tcpdump

By Han Zhang and Raymond Yeung

What is a packet?

- Small amount of data sent over a network (ie. internet or LAN)
- Usually consists of two sections: Header and Payload
  - Header - Information about the packet
    - Always includes source and destination
    - Other information depends on the type of header
  - Payload - the actual data being transferred
    - Often just a small part of a file/webpage.

What is Packet Sniffing and What Information can be obtained from it

- Packet Sniffing - reading and logging traffic over a network
  - A common use is for a network administrator to use collected data for monitoring bandwidth and traffic.
  - This can also be abused by hackers to steal private data
- Can be used to acquire:
  - Network consumption trends for optimization
  - Login information
  - Websites visited
- Often software based, but hardware packet sniffers also occasionally used

Network Protocols

- A set of rules for routing and addressing packets of data so they arrive at their destination accordingly.
- Three main types of network protocols:
    - Communication Protocols
    - Management Protocols
    - Security Protocols

Network Communication Protocols

Formats and rules by which data is transmitted over the internet

- HTTP - allows browser and server to communicate
- TCP - separates data into packets that can be sent over a network (used by switches and routers)
- UDP - Similar to TCP, but TCP ensures that a connection is made between app and server, while UDP doesn't. (UDP is simpler than TCP making it faster and more efficient)
- IRC - text-based communication protocol. Software client used to communicate with servers and send message to other clients. (Not as widely used anymore, think Slack/Discord)

Network Management Protocol

Processes and rules for managing, monitoring, and maintaining a computer network.

Usually used by network managers for maintaining the system.

- SNMP - *Simple Network Management Protocol*, TCP-based protocol which allows administrators to collect and send data.
- ICMP - *Internet Control Method Protocol*, diagnostic tool which allows devices on a network to send error messages and provide information about connectivity issues.

Network Security Protocols

Used to ensure that data over a network is safe and secure

Usually relies on cryptography and encryption to secure data

- SSL - *Secure Socket Layer*, protocol used for securing internet connections and protecting data. Allows Server/Client communication and Server/Server communication.
- SFTP - *Secure File Transfer Protocol*, used to securely transfer files over a network
- HTTPS - Secure HTTP, encrypts data sent between browser and server

What is Tcpdump and How it works

- Command line network capture and protocol analysis tool
- Despite the name, tcpdump, it can be used to identify non-TCP packets.
- Native to Linux and usually installed by default on Linux/Unix systems.
- Wireshark is a popular tool that does the same thing that tcpdump does with few differences.
  - Wireshark is GUI based, while tcpdump is command line based
  - This means you can ssh into a machine and use tcpdump
- tcpdump puts your firewall at risk because it exposes IPSO to packets that would otherwise be blocked. It is recommended that tcpdump is only ran for a short amount of time.
- Like any unix command line tool, the manual can be found using man.

How to use tcpdump and flags associated with it.

- Tcpdump requires sudo access
- -D to see which interfaces you can capture packets from
- -w to write output to a file
- -r *file* to read packets from a pcap file
- -nn will make sure the output displays hostnames as numeric IP addresses (the first n) and the ports as port numbers (the second n).
- -port # tells tcpdump to only capture traffic to and from that port.
- src *ip address* -finds traffic from only src
- dst *ip address* -finds traffic from only dst
- You can filter out results from tcpdump by reading the pcap file and then writing the outputs with a filter.
  - ex. -r *file* -w output.pcap host *ip* (would filter by the ip)