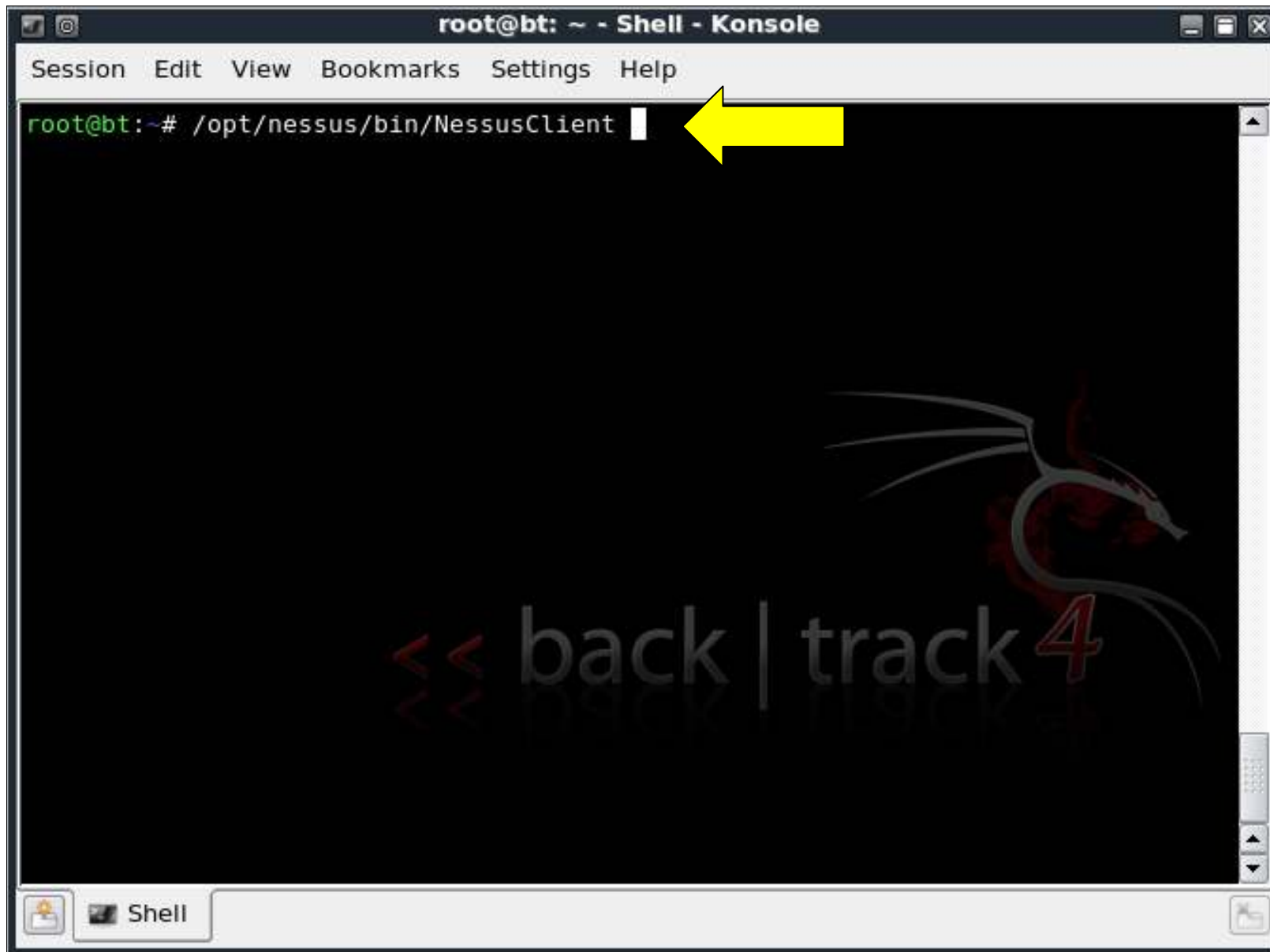
back | track4

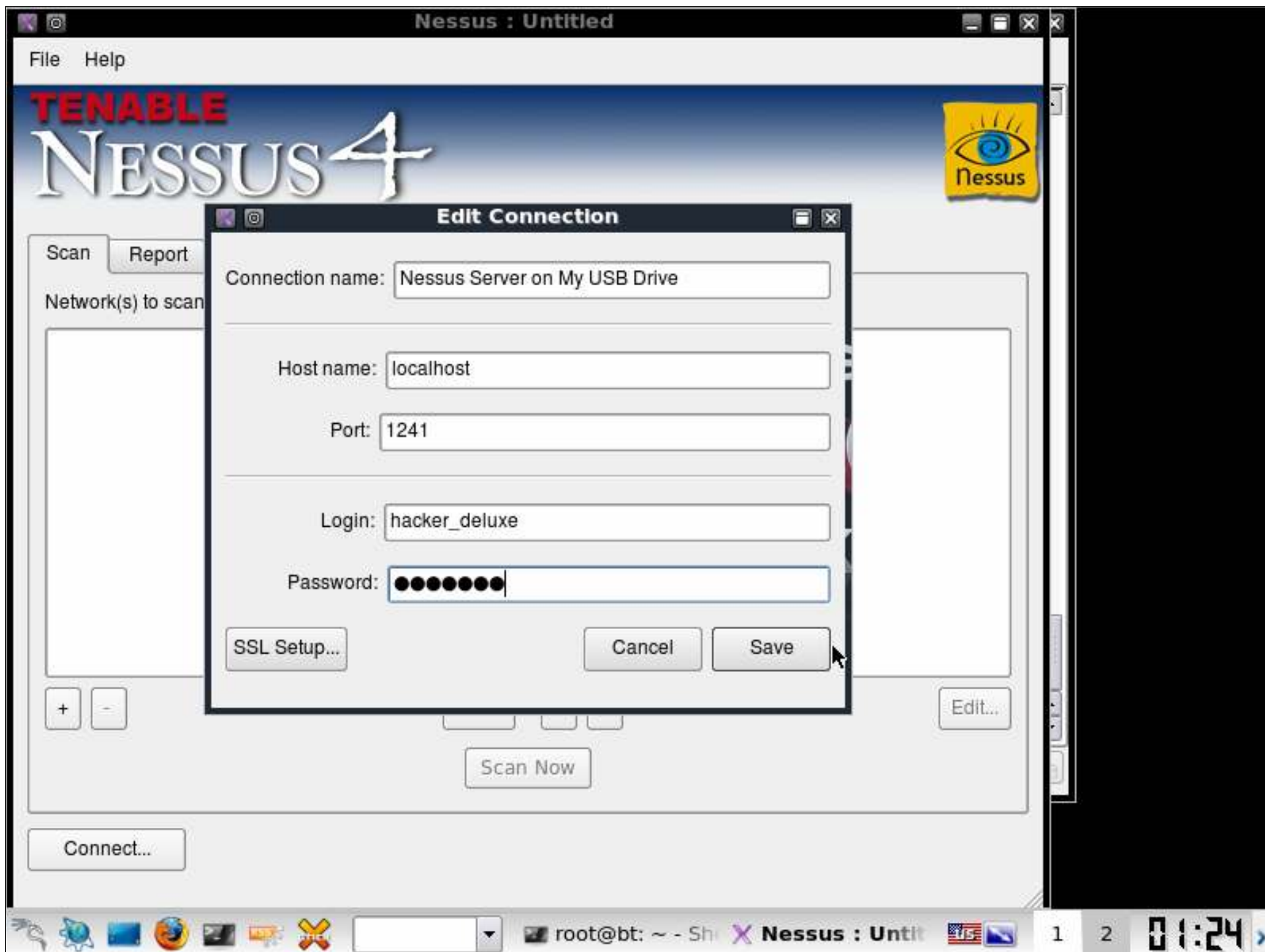
Shell

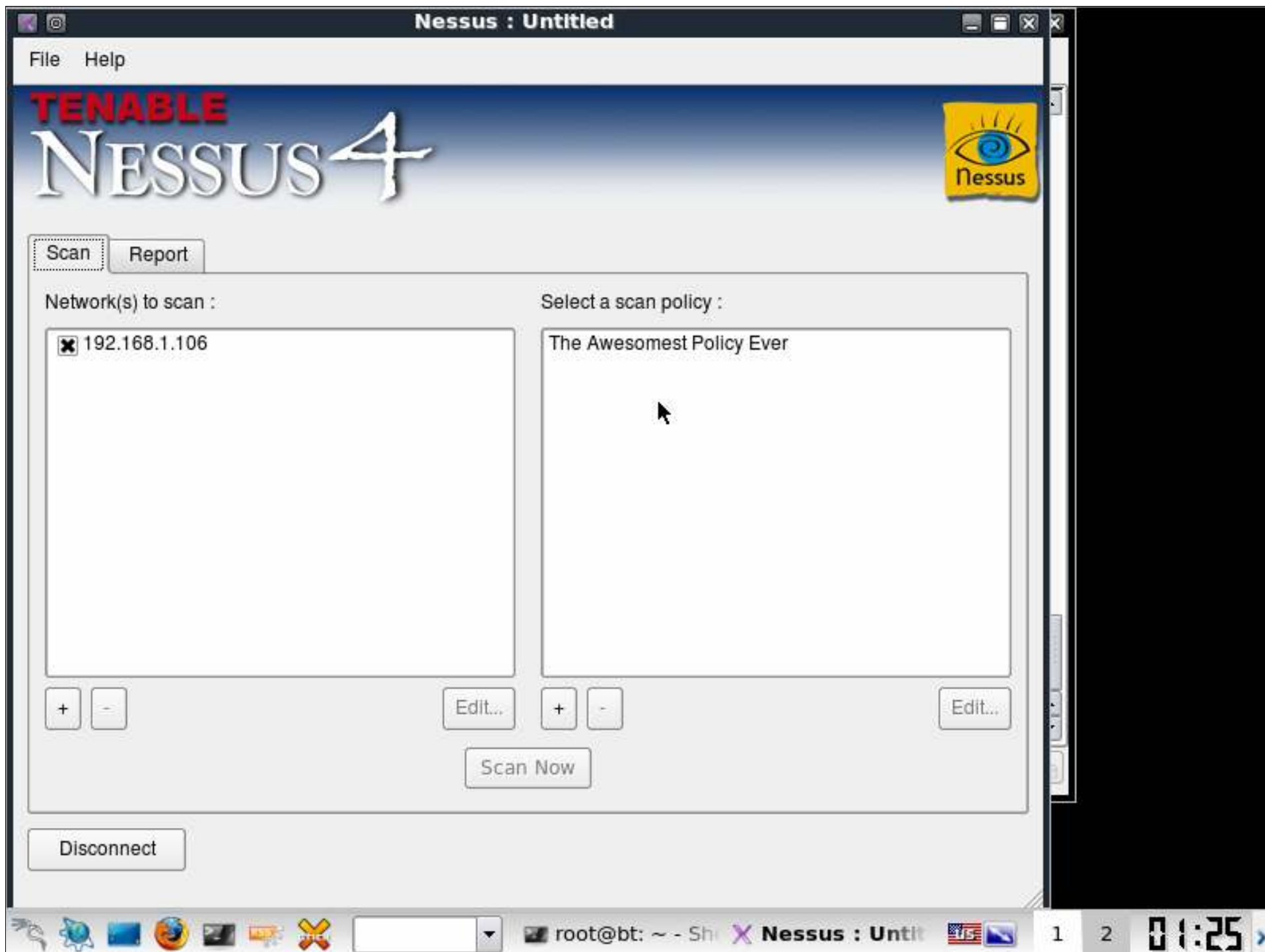
```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# netstat -napt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
root@bt:~# netstat -napt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:1241             0.0.0.0:*               LISTEN
8493/nessusd
tcp6       0      0 :::1241                 :::*                    LISTEN
8493/nessusd
root@bt:~# clea
```

<< back | track 4








Nessus : Untitled

File Help

TENABLE

NESSUS4



Scan

Report

Report:

09/08/15 01:25:37 AM - The Awesomest Policy Ever

Delete

Export...

192.168.1.106

general/tcp

general/udp

general/icmp

ipp (631/tcp)

mysql (3306/tcp)

CVE : CVE-1999-0524

Nessus ID : [10114](#)

Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Synopsis :

The remote host leaks memory in network packets.

Description :

The remote host is vulnerable to an 'Etherleak' - the remote ethernet driver seems to leak bits of the content of the memory of the remote


Filter...

Stylesheet:

Sort By CVE


View template...

Disconnect



root@bt: ~ - Sh

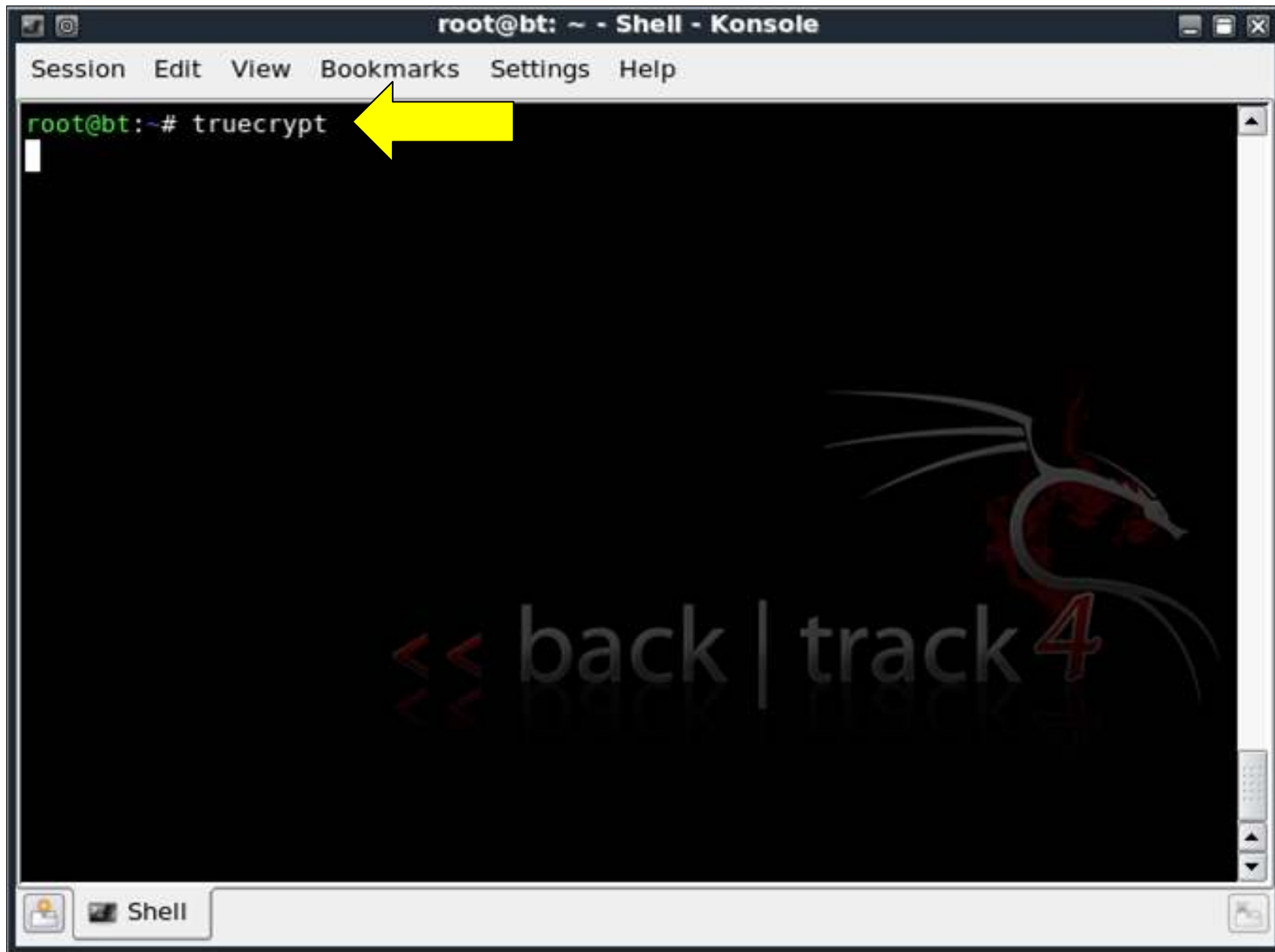
Nessus : Untit

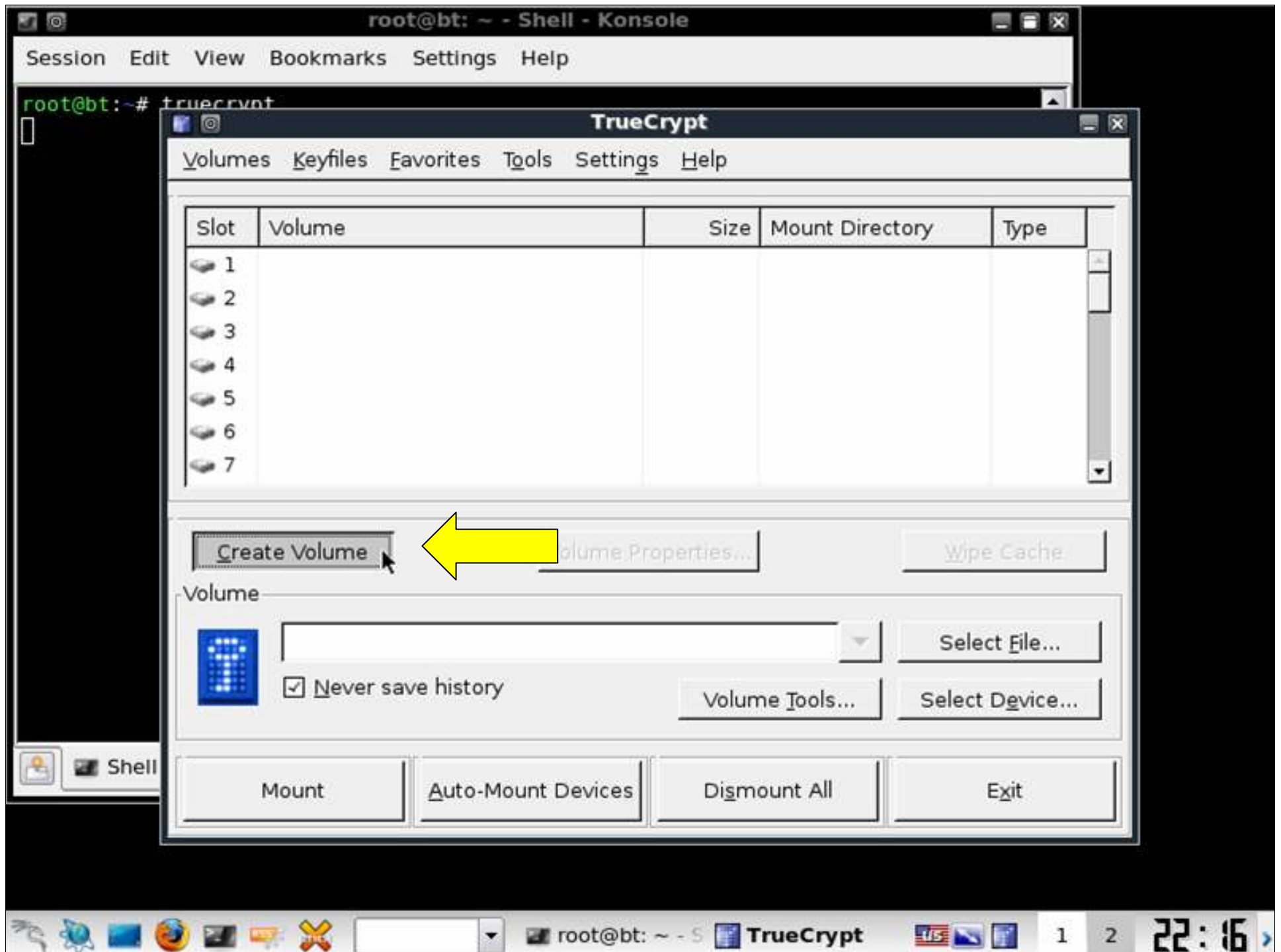


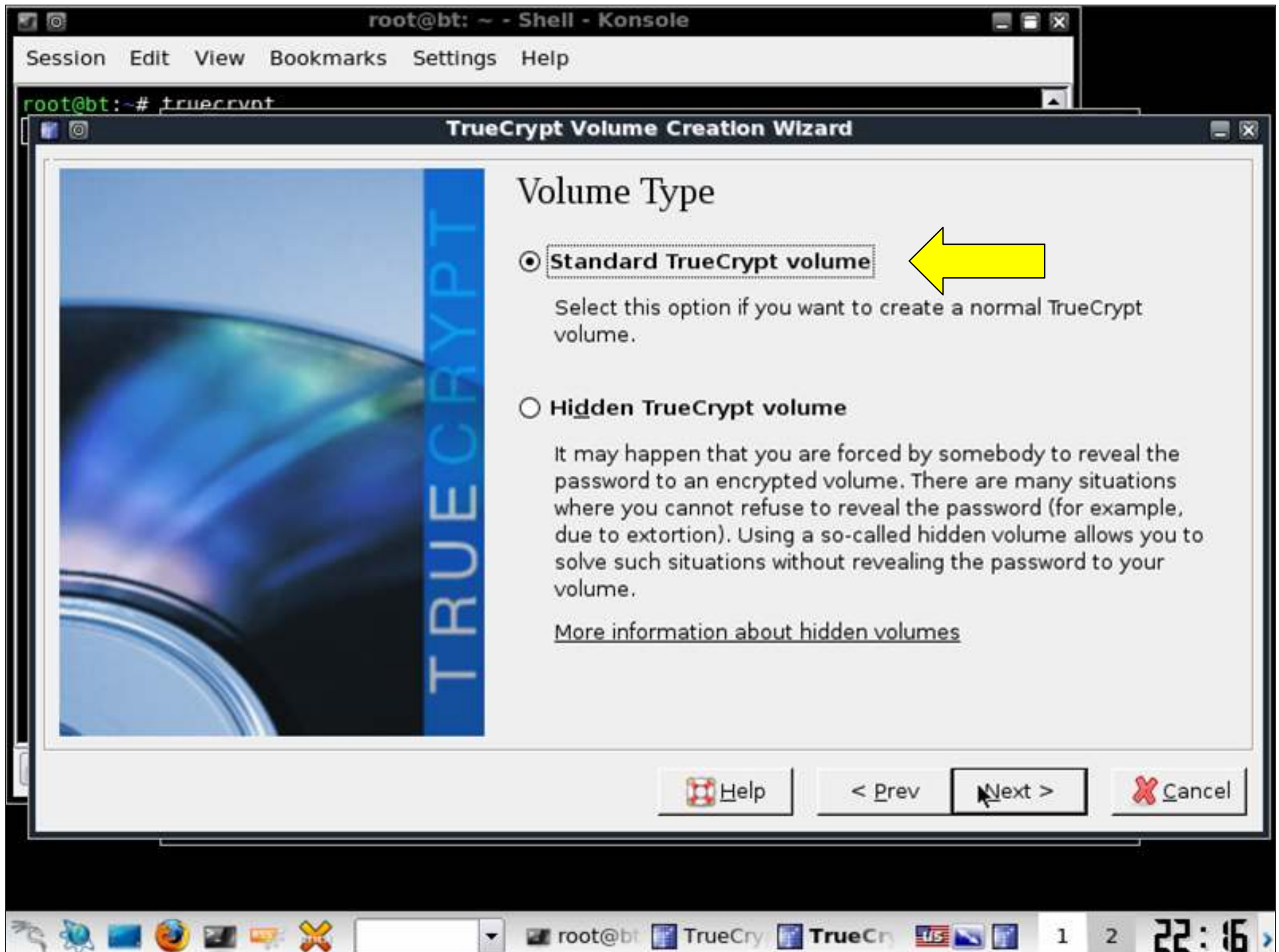
1 2

01:26

Configure Encryption







root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

root@bt:~# truecrypt

TrueCrypt Volume Creation Wizard

Volume Type

☒ **Standard TrueCrypt volume**

Select this option if you want to create a normal TrueCrypt volume.

☐ **Hidden TrueCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

[More information about hidden volumes](#)



Help

< Prev

Next >



Cancel

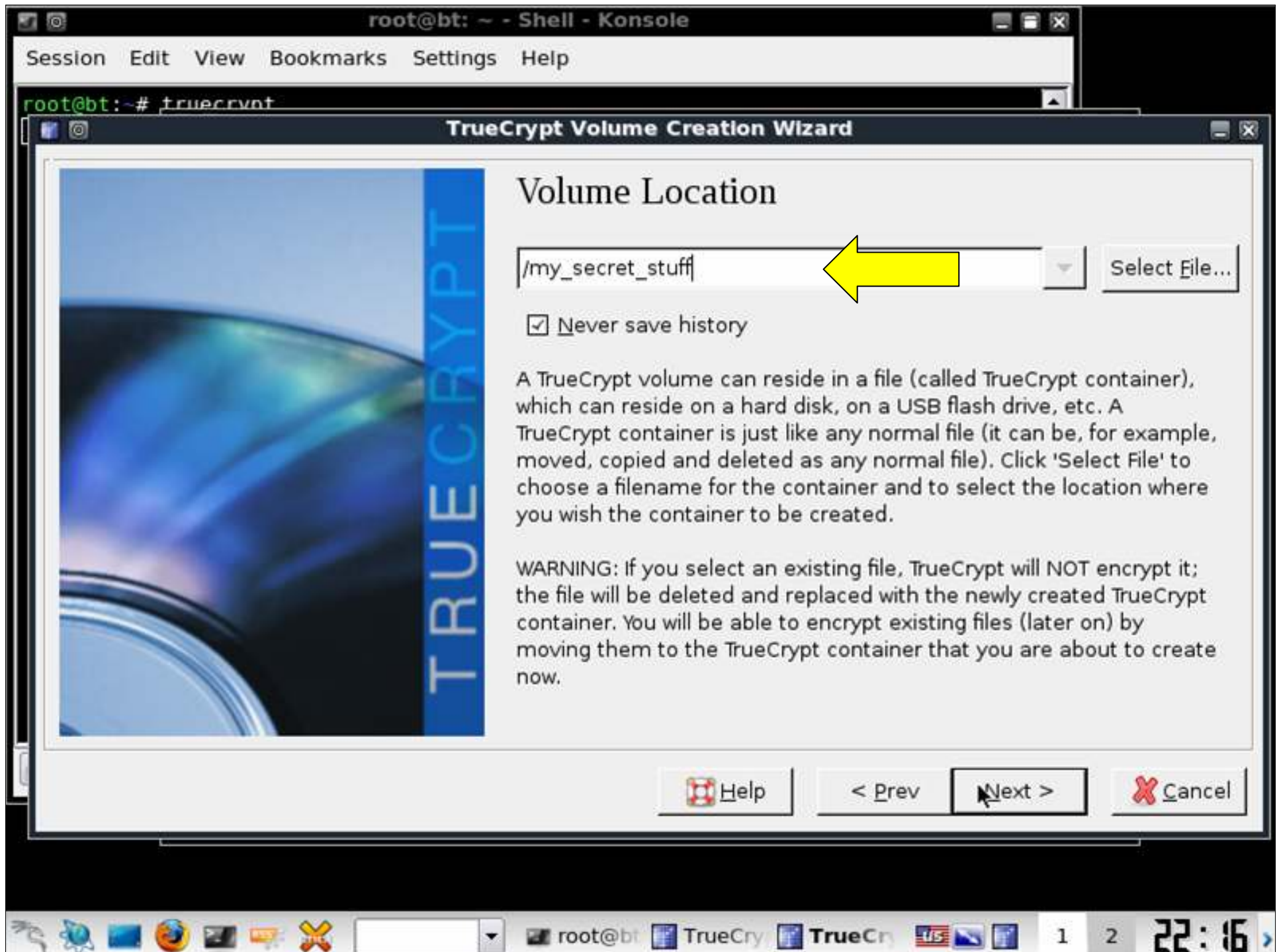
root@bt

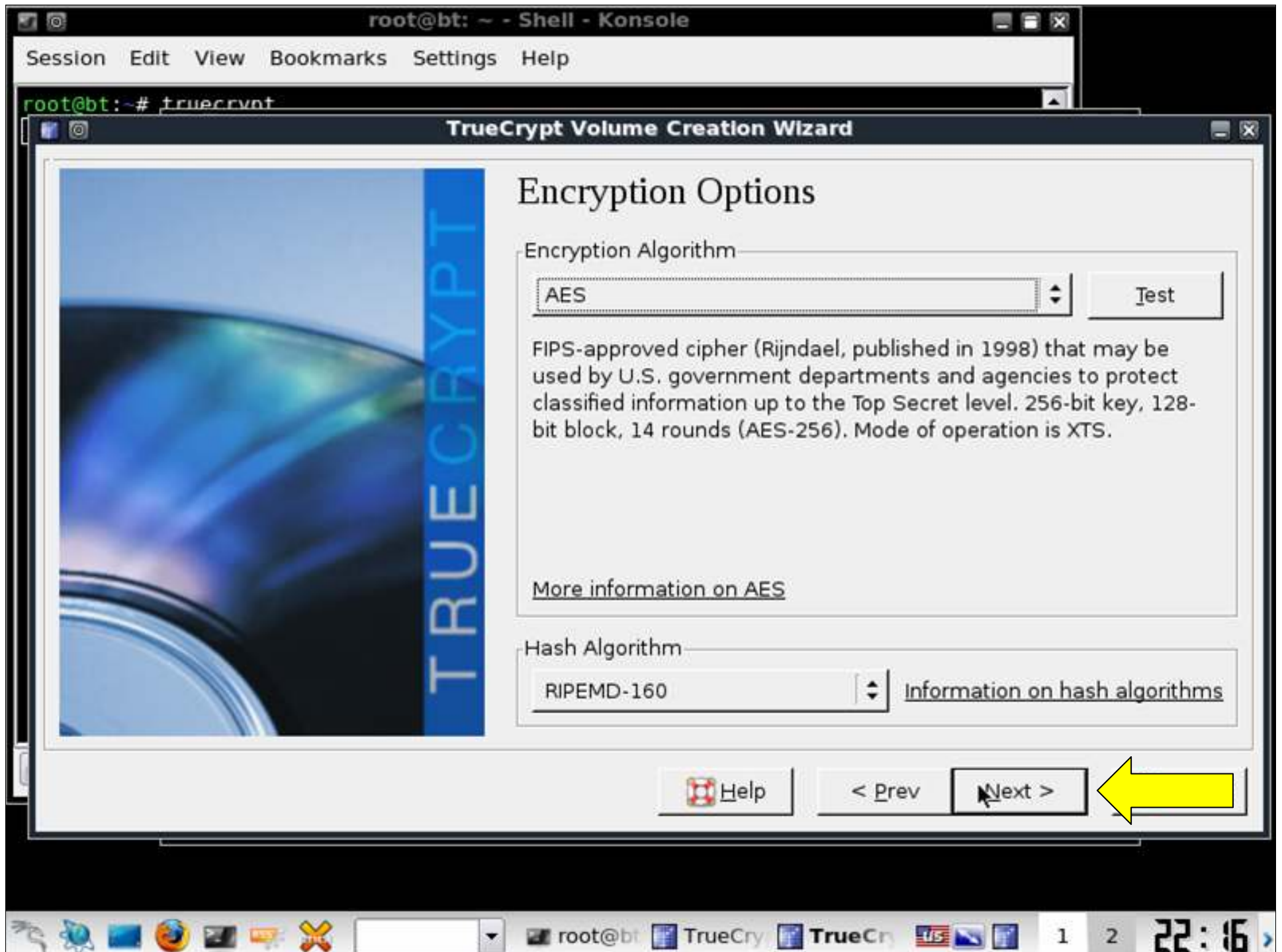
TrueCrypt

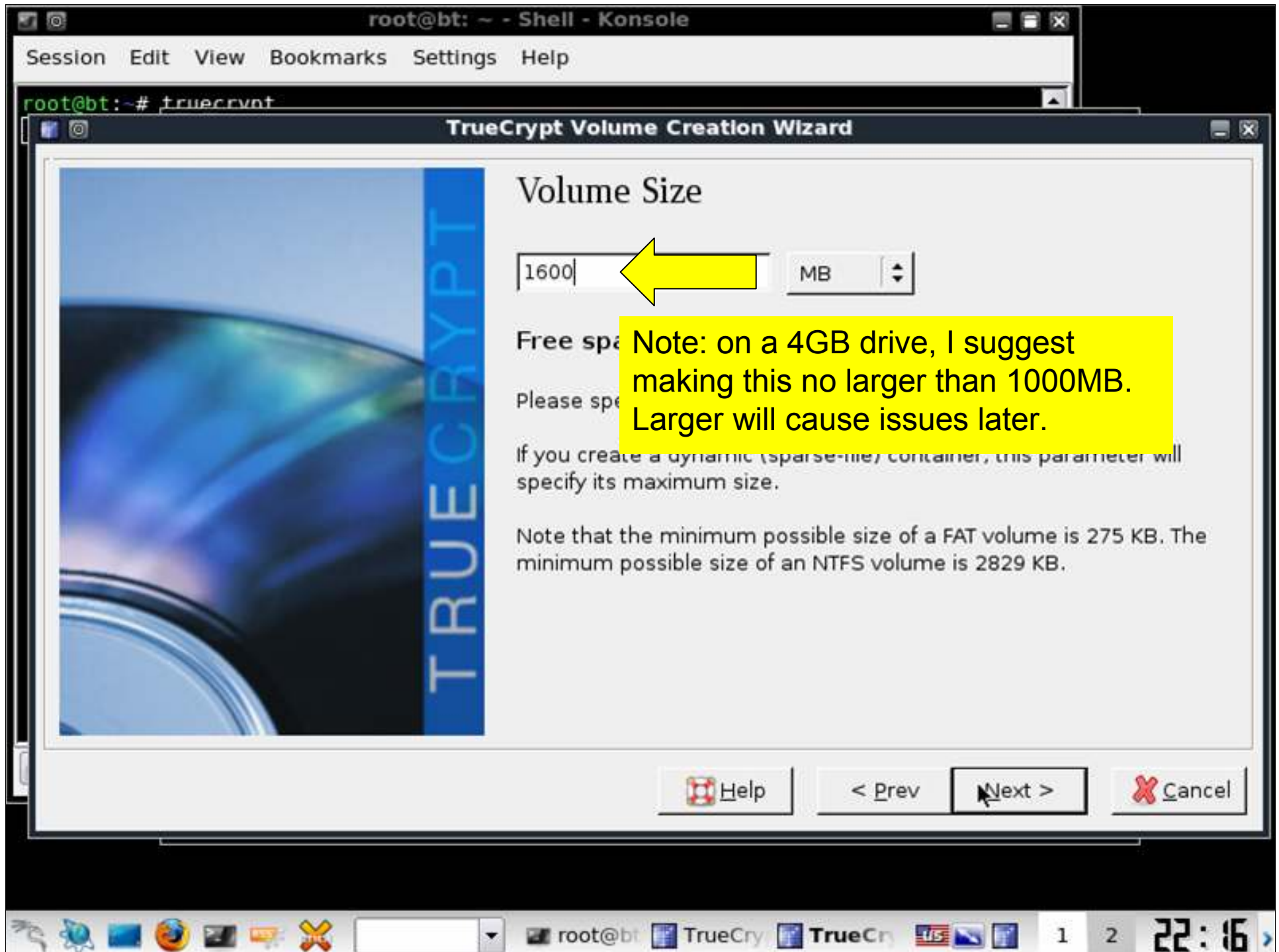
TrueCrypt

1 2

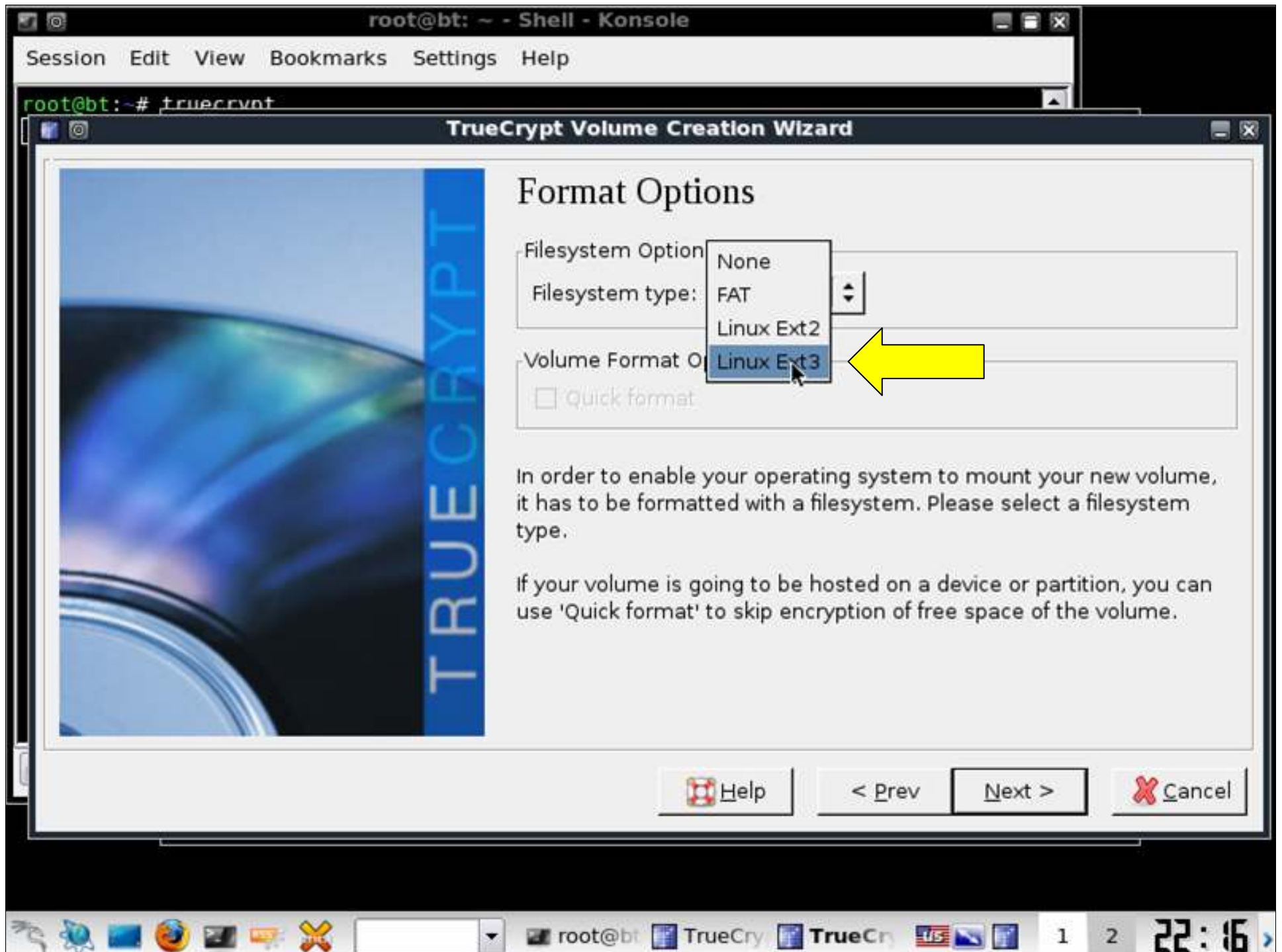
22:16

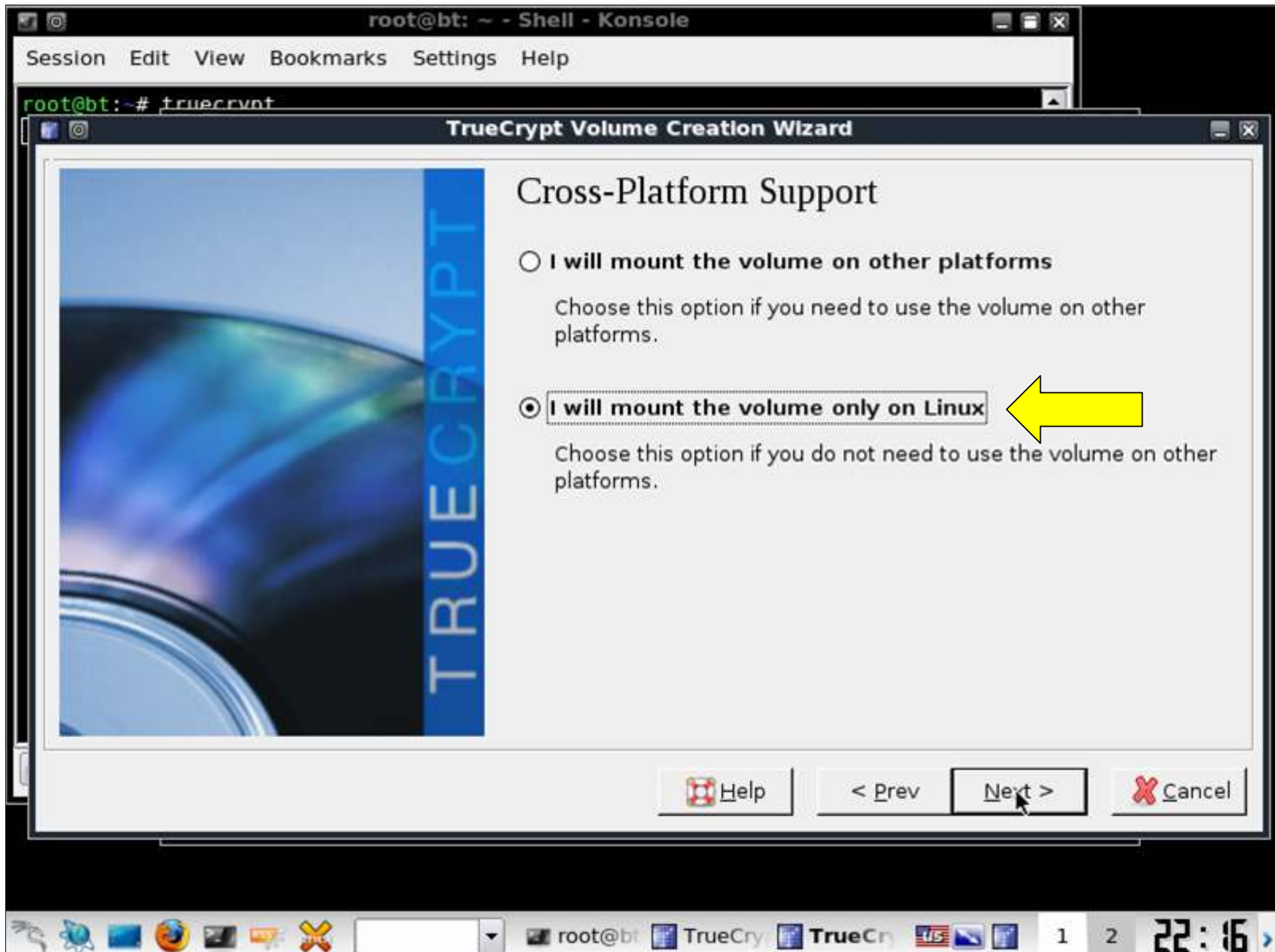


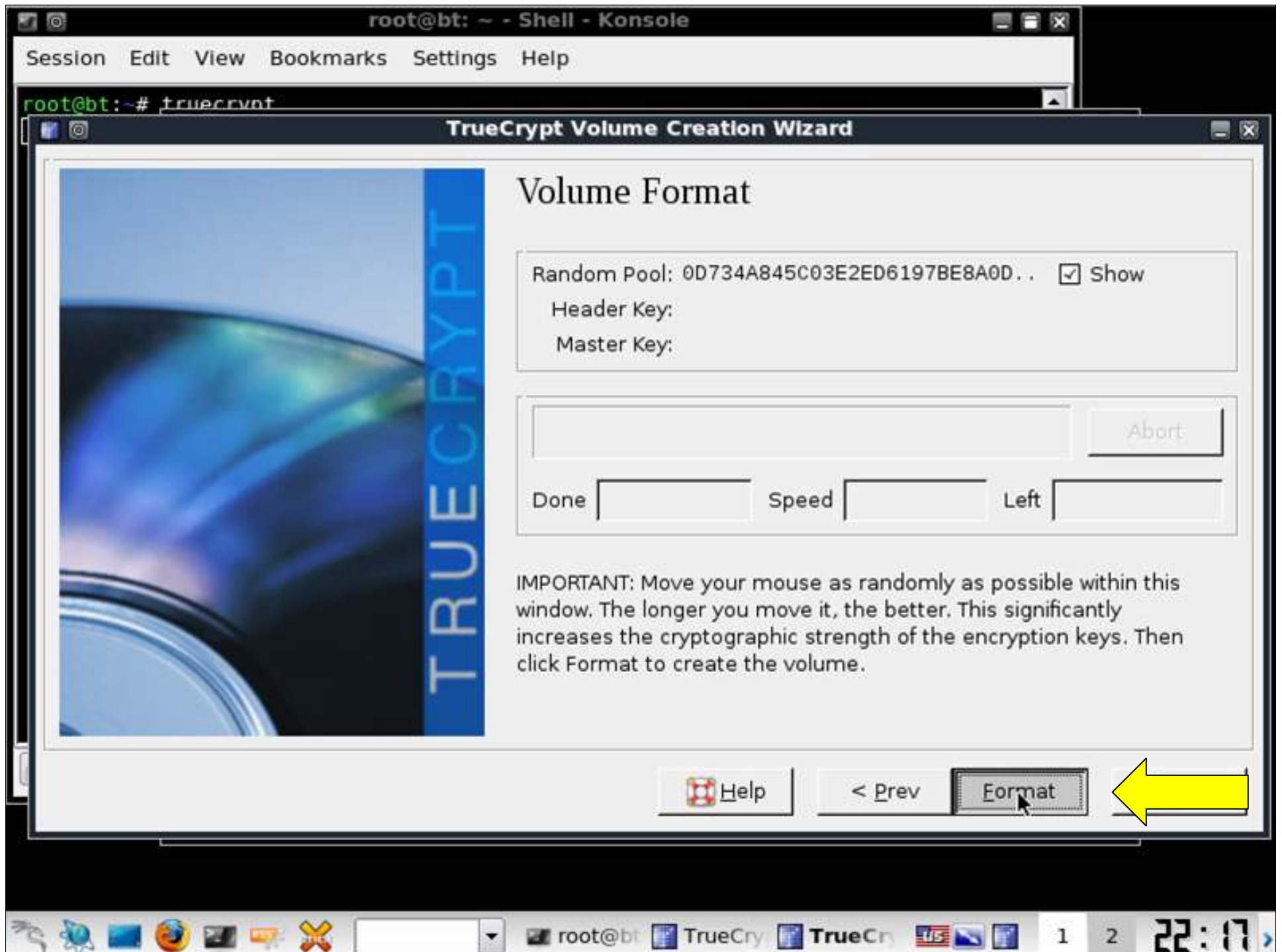


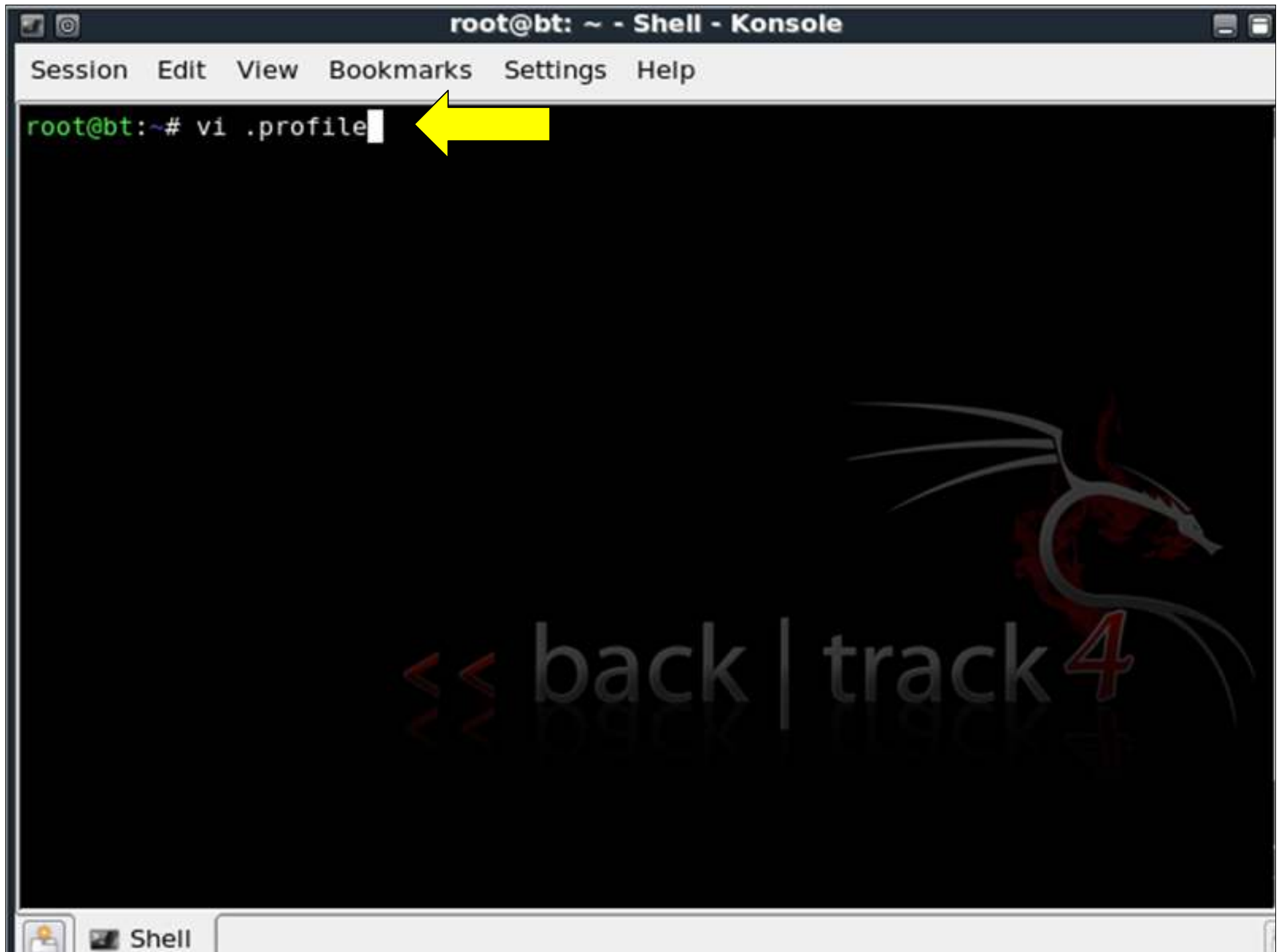













```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

/usr/bin/truecrypt -t -k '' --protect-hidden=no /my_secret_stuff /media/truecrypt1

mesg n

<< back | track4
```

<< back | track 龍

```
Checking file systems...fsck 1.41.3 (12-Oct-2008)
done.
Mounting local filesystems...done.
Activating swapfile swap...done.
Skipping firewall: ufw (not enabled)...done.
Setting up console font and keymap...done.
Starting VirtualBox Additions ...done.
Starting VirtualBox Guest Addition service ...done.
Loading cpufreq kernel modules...done (none).
Loading ACPI modules....
Starting ACPI services....
Starting system log daemon....
Doing Wacom setup....
Starting kernel log daemon....
Starting system message bus: dbus.
CPUFreq Utilities: Setting ondemand CPUFreq governor...disabled, governor not available...done.
Starting Nessus : .
Starting Hardware abstraction layer: hald.
Starting System Tools Backends: system-tools-backends.
Starting periodic command scheduler: crond.


BackTrack 4 (PwnSauce) Penetration Testing and Auditing Distribution

Enter password for /my_secret_stuff:
```



"The quieter you become, the more you are able to hear."



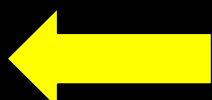
```
root@bt:~# mount
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
rootfs on / type rootfs (rw)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
/dev/sdal on /media/cdrom0 type vfat (rw,fmask=0022,dmask=0022,codepage=cp437,io
charset=iso8859-1)
/dev/loop0 on /rofs type squashfs (ro,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
/dev/hdc on /media/cdrom0 type iso9660 (ro)
truecrypt on /tmp/.truecrypt aux_mnt1 type fuse.truecrypt (rw,nosuid,nodev,allow
_other)
/dev/mapper/truecrypt1 on /media/truecrypt1 type ext3 (rw)
```



```
root@bt:~#
```

Tweak a Few Things

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# nmap --version
Nmap version 4.85BETA10 ( http://nmap.org )
root@bt:~#
```




```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help



root@bt:~# apt-get update
Get:1 http://archive.offensive-security.com pwnsauc Release.gpg [489B]
Ign http://archive.offensive-security.com pwnsauc/main Translation-en_US
Ign http://archive.offensive-security.com pwnsauc/microverse Translation-en_US
Ign http://archive.offensive-security.com pwnsauc/macrovers Translation-en_US
Ign http://archive.offensive-security.com pwnsauc/restricted Translation-en_US
Ign http://archive.offensive-security.com pwnsauc/universe Translation-en_US
Ign http://archive.offensive-security.com pwnsauc/multiverse Translation-en_US
Get:2 http://archive.offensive-security.com pwnsauc Release [9106B]
Get:3 http://archive.offensive-security.com pwnsauc/main Packages [1560kB]
Get:4 http://archive.offensive-security.com pwnsauc/microverse Packages [54.9kB]
]
Get:5 http://archive.offensive-security.com pwnsauc/macrovers Packages [11.5kB]
]
Get:6 http://archive.offensive-security.com pwnsauc/restricted Packages [11.9kB]
]
Get:7 http://archive.offensive-security.com pwnsauc/universe Packages [4560kB]
Get:8 http://archive.offensive-security.com pwnsauc/multiverse Packages [204kB]
Fetched 6412kB in 18s (338kB/s)
Reading package lists... Done
root@bt:~#
```

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

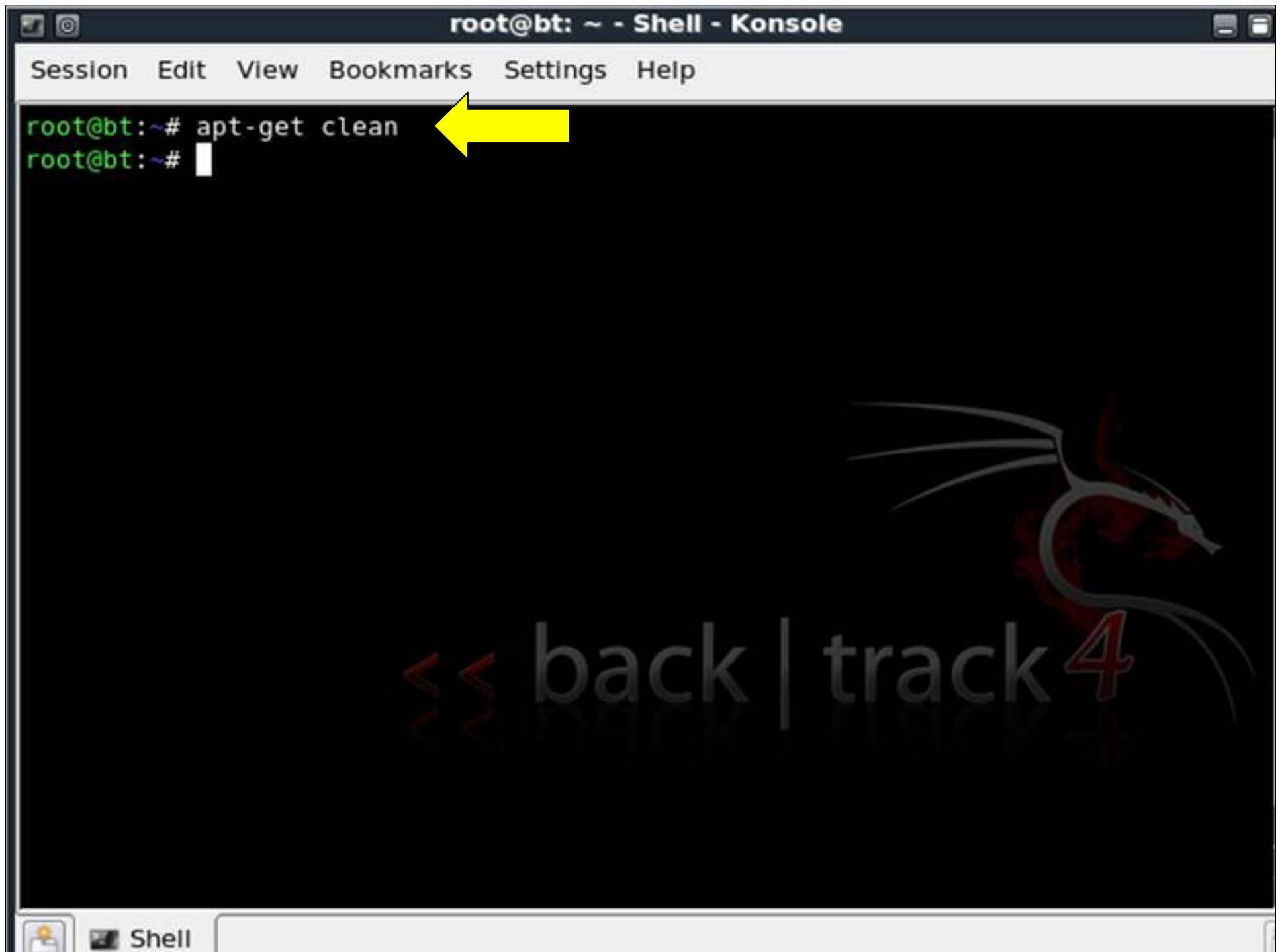
root@bt:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  backtrack-web backtrack-wireless backtrack-world framework3
The following packages will be upgraded:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-common
  backtrack-bruteforce crunch dbus dbus-x11 dhcp3-client dhcp3-common
  dhcp3-server giskismet irssi kismet-newcore libcompress-raw-zlib-perl
  libdbus-1-3 libperl5.10 libpulse0 libsasl2-2 libsasl2-modules libssl-dev
  libssl0.9.8 libtiff4 medusa medusa-menu nmap openssl perl perl-base
  perl-modules proxystrike pyrit seat sslstrip w3af
35 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
Need to get 55.8MB of archives.
After this operation, 50.9MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://archive.offensive-security.com pwnsauce/main perl-modules 5.10.0-11
.lubuntu2.3 [3273kB]
0% [1 perl-modules 0/3273kB 0%]
```



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# nmap --version
Nmap version 5.00 ( http://nmap.org )
root@bt:~#
```


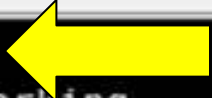


<< back | track4

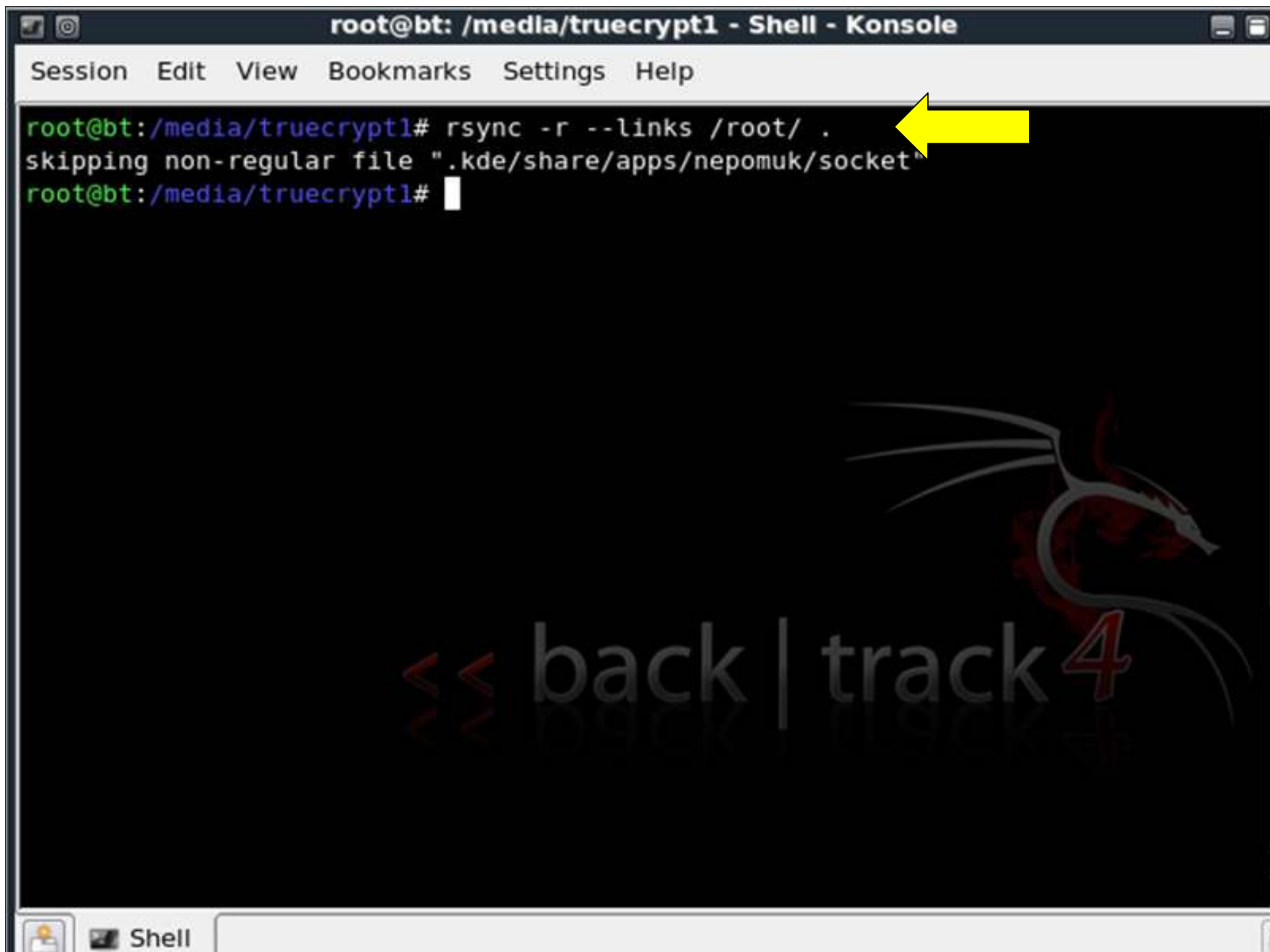


```
root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help

root@bt:~# update-rc.d networking defaults
Adding system startup for /etc/init.d/networking ...
/etc/rc0.d/K20networking -> ../init.d/networking
/etc/rc1.d/K20networking -> ../init.d/networking
/etc/rc6.d/K20networking -> ../init.d/networking
/etc/rcS.d/S20networking -> ../init.d/networking
root@bt:~#
```



<< back | track4





```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
# ~/.profile: executed by Bourne-compatible login shells.

if [ "$BASH" ]; then
  if [ -f ~/.bashrc ]; then
    . ~/.bashrc
  fi
fi

/usr/bin/truecrypt -t -k '' --protect-hidden=no /my_secret_stuff /media/truecrypt1

export HOME=/media/truecrypt1
export HISTFILE=/media/truecrypt1
cd

mesg n
```



<< back | track 龍

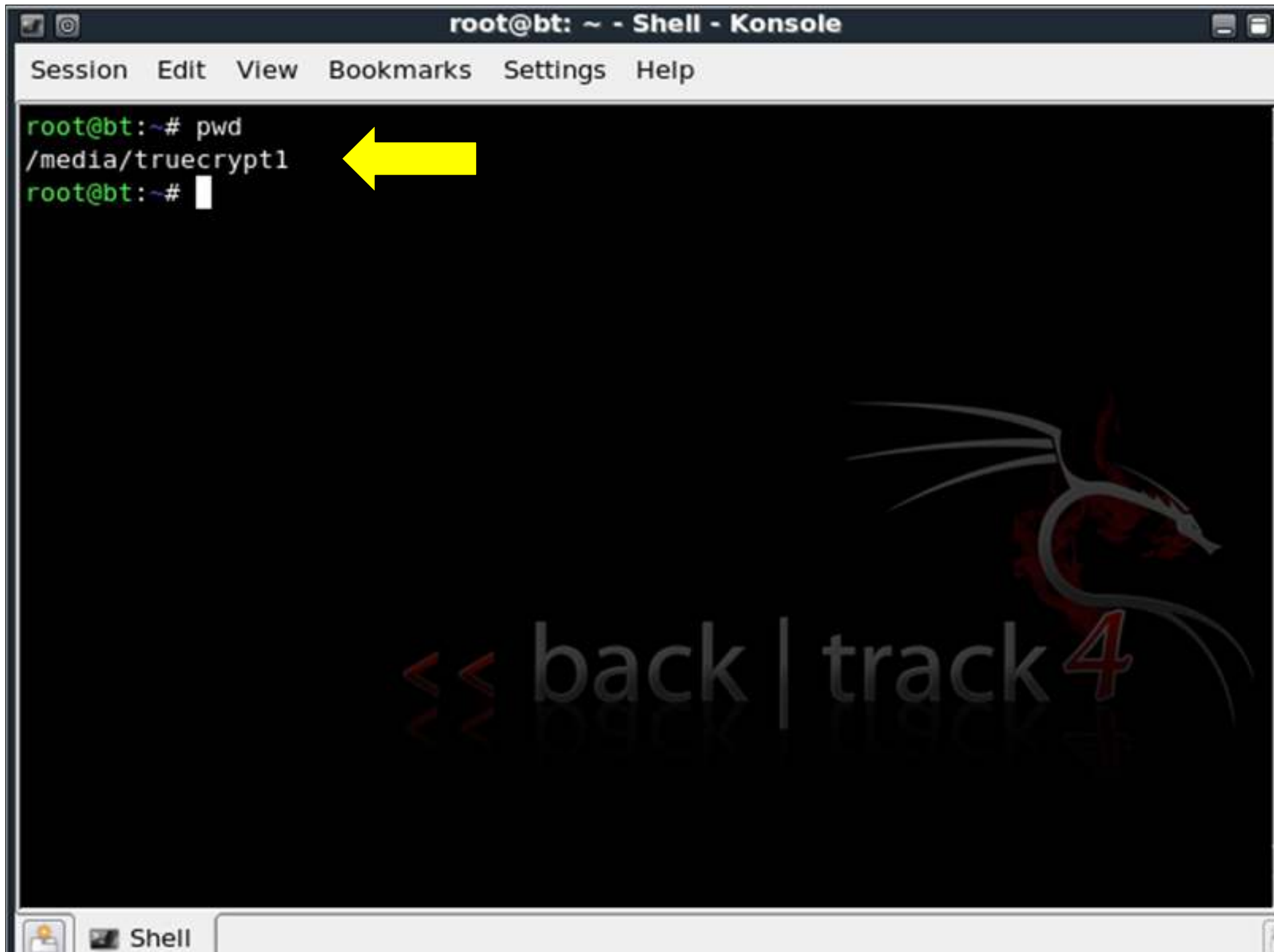
```
X.Org X Server 1.5.2
Release Date: 10 October 2008
X Protocol Version 11, Revision 0
Build Operating System: Linux 2.6.24-19-server i686 Ubuntu
Current Operating System: Linux bt 2.6.29.4 #3 SMP Mon May 25 18:50:05 EDT 2009 i686
Build Date: 09 March 2009 10:48:54AM
xorg-server 2:1.5.2-2ubuntu3.1 (buildd@rothera.buildd)
    Before reporting problems, check http://wiki.x.org
    to make sure that you have the latest version.
Module Loader present
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Sun Aug 16 22:40:13 2009
(==) Using config file: "/etc/X11/xorg.conf"
(EE) AIGLX error: vboxvideo does not export required DRI extension
(EE) AIGLX: reverting to software rendering

Broadcast message from root@bt
        (/dev/pts/1) at 22:42 ...

The system is going down for reboot NOW!
```

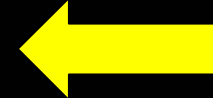


"The quieter you become, the more you are able to hear."

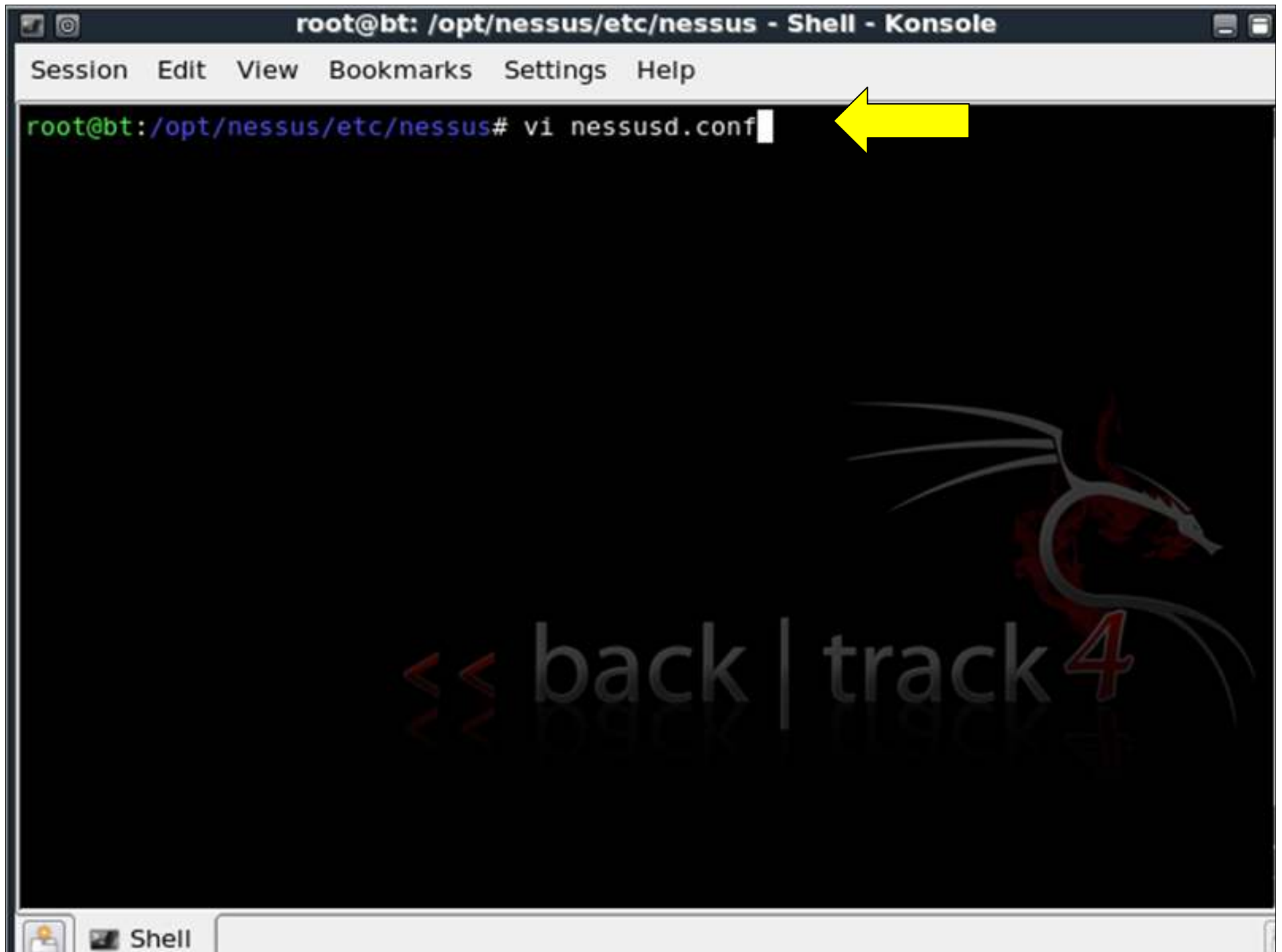


Session Edit View Bookmarks Settings Help

```
root@bt:/# cd /media/truecrypt1
root@bt:/media/truecrypt1# mkdir -p nessus/logs
root@bt:/media/truecrypt1# cd /opt/nessus/etc/nessus
root@bt:/opt/nessus/etc/nessus#
```



<< back | track4



```
root@bt: /opt/nessus/etc/nessus - Shell - Konsole

Session Edit View Bookmarks Settings Help

# Every line starting with a '#' is a comment


# Automatic plugins updates - if enabled and Nessus is registered, then
# fetch the newest plugins from plugins.nessus.org automatically
auto_update = yes
# Number of hours to wait between two updates
auto_update_delay = 24
# Should we purge the plugin db at each update ? (slower)
purge_plugin_db = no

# Maximum number of simultaneous hosts tested :
max_hosts = 40

# Maximum number of simultaneous checks against each host tested :
max_checks = 5

# Throttle scan when CPU is overloaded
throttle_scan = yes

# Log file :
logfile = /opt/nessus/var/nessus/logs/nessusd.messages
```



back | track4

Session Edit View Bookmarks Settings Help

```
# Every line starting with a '#' is a comment

# Automatic plugins updates - if enabled and Nessus is registered, then
# fetch the newest plugins from plugins.nessus.org automatically
auto_update = yes
# Number of hours to wait between two updates
auto_update_delay = 24
# Should we purge the plugin db at each update ? (slower)
purge_plugin_db = no

# Maximum number of simultaneous hosts tested :
max_hosts = 40

# Maximum number of simultaneous checks against each host tested :
max_checks = 5

# Throttle scan when CPU is overloaded
throttle_scan = yes

# Log file :
logfile = /media/truecrypt1/nessus/logs/nessusd.messages
```



```
root@bt: /opt/nessus/etc/nessus - Shell - Konsole

Session Edit View Bookmarks Settings Help

auto_update = yes
# Number of hours to wait between two updates
auto_update_delay = 24
# Should we purge the plugin db at each update ? (slower)
purge_plugin_db = no

# Maximum number of simultaneous hosts tested :
max_hosts = 40


# Maximum number of simultaneous checks against each host tested :
max_checks = 5

# Throttle scan when CPU is overloaded
throttle_scan = yes

# Log file :
logfile = /media/truecrypt1/nessus/logs/nessusd.messages

# Shall we log every details of the attack ? (disk intensive)
log_whole_attack = no

# Dump file for debugging output
dumpfile = /opt/nessus//var/nessus/logs/nessusd.dump
```



Session Edit View Bookmarks Settings Help

```
# Number of hours to wait between two updates
auto_update_delay = 24
# Should we purge the plugin db at each update ? (slower)
purge_plugin_db = no

# Maximum number of simultaneous hosts tested :
max_hosts = 40


# Maximum number of simultaneous checks against each host tested :
max_checks = 5

# Throttle scan when CPU is overloaded
throttle_scan = yes

# Log file :
logfile = /media/truecrypt1/nessus/logs/nessusd.messages

# Shall we log every details of the attack ? (disk intensive)
log_whole_attack = no

# Dump file for debugging output
dumpfile = /media/truecrypt1/nessus/logs/nessusd.dump
```



:

Resources

My Blog

Infosec Ramblings

<http://www.infosecramblings.com/backtrack>

Remote Exploit

Backtrack 4 Creators

<http://www.remote-exploit.org/>

Offensive Security

Backtrack/Pentesting Training

<http://www.offensive-security.com/>

Questions?

Contact Info

Kevin Riggins

Email: kriggins@infosecramblings.com

Twitter: [kriggins](https://twitter.com/kriggins)

LinkedIn: <http://www.linkedin.com/in/kevinriggins>