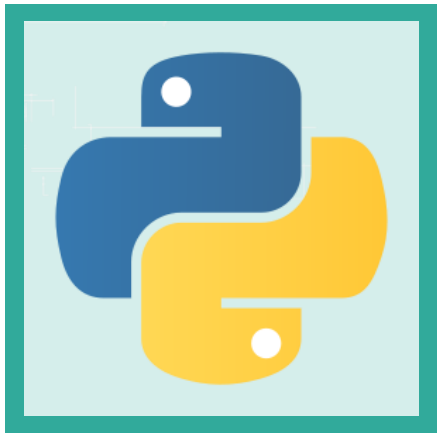
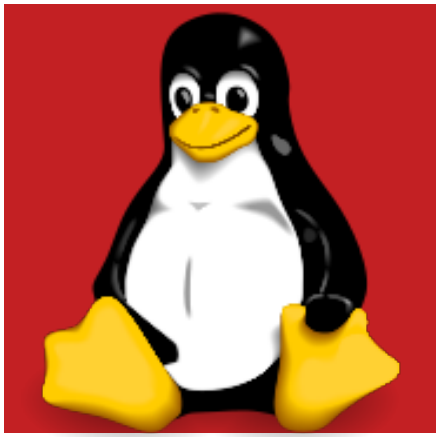




Cyber Security

CS301 – Fundamentals of Computer Science
United States Military Academy

An Exercise in Cyber Security

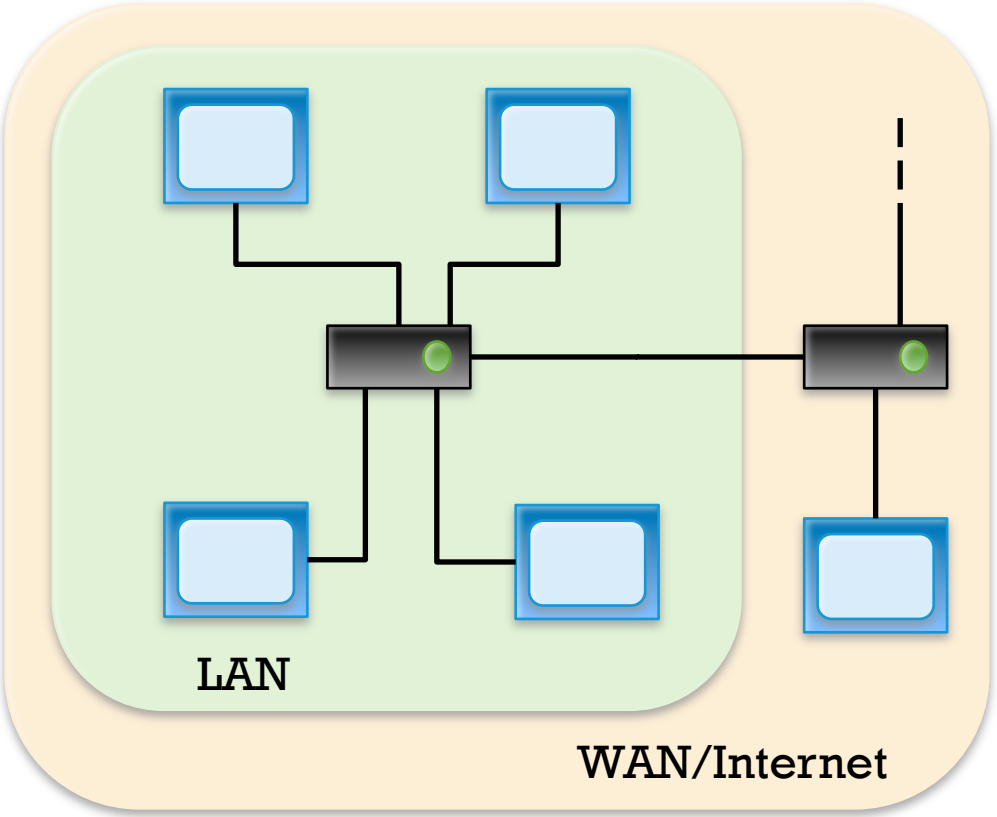
- Your identity is a valuable thing that is worth stealing.
- Previous courses: how to protect yourself
- This lab: how your information can get stolen.
- Today, you will be learning how to use Python to inspect packets streaming wirelessly over a network.
- You will use your Python skills to steal identity-related information of some individuals in a hypothetical situation.

Credits:

- This lab would not be possible without LTC David Raymond, CDX Leader and Head Coach.
- Be sure to thank him if you see him!

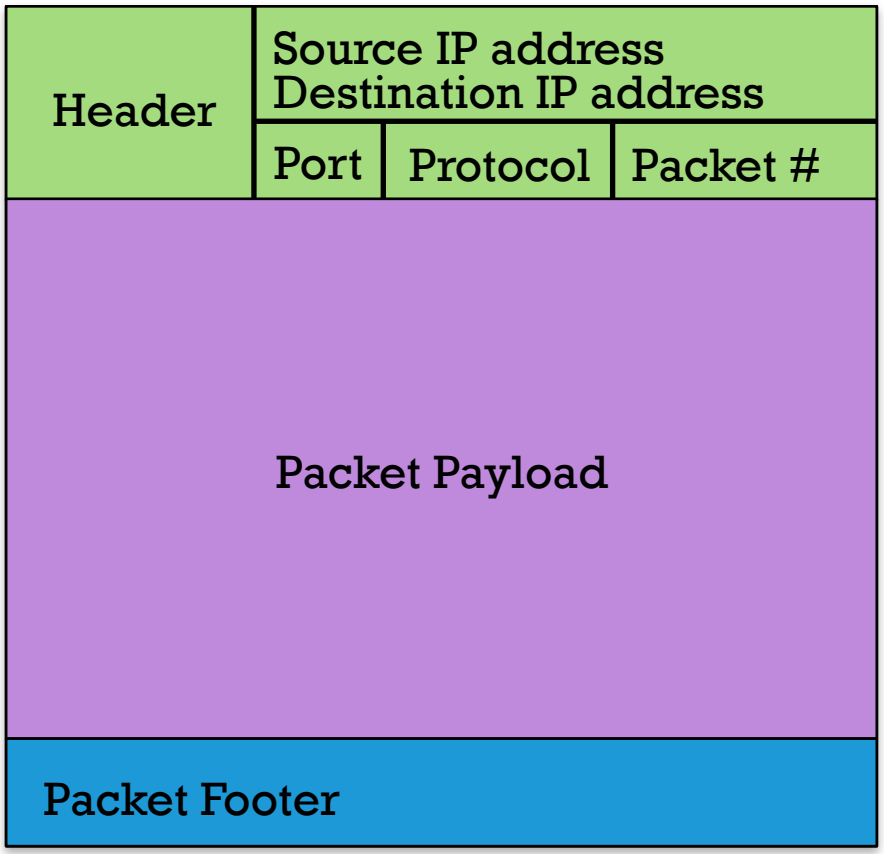
Preliminaries: Networks

- A network enables information to pass between multiple computers.
- Each computer is referenced by an address: the IP address.
- Computers are networked together and communicate through the use of routers.
- Internet: set of all visible routers.



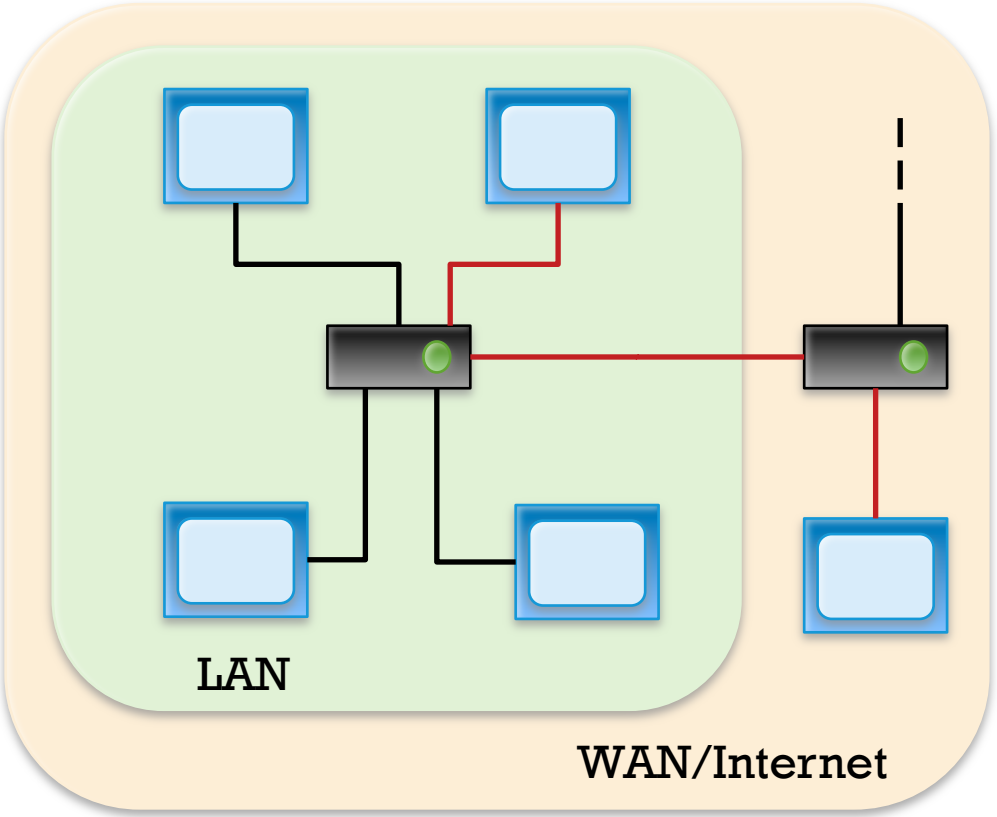
Information Sharing

- Computers communicate across the network by sending and receiving tiny units of information called packets.
- Each packet contains:
  - Header (directions)
  - Payload (info being transmitted)
  - Footer (error checking)
- For certain networks, packets may also store their length in the header. For others, each packet is of fixed length.



Information Sharing

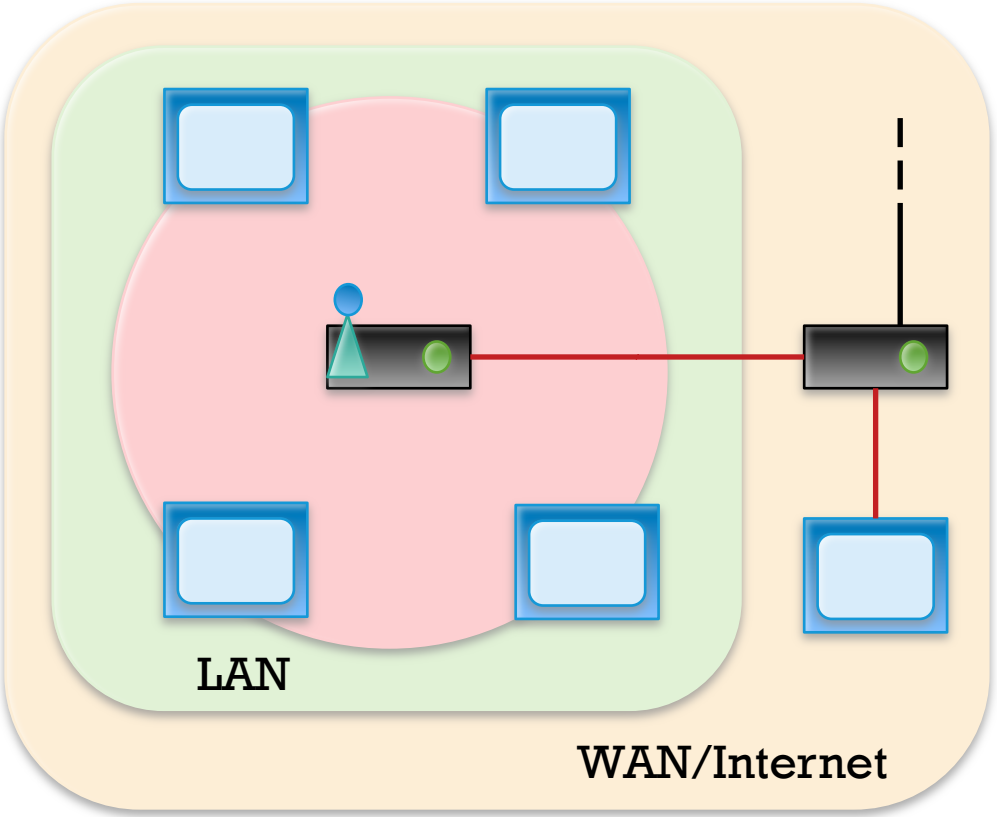
- Routers forward packets to their intended destination.
- In the unicast model (used for most wired network connect), packets are sent from one computer to another via routers.
- A router looks at a packet's header to determine where it should go.



unicast model

Wireless Information Sharing

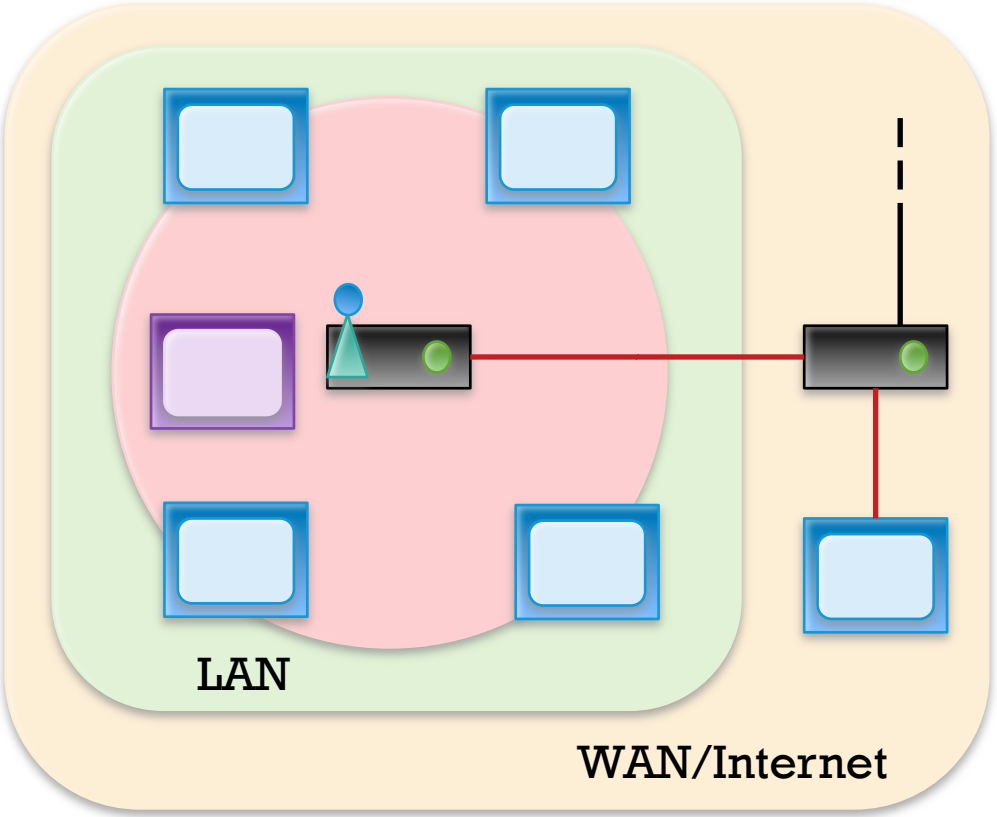
- In a wireless network, packets are transmitted to and from the router through the air.
- Packets that are received by computers that are not the intended recipient are ignored.
- Or, that's how it's supposed to work…



Multicast model

Packet Sniffing on a Wireless Network

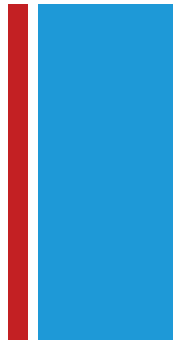
- A malicious user on the network can employ a piece of software called a packet sniffer.
- A packet sniffer allows our malicious user to collect and eavesdrop on packets being transmitted over the network.
- This enables our malicious user to steal identity related information.
- Practice is common on unsecured wireless networks.



Is packet sniffing legal on unencrypted wireless networks?

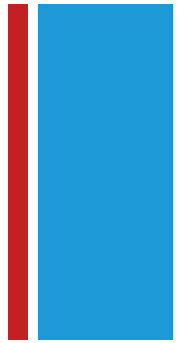
- US Wiretap law makes it illegal to intercept or procure wire, oral or electronic communication.
- HOWEVER, it is legal to collect information radio communication or any electronic communication through a system that is configured as to be readily accessible to general public.
- Court cases:
  - No! San Franciso vs Google, 2011: A judge ruled that the packet sniffer used by Google Street View vehicles can be considered wiretapping.
  - Yes! Innovation IP Ventures vs Everyone, 2012: A judge ruled that communications sent over an unencrypted wireless network as being readily accessible to the public.
- Still a gray area, so don't do it. This lab is meant for educational purposes only!

More about packet sniffers



- Wireshark – open source cross platform software
- tcpdump – linux utility
- Firesheep – Firefox extension
- Packet sniffers can store captured packets in PCAP (Packet CAPture) files.
- Today's lab: analyze packets using python!
- Go to lab website, and download:
  - cyber_lab.pcap
  - sample.py

Scapy



- Scapy is a utility for allowing people to manipulate packets on networks.
- They have a python module which you can use to create, decode, send and capture packets over a network.
- The file lab3.py illustrates how Scapy can be used to read and decode PCAP files.
- This is all the code we will give you. The rest is up to you!

Lab Today: Exploits at a Coffee Shop

- You and your trusty Linux machine are hanging out at a coffee shop which has free wireless internet. You connect to the network and use tcpdump to capture the packets being transmitted over the network (stored in cyber_lab.pcap).
- Your task: Use your Python knowledge to
  - Identify the number of machines (and their IP addresses!) in use on the wireless network.
  - Find out the identities of the people who are using the machines on the network, along with their activities:
    - Names, e-mail addresses
    - Usernames, passwords (if any)
    - Activities: Websites visited, e-mails sent (if any), guesses at occupations.
- Place the completed lab in a folder called lab3 in your turn-in folder.

A Starting Strategy

- You are in a local area network. The computers that transmit and send the most packets are likely the machines on the network.
- IP addresses on the same local network share the same subnet, and thus share a common network address. That is the first three bytes (XXX.XXX.XXX) in an IP address! They are identified uniquely by their host number (last byte).
- Your IP address is: 10.3.0.15 (note that your IP may not be in the packet capture)
- Write to a file a list of all the IP addresses in your local network! Save the IP addresses to the file: `coffeeshop.txt`

A Starting Strategy

- Step 2: Now, using the file that you created, create individual files holding the packets specific to each person.
- Step 3: Steal as much personal info from each person's set of packets! Create a keyword search that allows you to search for particular keywords in each file. Some good keywords to search on:
  - HTTP (port 80) - used in most website requests
    - Associated header tags: GET/POST
  - SMTP/IMAP (port 25, 143) - e-mail
    - Associated header tags: MAIL, SMTP
  - See /etc/services for a full list of services and their associated ports.

Discussion: Lessons Learned

- Does this mean you should stop using unencrypted wireless networks?
- What is the best way of making sure the packets you receive or transmit don't get stolen?
- What are the challenges at
  - For users?
  - For companies that maintain websites?
  - At a national level?