Make your own Hacker Gadget

Vivek Ramachandran

Chief Trainer

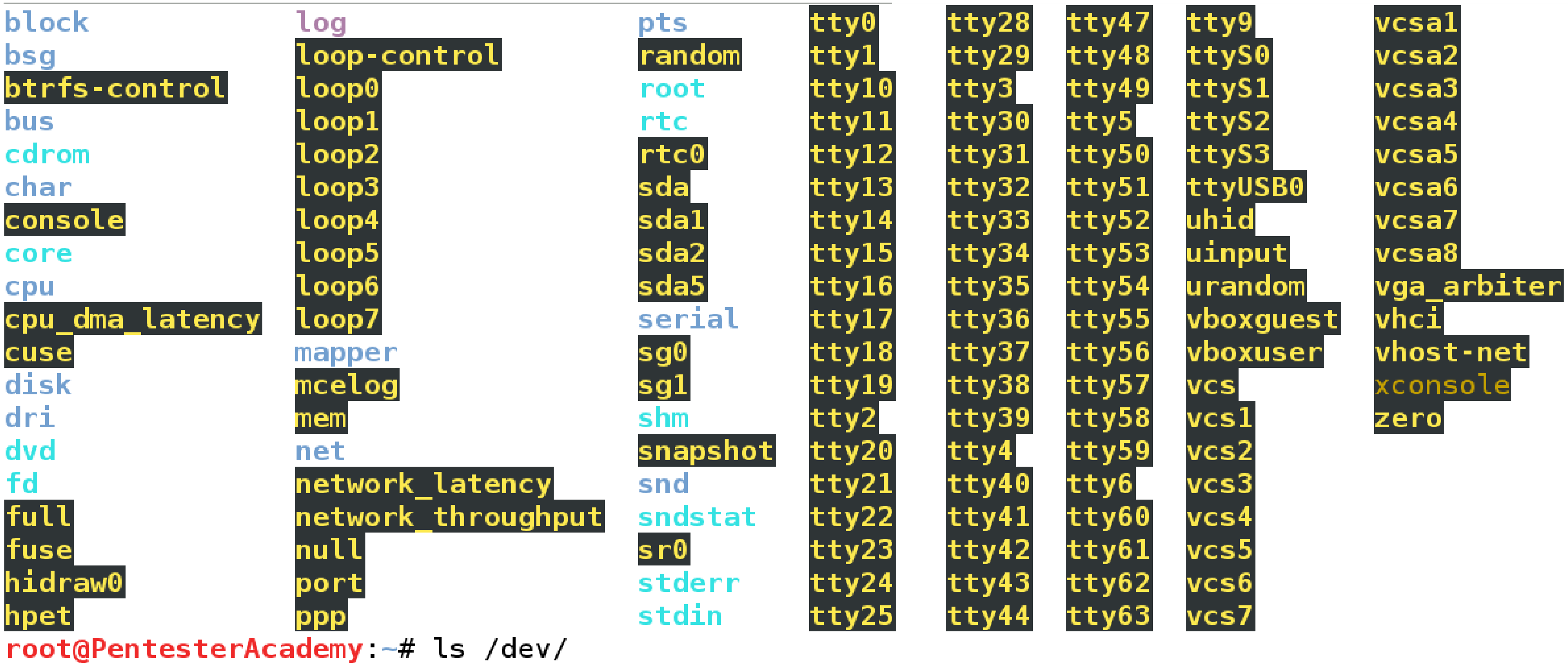
http://PentesterAcademy.com

Access Bootloader over Serial

IMPORTANT NOTE!

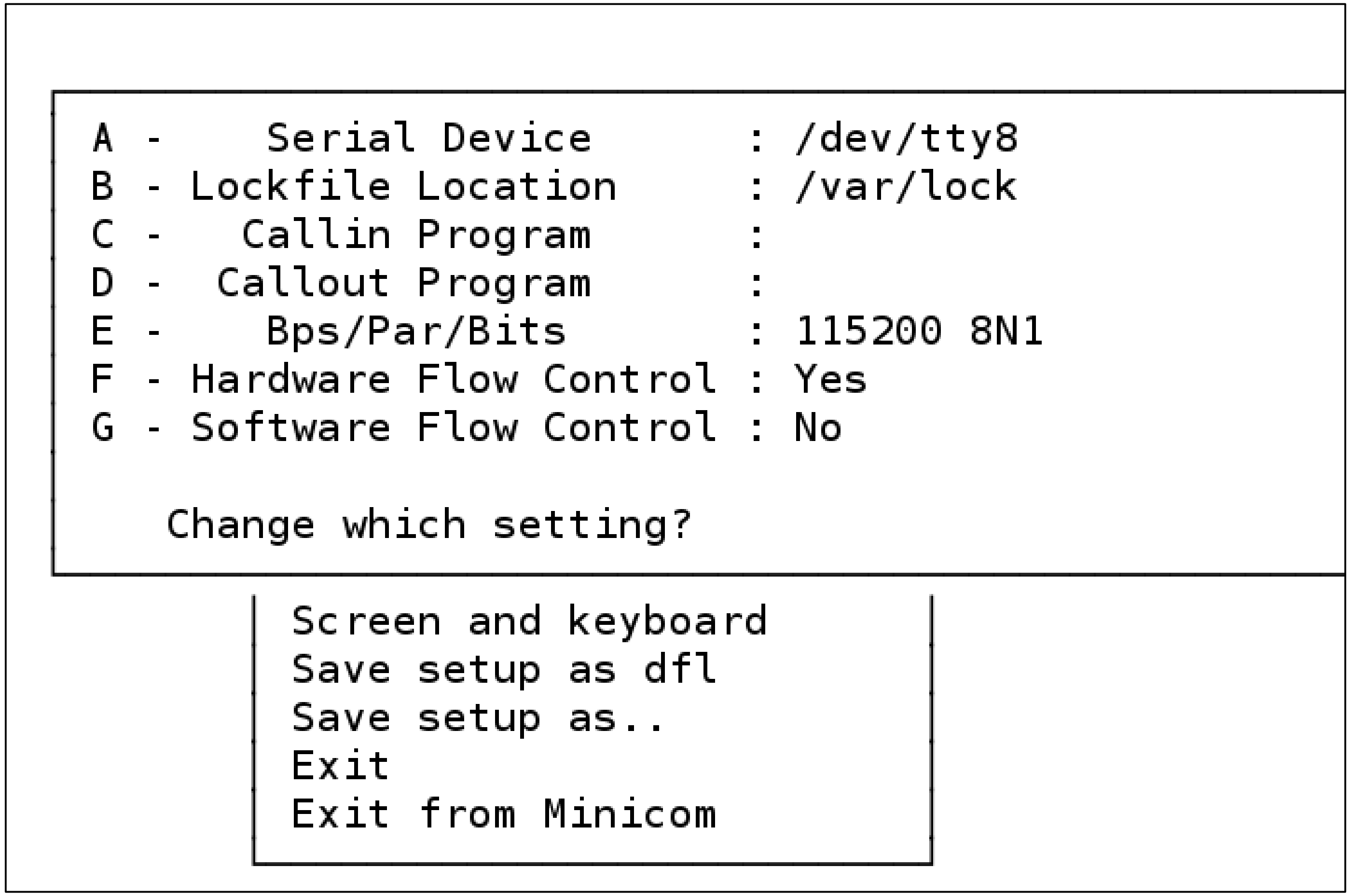
- We are using a MR-3020 straight out of the box for this demo!
- OpenWrt is not yet installed on it! => it runs manufacturer's firmware at this point!
- You can try with your OpenWrt version

Locate Device



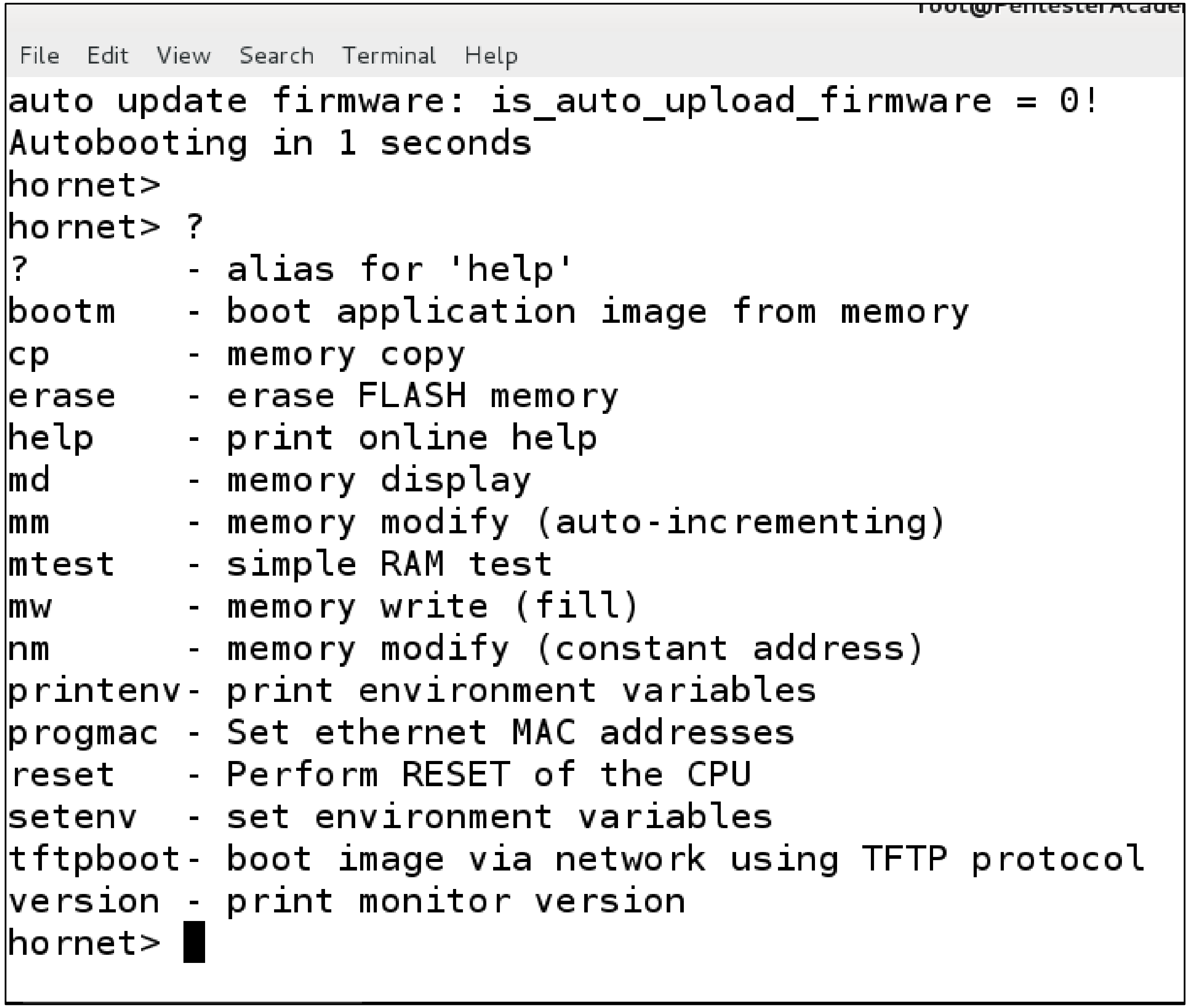
```
block            log                 pts       tty0    tty28   tty47   tty9       vcsa1
bsg              loop-control        random    tty1    tty29   tty48   ttyS0      vcsa2
btrfs-control    loop0               root      tty10   tty3    tty49   ttyS1      vcsa3
bus              loop1               rtc       tty11   tty30   tty5    ttyS2      vcsa4
cdrom            loop2               rtc0      tty12   tty31   tty50   ttyS3      vcsa5
char             loop3               sda       tty13   tty32   tty51   ttyUSB0    vcsa6
console          loop4               sda1      tty14   tty33   tty52   uhid       vcsa7
core             loop5               sda2      tty15   tty34   tty53   uinput     vcsa8
cpu              loop6               sda5      tty16   tty35   tty54   urandom    vga_arbiter
cpu_dma_latency  loop7               serial    tty17   tty36   tty55   vboxguest  vhci
cuse             mapper              sg0       tty18   tty37   tty56   vboxuser   vhost-net
disk             mcelog              sg1       tty19   tty38   tty57   vcs        xconsole
dri              mem                 shm       tty2    tty39   tty58   vcs1       zero
dvd              net                 snapshot  tty20   tty4    tty59   vcs2
fd               network_latency     snd       tty21   tty40   tty6    vcs3
full             network_throughput  sndstat   tty22   tty41   tty60   vcs4
fuse             null                sr0       tty23   tty42   tty61   vcs5
hidraw0          port                stderr    tty24   tty43   tty62   vcs6
hpet             ppp                 stdin     tty25   tty44   tty63   vcs7
root@PentesterAcademy:~# ls /dev/
```

Configure Minicom



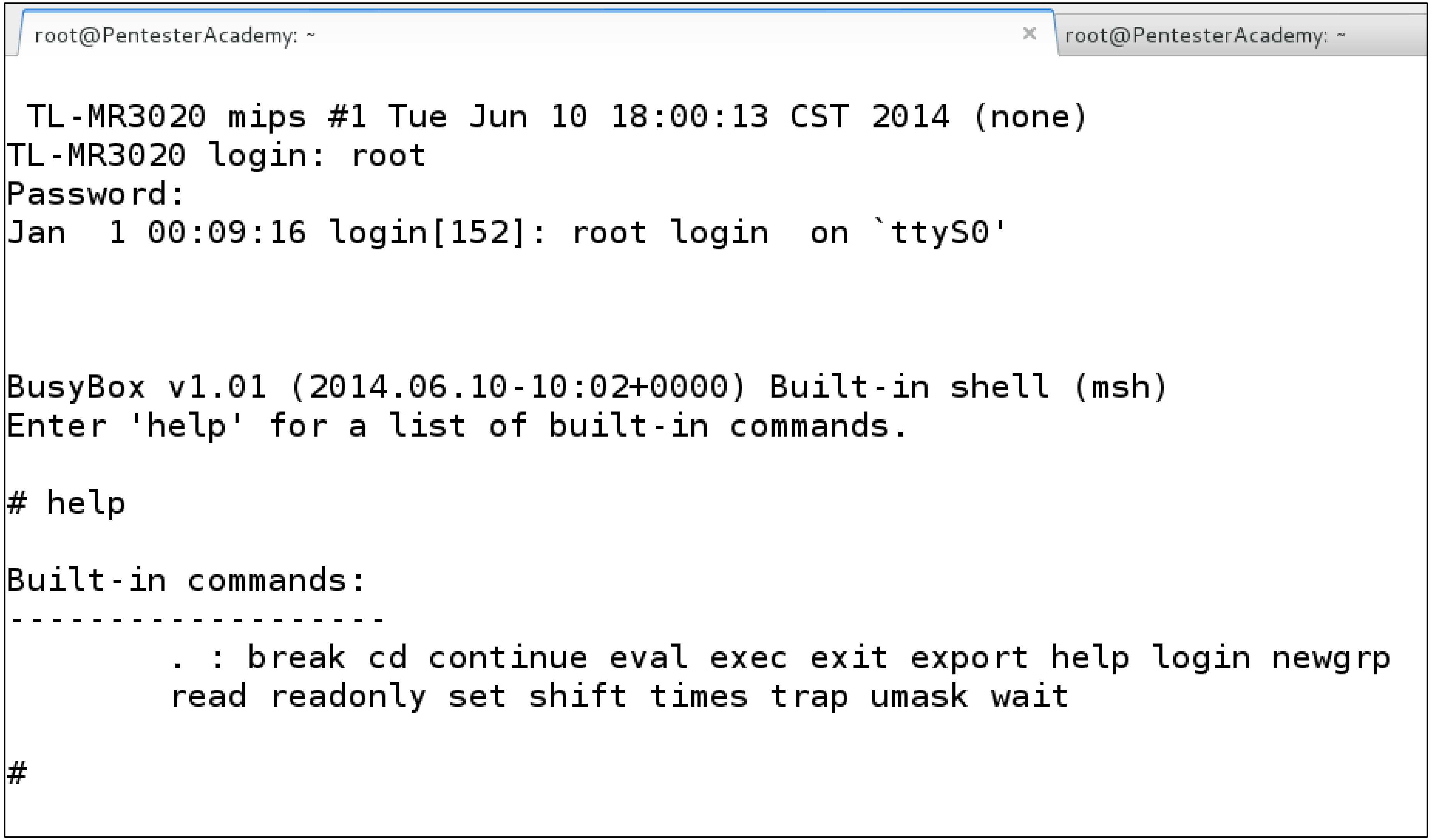
```
A -    Serial Device      : /dev/tty8
B - Lockfile Location     : /var/lock
C -   Callin Program      :
D -  Callout Program      :
E -    Bps/Par/Bits       : 115200 8N1
F - Hardware Flow Control : Yes
G - Software Flow Control : No

   Change which setting?
```

Access Bootloader



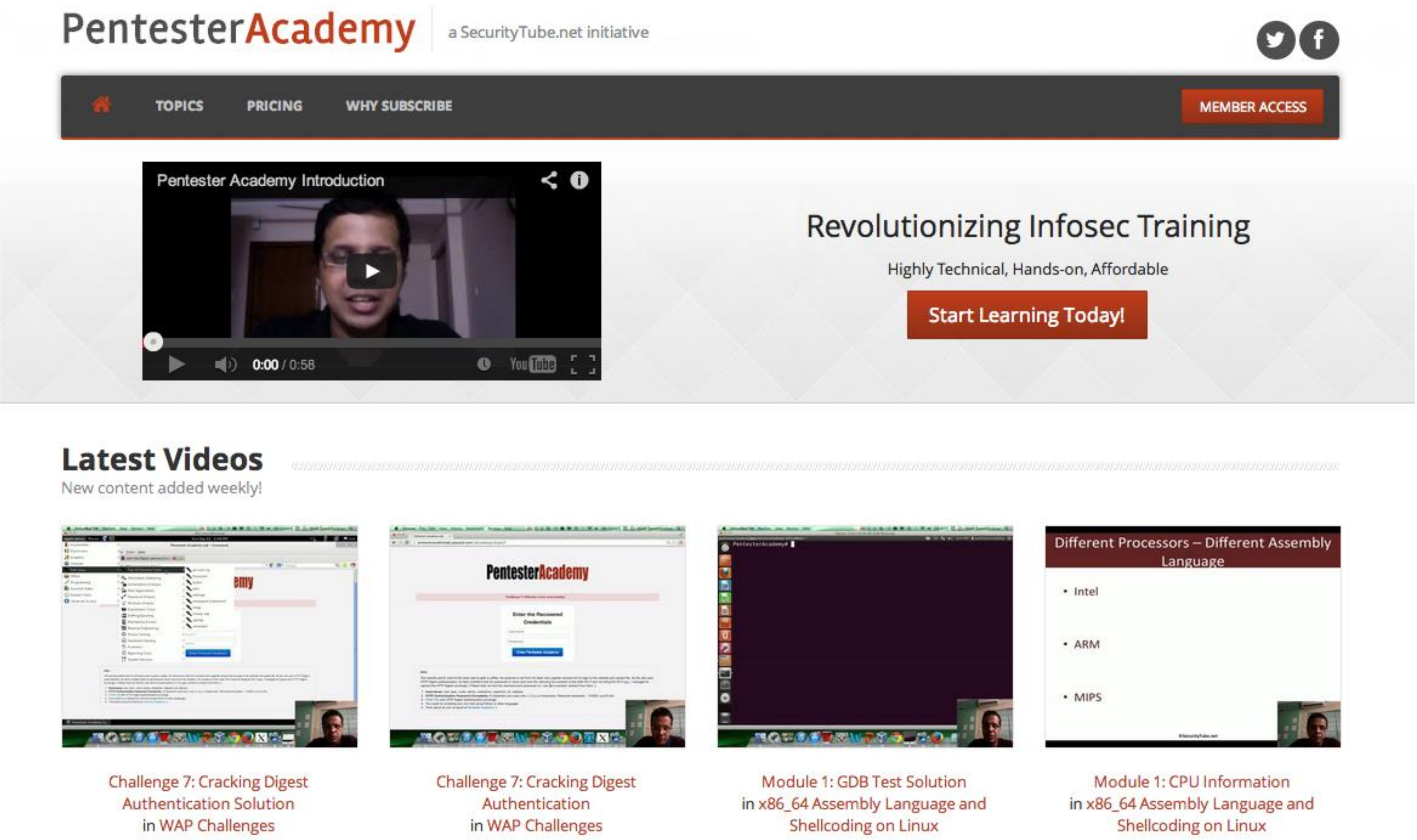
```
auto update firmware: is_auto_upload_firmware = 0!
Autobooting in 1 seconds
hornet>
hornet> ?
?         - alias for 'help'
bootm     - boot application image from memory
cp        - memory copy
erase     - erase FLASH memory
help      - print online help
md        - memory display
mm        - memory modify (auto-incrementing)
mtest     - simple RAM test
mw        - memory write (fill)
nm        - memory modify (constant address)
printenv- print environment variables
progmac - Set ethernet MAC addresses
reset     - Perform RESET of the CPU
setenv    - set environment variables
tftpboot- boot image via network using TFTP protocol
version - print monitor version
hornet> █
```

Login to Router!



```
 TL-MR3020 mips #1 Tue Jun 10 18:00:13 CST 2014 (none)
TL-MR3020 login: root
Password:
Jan  1 00:09:16 login[152]: root login  on `ttyS0'



BusyBox v1.01 (2014.06.10-10:02+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

# help

Built-in commands:
-------------------
        . : break cd continue eval exec exit export help login newgrp
        read readonly set shift times trap umask wait

#
```

Pentester Academy



Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

New content added weekly!

Different Processors – Different Assembly Language

- Intel
- ARM
- MIPS

Challenge 7: Cracking Digest Authentication Solution
in WAP Challenges

Challenge 7: Cracking Digest Authentication
in WAP Challenges

Module 1: GDB Test Solution
in x86_64 Assembly Language and Shellcoding on Linux

Module 1: CPU Information
in x86_64 Assembly Language and Shellcoding on Linux