

# Lab 3 - Overview

Forensics, Password Cracking,  
Network API Reversing

# Physical Access -> owned

- Access to power switch and all hardware

# Physical Access -> owned

- Access to power switch and all hardware
- Barring some fairly awesome FDE, access to boot loader and `/boot` partition

# Physical Access -> owned

- Access to power switch and all hardware
- Barring some fairly awesome FDE, access to boot loader and `/boot` partition

Lab 3 part 1: Get root

Change the boot process to skip user authentication

# How to root Linux

Normal boot:

1. Boot loader loads the kernel
2. Kernel runs init
3. init runs init scripts to start services and login

# How to root Linux

Normal boot:

1. Boot loader loads the kernel
2. Kernel runs init
3. init runs init scripts to start services and login

To root Ubuntu:

- Tell the kernel where to find init

# How to root Linux

- GRUB

```
Ubuntu 8.10, kernel 2.6.27-7-server
Ubuntu 8.10, kernel 2.6.27-7-server (recovery mode)
Ubuntu 8.10, memtest86+
```

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.

# How to root Linux

- GRUB

```
uuid 089ef2cd-41e2-484a-95fc-959ca39112fa
kernel /boot/vmlinuz-2.6.27-7-server root=UUID=089ef2cd-41e2-484a-95→
initrd /boot/initrd.img-2.6.27-7-server
quiet
```

Use the ↑ and ↓ keys to select which entry is highlighted. Press 'b' to boot, 'e' to edit the selected command in the boot sequence, 'c' for a command-line, 'o' to open a new line after ('O' for before) the selected line, 'd' to remove the selected line, or escape to go back to the main menu.

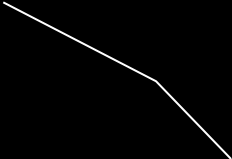


# How to root Linux

- Let's help the kernel find a better init
  - Default is /sbin/init

```
[ Minimal BASH-like line editing is supported.  For
the first word, TAB lists possible command
completions.  Anywhere else TAB lists the possible
completions of a device/filename.  ESC at any time
exits. ]
```

```
<41e2-484a-95fc-959ca39112fa ro init=/sbin/init_
```



Pick something  
more useful

# After root

- To make lasting changes:

```
# mount -o remount,rw /dev/sda1
```

```
...
```

```
# sync
```

# Tips for VM forensics

- Setup host-only network and ssh in
  - (use ssh -X for X applications)
- If you have problems setting up networking

```
# mv /etc/udev/rules.d/70-persistent-net.rules ~/
```

# Tips for wireshark

- Use capture filters



# Tips for wireshark

- Use capture filters



- Use display filters



# Tips for wireshark

- Use capture filters



- Use display filters



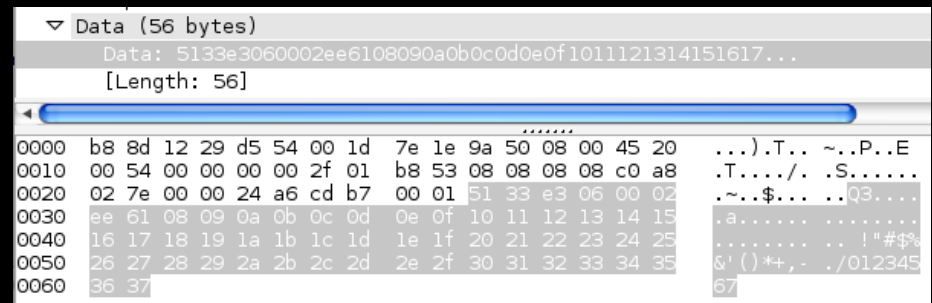
- Select interesting packet bytes and export
  - File -> Export -> Selected Packet Bytes...

- If you use vim, try

- `:%!xxd`

- Otherwise, try

```
$ hexdump -C ./file.bytes
```



# Tips for Lab 3

- Don't assume you know all parts of the protocol
- Watch wireshark to confirm your packets are sending what you want

Happy hacking!