Capturing and processing packets with tcpdump and Wireshark

CS-335a Tutorial

Manolis Surligas
surligas@csd.uoc.gr

29 November, 2011

Get the software

- Tcpdump can be downloaded from http://www.tcpdump.org/ for both Windows and Linux
- Most Linux distributions include tcpdump in their standard packages so you do not need to compile it from the source.
  Just type as **root**:
  - apt-get install tcpdump (Debian based distributions like Ubuntu)
  - zypper install tcpdump (openSuse)
  - yum install tcpdump (Fedora)

Get the software

- Wireshark is a graphical tool for capturing and analyzing easily packets.
- Can be downloaded for Windows from http://www.wireshark.org/
- Most Linux distros have it on their standard package, so just type as **root**:
  - apt-get install wireshark (Debian based distros)
  - zypper install wireshark (openSuse)
  - yum install wireshark (Fedora)

Linux? Oh noooo...

- It is highly recommended to to your projects and your capture on Linux machines
- You can avoid several Windows restrictions
- Powerful command line
- More capabilities with your network interfaces
- If you haven't a Linux OS installed, you can use a Linux Live DVD
- Use BackTrack (comes with most tools pre-installed)

Start capturing packets

- Although Wireshark has the ability to capture packets, it consumes lot of memory
- Better to capture packets with tcpdump, split the trace file in smaller files
- Then analyze easily one by one the smaller files

With this way we avoid:

- System and memory overload
- Save time from waiting Wireshark to proccess large files

Start capturing packets

- In a console run:

```
tcpdump -i eth0 -s 0 -w filename.pcap
```

- -i: Specifies the name of the interface in which tcpdump will start capturing packets
  - To list all your available interfaces run:

    ```
    ifconfig -a
    ```

- -w: Give the name of the file in which the packets should be saved. Should end with .pcap extension
- When you are finished press Ctrl+C to stop
- Some systems may need to run these commands as root

Spitting the trace file into smaller

- As we said before it is a good practice to split large traces into smaller.
- To do that run:

```
tcpdump -r old_file -w new_file -C file_size
```

  - file_size unit is 1.000.000 bytes (e.g. -C 10 will split the trace file in files with size 10.000.000 bytes)
  - The files that are created have names new_file1, new_file2 e.t.c
- Do that if you trace file has size larger than the 1/4 of your physical memory

Analyzing with Wireshark

- Open Wireshark
- Go File->Open... and select on of your trace files
- You can see the packets that you captured
- If you click on one of them, you can see below more info about it, like its Tranfer Protocol or even if the data that contains!!!

Apply filters

- You can apply several filters, in order to categorize your captured packets
- In the *Filter* field type for example *tcp* and click apply.
- These should list all the TCP packets of your trace
- Some other filters keywords are: http, arp, udp e.t.c
- You can also specify and combinations (e.g *http and arp, tcp and not arp,* e.t.c)

More info

- This was the begging. You should experiment a lot by your own
- man tcpdump
- Tcpdump online documentation http://www.tcpdump.org/#documentation
- Many resources on the web
- Use the mailing-list (hy335a-list@csd.uoc.gr) for questions