Internet Protocols and Network Security

Damas Makweba, tzNOG4 2016 (adopted from AfNOG 2016 by Chris Wilson)

Questions to get you thinking – For Discussion

- What is an IP address?
- What is a port?
- What is ARP?
- Source and Destination Ports
- Ports used by common services
- What is a firewall?
- What is Wireshark?

Investigations

Install Wireshark on your computer

Download from: https://www.wireshark.org/download.html

Capture some traffic

Start a capture (e.g. 1000 packets), look at the traffic and analyse it.

Look out for:

- Wireless (802.11)
- ARP
- DNS
- UDP (Skype/VPN/unusual)

Investigate the properties of the packets by expanding layers at the bottom.

Investigate a DNS packet. What host is being looked up, by who and why?

What's the source MAC address of your incoming packets? And destination of your outgoing packets? Why?

If you find something interesting/unusual, send a pcap file to the intructor.

Learn how to filter captures

- What filter would you put in the capture box to select HTTP traffic?
- How would you select HTTP traffic in the packet list view (main screen)?

Reading TCP Stream

- Start capturing and then browse a website.
- Right click on an HTTP packet and view TCP stream.
- Look at the HTTP headers: what do they mean?

Drawing Graphs

- Start a capture.
- Set up charting with an unfiltered graph and a filtered one (e.g. http traffic).
- Try downloading something and see what happens.
- What speed do you get? What causes the dips in the transfer rate?

Check for open ports

```
$ sudo apt-get install nmap
```

Find out which hosts are up on our LAN, and the whole of tzNOG4. Try to identify them.

```
$ nmap -sP 10.10.0.0/24
```

Check for open ports:
- On your virtual server
- On your laptop
- On a real server under your control nmap -sS “server-ip”

    Note: Replace “server-ip” with your own system

What do the different states mean? open/closed/filtered

What difference does it make if you stop your firewall?

What can you do with these ports?

Try connecting to one:

- SSH port with `ssh`
- HTTP port with `fetch`
- DNS port with `dig`

What log messages do you get when someone hits these services?

Do you see other such records?