# NASA Lab 2: Network Admin Tools

2018 NASA Training - Week3

bookgin

# Bandwidth Measurement: iPerf

*iPerf is a tool for active measurements of the maximum achievable bandwidth on IP networks.*

For convenience, we'll use precompiled cross-platform version.

# Introduction

- iPerf client + iPerf server
- The server side listens on a TCP/UDP port
- The client side connects to the server

# Installation

- In any 2 different CSIE workstations, install iPerf.
- Download iPerf3 Linux manual installation 64 bits
- Manually specify library path by set the environment variable LD_LIBRARY_PATH

```
LD_LIBRARY_PATH=`pwd` ./iperf3
```

# Getting Started

## Server

```
# Listen on all interface on port 9453
./iperf -s -p 9453
```

## Client

```
# Connect to remote on port 9453
./iperf -c SERVER_HOSTNAME -p 9453
```

# Exercise 1:

Measure the bandwidth between your PC/204/workstations and CSIE workstations under wire/wireless environment.

- 204 - 204, wired
- 204 - workstation, wired
- PC - workstation, wireless

# Bottleneck ?

- CPU
- Network interface
- Link capacity
- Switching capacity

# Network Packet Analyzer: Wireshark, tcpdump

*Wireshark is the world's foremost and widely-used network protocol analyzer.*

*tcpdump - dump traffic on a network.*

Wireshark is a GUI tool, while tcpdump is a CLI tool.

# Plaintext vs. Ciphertext

In hw1, we know the importance of HTTPS. Here are some protocols in plain text:

- HTTP -> HTTPS
- telnet -> ssh
- ftp, tftp -> sftp (FTP over SSH) and ftps (FTP over TLS)
- DNS

# Are they encrypted?

- Server IP address
- Server port
- GET parameter
- POST parameters
- hostname
- HTTP cookies

# Wireshark...

Analyze the HTTPS captured packets csie.pcap

# Server Name Indication

*Server Name Indication (SNI) is an extension to the TLS computer networking protocol by which a client indicates which hostname it is attempting to connect to at the start of the handshaking process.*

- Wikipedia
- Efficiently bypassing SNI-based HTTPS filtering

# Exercise 2: Let's Decrypt

Suppose the server is compromised, and you get the server's private key. How to decrypt the TLS traffic?

# More fun: DNS/ICMP tunnel

- https://github.com/yarrick/iodine
- https://github.com/DhavalKapil/icmptunnel