TCPDUMP/WINDUMP

Introduction

Tcpdump is a linux command that shows traffic (contents of packets) on a particular interface. It has the following format:

```
tcpdump [ -AdDeflLnNOpqRStuUvxX ] [ -c count ] [ -C file_size ] [ -F
file ]  [ -i interface ] [ -m module ] [ -M secret ]  [ -r file ] [ -s
snaplen ] [ -T type ] [ -w file ]  [ -W filecount ] [ -E spi@ipaddr
algo:secret,... ] [ -y datalinktype ] [ -Z user ] [ expression ]
```

Depending on the given boolean *expression*, the content to be displayed can be filtered. WinDump is tcpdump alternative command for windows. It is totally compatible with tcpdump.

For this lab, read the tcpdump/winDump manual from https://www.winpcap.org/windump/ and do the following:

1) Write a filter to capture all the traffic with host 192.168.1.1 as destination or source.
2) Write a filter to capture all the incoming or outgoing traffic on TCP port 53.
3) Write a filter to capture all the incoming or outgoing traffic on port 53.
4) Write a filter to capture all the traffic coming for 192.168.1.1/16 except 192.168.1.100.
5) Write a filter to capture all the traffic coming on ports 10 to 100 except port 80.
6) Write a filter to capture all the traffic with source address or destination address 192.168.1.1 on port 53.
7) Write a filter to capture all the traffic with source address 192.168.1.2 or 192.168.1.3 and source port 21 or 20.
8) Write a filter to capture and store all the traffic in a file log.txt coming from 192.168.1.1, 192.168.1.3 or 192.168.1.2 with source port 20 or 21 and destination port 12345 or 12346.
9) Write a filter to capture first 50 packets in numeric format (both port and IP) including Ethernet header and verbosity level 2 and any source host from 192.168.1.96 to 192.168.1.120.
10) Write a filter to capture all the UDP traffic coming from google on port 19191 and write it to a file log.txt.