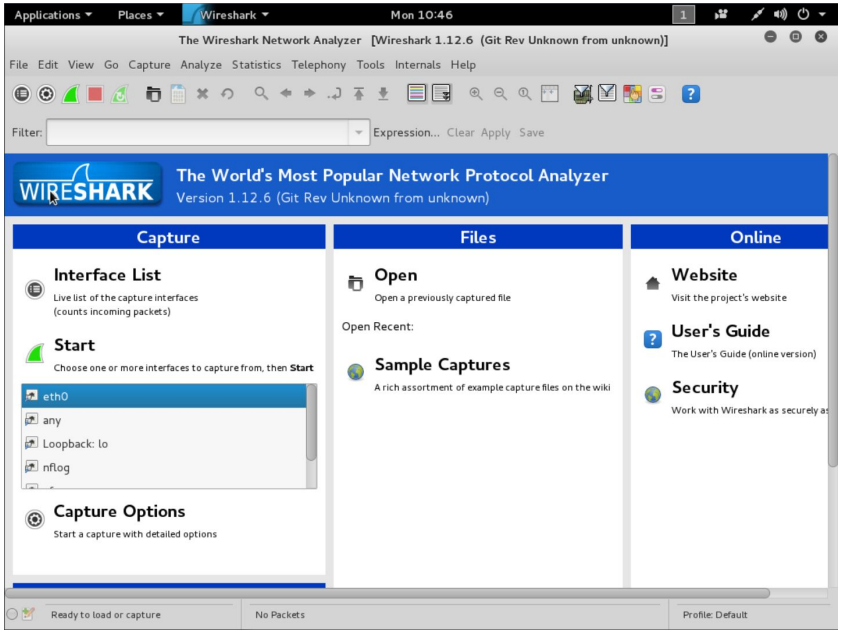
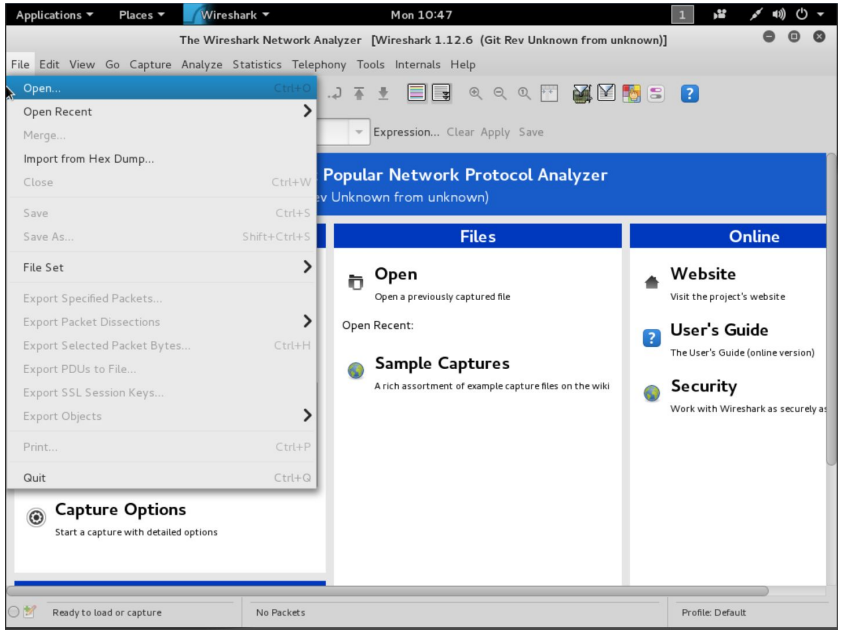
Project 3 Introduction

- Part 1: Network traces (1-2 hours)
- Part 2: Anomaly Detection (1-3 hours)
- Part 3: Penetration Testing (2-4 hours, save time for this one)

Part 1: Exploring Network Traces

You will need to use Wireshark to open and analyze the packet trace.





Part 1: Exploring Network Traces (continued)

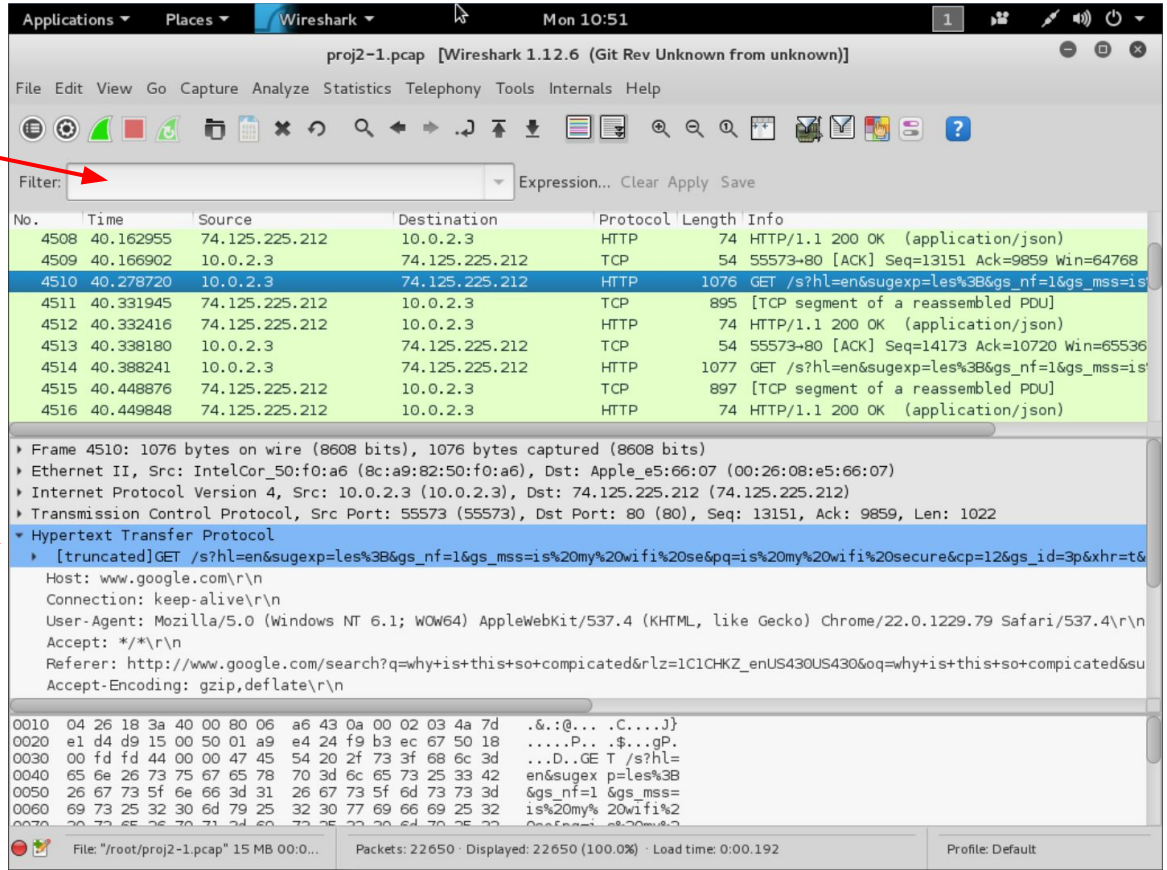
Can filter packets by

- protocol (http, tls, etc.)
- ip address

Packet List

Protocol Breakdown

Bytes



Part 2: Anomaly Detection

- SYN, SYN+ACK packets
  - SYN is the client-side initial handshake
  - SYN+ACK is server-side acknowledgement of the handshake

- Port scanning
  - Attackers may send SYN packets to identify active network hosts listening to a specified port
  - You will need to find sources sending more SYN packets than receiving SYN+ACK packets

- nmap (this command will be useful for Part 3)
  - Very (most?) popular network scanner (sudo apt-get install nmap)
  - Command “nmap 192.168.0.0/24” will scan top 1000 most-used ports on your local network
  - Be CAREFUL! Port scanning sends traffic out on the network that may interfere with other processes. Don’t port scan on networks you don’t own or have authorization for.

Part 3: Penetration Test

What's a penetration test?

- A fun project where you get paid to hack someone!
- A formal agreement between you and a company defining the scope of work to be performed, the rules of engagement to be followed, and giving you official authorization to begin.

Why is it important to have a Pen-test Pre-Agreement?

- To protect yourself!
- It gives you explicit authorization to conduct the pen test. Without it, you are subject to criminal penalties.

Part 3: Penetration Test (continued)

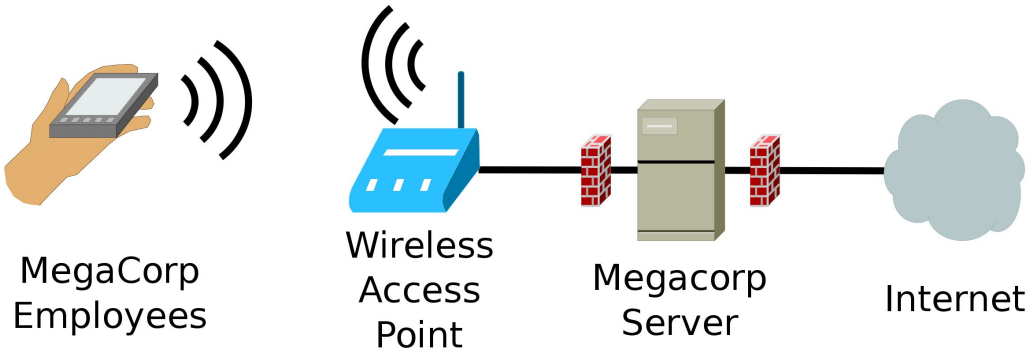
You must read and agree to the Pen-Test Pre-Agreement!

Make sure you send us the proper email accepting the conditions of the Pen-Test ***before*** you begin.

(Both partners must email us.)

Pen Test: What are you trying to do?

- MegaCorp needs its systems tested to determine if they're vulnerable.
- MegaCorp recently set up a wireless network in BBB for its employees to use.
  - This would be a good starting place to see if there are any vulnerabilities.
- MegaCorp also has a server that uses Kerberos passwords to log on.
- Intentionally, this project is left somewhat open-ended.
  - You never know what you're going to find on a PenTest.



Pen Test: What are you trying to do? (continued)

- You are looking for at least three notable findings.
  - Hostnames of any machines you gain access to.
  - Encryption keys for networks you gain access to.
  - Username/Passwords you are able to obtain (not including your own).

- Rules of Engagement
  - Spelled out in detail in the project document.
  - They are *really* important. Make sure you stay within the allowed scope of the Pen Test.
  - If you have any questions, please ask us before you try something that isn't specifically allowed.

Pen Test: Getting set up

You will need a variety of hacking tools for this project. The easiest way to get set up is to use Kali Linux, widely known as the Pen-Testing Linux Distro.

Install VirtualBox: https://www.virtualbox.org/wiki/Downloads
On Linux, use your package manager (sudo apt-get install virtualbox)
Make sure to download and install the Extension Pack! (even Linux!)

Download the Kali Virtualbox image:
https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

Import the image into VirtualBox. Start up your new virtual machine.
The default username and password is “root” / “toor”

Pen Test: Wireless Networks

- Unlike wired networks, wireless packets are *broadcast*
- Only one device can talk at a time
- Devices use different “channels” (slightly different frequencies) to talk at the same time
- Encryption
  - No security
    - Lets you right in
  - WEP
    - Can be mathematically cracked in seconds
  - WPA (WPA2 is essentially the same, just uses AES instead of TKIP)
    - Current generation of personal wireless encryption. Can’t easily be mathematically broken.
    - But, you can capture the 4-way handshake and guess passwords until it decrypts.

Pen Test: Wireless attacks (borrow one of our adapters!)

- Aircrack-ng suite
  - Set of tools for breaking into wireless networks.
  - http://www.aircrack-ng.org/doku.php?id=cracking_wpa (Start at part 2)
  - http://lewiscomputerhowto.blogspot.com/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html
  - “airmon-ng check kill” -- Kill all networking processes that may interfere with wireless attacks
  - airodump-ng
    - Sets up your wireless interface to capture packets (like wireshark or tcpdump)
  - aireplay-ng
    - Inject packets into the wireless network
    - Specifically, for a WPA attack, you will want to send the client and base station a “deauth” packet to force the client off the network. It should reconnect automatically.
  - aircrack-ng
    - Read through captured wireless packets and crack any passwords you find.
    - For WPA attacks, it will require a wordlist. If you know the format of the password, you can create a wordlist yourself.

Pen Test: Capturing network traffic without Wireshark

Use tcpdump! (It's actually easier/faster for small stuff)

tcpdump -i eth1

- Capture network traffic on interface *eth1*

tcpdump -nni eth1

- Capture network traffic without resolving domain names or ports (faster!)

tcpdump -nni eth1 -w capturefile.pcap

- Capture network traffic and write the raw packets to file capturefile.pcap

tcpdump -Anni eth1 -w capturefile.pcap

- Capture traffic and write out all printable characters in packets to terminal

tcpdump -Anni eth1 -w capturefile.pcap tcp port 22

- Capture only traffic using TCP protocol and on port 22 (SSH)