

Network Sniffers

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 9 November 21th, 2005

Link Layer

- Not really part of the Internet protocol suite
- The method used to pass packets from the Internet layer of one device to the Internet layer of another
- Can be controlled both in the software device driver for the network card, as well as on firmware or specialist chipsets
- These perform data link functions such as adding a packet header to prepare it for transmission, then actually transmit the frame over a physical medium
- On receiving end, the link layer gets data frames, strip off the packet headers, and hand the received packets to the Internet layer

- Includes OSI physical layer (physical cabling or other media used to create the network) and data link layer (where data is first encoded to travel over some specific medium)

Network Sniffers

- Listens or "sniffs" packets on a specified physical network segment
- Allows you to analyze the traffic for patterns, troubleshoot specific problems, and spot suspicious behavior.
- Sniffers are generally specific to the type of network they work on — you must have an Ethernet sniffer to analyze traffic on an Ethernet LAN.
- Commercial sniffers usually are dedicated and expensive hardware devices
- We will focus on Ethernet sniffers since it is mostly widely deployed data link protocol for LANs (now a de facto standard)

History of Ethernet

- Bob Metcalfe invented and patented Ethernet in 1973 while at the Xerox Palo Alto Research Center (PARC)
- Went on to form a company dedicated to building equipment for this new protocol (3Com)
- Ethernet was released into the public domain so other companies could build to the specification.
- This was not true of Token Ring and most of the other network protocols of the day
- Eventually adopted as an official standard by the International Electrical and Electronic Engineers (IEEE) and a de facto industry standard

What is Ethernet?

- Ethernet handles both the physical media control and the software encoding for data going onto a network.
- Since Ethernet is a broadcast topology, where every computer can potentially "talk" at once, it has a mechanism to handle collisions
- If a collision is detected, both sides retransmit the data after a random delay.

MAC Addresses

- Ethernet networks use an addressing scheme called Medium Access Control (MAC) addresses.
- IEEE handles numbering — old standard 48 bits, new standard 64 bits
- They are 12-digit hexadecimal numbers, and are assigned to the card at the factory.
- Every manufacturer has its own range of numbers — first 3 octets of the MAC address.

Changing MAC addresses

- While physical MAC addresses are permanent by design, mechanisms allow modification, or "spoofing" of the MAC address that is reported by the operating system.
- Can be useful for privacy reasons, for instance when connecting to a Wi-Fi hotspot, or to ensure interoperability.
- Some internet service providers bind their service to a specific MAC address; if the user then changes their network card or intends to install a router, the service won't work anymore.
- Changing the MAC address of the new interface will solve the problem. Similarly, some software licenses are bound to a specific MAC address.
- Changing the MAC address is not permanent: after a reboot, it will revert to the MAC address physically stored in the card.

- macchanger and other tools

Ethernet and Security

- All computers attached to an Ethernet network are broadcasting on the same physical wire
- An Ethernet card on the network sees all the traffic passing it.
- The Ethernet card is designed to process only packets addressed to it but still sees and processes everything
- Nowadays, most Ethernet networks are switched to improve efficiency.
- This means that instead of each Ethernet port seeing all the traffic, it sees only traffic intended for the machine plugged into it.
- This helps alleviate some of the privacy and congestion issues, but plenty of broadcast traffic still goes to every port.

Broadcast Traffic

- Broadcast traffic is sent out to every port on the network usually for discovery or informational purposes.
- DHCP, where the machine sends out a broadcast looking for any DHCP servers on the network to get an address from.
- Machines running Microsoft Windows are also notorious for putting a lot of broadcast traffic on the LAN.
- Address Resolution Protocol (ARP); this is when a machine first tries to figure out which MAC address relates to which IP address
- Send out ARP packets asking, "Who has this IP address?" Using reply, it then sends the rest of the communication to the proper MAC address.

- If crackers get access to the switch, they can sometimes turn their own ports into a "monitor" or "mirror" port that shows traffic from other ports.

Always Get Permission

- By capturing every transmission on the wire, you are very likely to see passwords for various systems, contents of e-mails, and other sensitive data
- In the wrong hands, could obviously lead to serious security breaches.
- In addition, it could be a violation of your employees' privacy, depending on company and government policies.
- Always get written permission from a supervisor, and preferably upper management, before you start this kind of activity.
- Generally, network-sniffing logs should be purged from your system

- There are documented cases of well-intentioned system administrators being fired for capturing data without permission.

Understand Your Network Topology

- Make sure you fully understand the physical and logical layout of your network before setting up your sniffer.
- Sniffing from the wrong place on the network will cause you either to not see what you are looking for or to get erroneous results.
- Make sure there is not a router between your sniffing workstation and what you are trying to observe.
- On a switched network, configure the port you are plugged into to be a "monitor" or "mirror" port (need the port to act like a hub so it sees all the traffic on that switch)
- Without this setting, all monitor port sees is the traffic addressed to the specific plugged into and the network's broadcast traffic.

Use Tight Search Criteria

- Using an open filter (that is, seeing everything) will make the output data voluminous and hard to analyze.
- Use specific search criteria to narrow down the output that your sniffer shows.
- Filter even if you are not exactly sure what you are looking for,

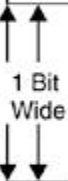
Establish a Baseline for Your Network

- Use your sniffer to analyze your network during normal operation and record the summary results
- This serves as a baseline to compare it to when you are trying to isolate a problem.
- Monitor and record network traffic over time
- Ethereal sniffer creates several nice reports for this.

TCP Header Diagram

TCP Header

| | | | | | | | | | | | | | | | | | | | |
|------------------------|--|--|--|--|----------|--|--|--|--|-------------------------|--|--|--|--|-------------|--|--|--|--|
| Source Port Number | | | | | | | | | | Destination Port Number | | | | | | | | | |
| Sequence Number | | | | | | | | | | | | | | | | | | | |
| Acknowledgement Number | | | | | | | | | | | | | | | | | | | |
| Off-Set | | | | | Reserved | | | | | TCP FLAGS | | | | | Window Size | | | | |
| TCP Checksum | | | | | | | | | | Urgent Pointer | | | | | | | | | |
| TCP Options | | | | | | | | | | | | | | | | | | | |
| DATA | | | | | | | | | | | | | | | | | | | |



IP Header

| | | | | | | | | | | | | | | | | | | | |
|------------------------------|--|--|--|--|---------------|--|--|--|--|-----------------------|--|--|--|--|--------------|--|--|--|--|
| IP Version | | | | | Header Length | | | | | Type Of Service (TOS) | | | | | Total Length | | | | |
| Identification (Fragment ID) | | | | | | | | | | Fragment Offset | | | | | | | | | |
| Time to Live (TTL) | | | | | Protocol | | | | | Header Checksum | | | | | | | | | |
| Source IP Address | | | | | | | | | | | | | | | | | | | |
| Destination IP Address | | | | | | | | | | | | | | | | | | | |
| Options | | | | | | | | | | | | | | | | | | | |
| DATA | | | | | | | | | | | | | | | | | | | |

TCP/IP Packet Headers

- The layout of the TCP/IP packet is specified in RFC 793 for the TCP portion and RFC 791 for the IP portion.
- Both header types are at least 20 bytes long and are usually shown in five 32-bit (4-byte) sections with the addresses, options, and other settings for the session

IP Header

- Contains the delivery address for the packet and its sender.
- IP version — 4
- Header Length — usually 20 bytes in IPv4 (may vary in IPv6)
- Type Of Service (TOS) — allows routers and NICs to differentiate the priority of packets (may be used in VoIP)
- Total Length – if subtract header length. get length of data
- Fragment identification — routers may need to break up original datagram
- TTL — number of routers hops packet goes through before it is dropped (decremented by each router)

- Protocol — TCP, UDP, ICMP etc.
- Checksum used to verify header integrity
- Source and destination IP addresses — each address is 32 bits (4 octets of 8 bits each) hence takes up 8 bytes.
- Options field — variable length, padded with zeros or any data (rarely used)

TCP header

- Takes care of establishing a TCP session and higher-level functions — usually 20 bytes long
- Source port number of 16 bits and a destination port number of 16 bits (hence 65,535 ports)
- Sequence number — used to reassemble the packets in the right order at the other end, even if they arrive in a different order.
- Acknowledgment number — based on sequence number
- Data offset gives how many 32-bit lines or "words" are in this header (typically 4) and
- 6 bits that are reserved for future use

- 6-bit section for the TCP Flags (U,A,P,R,S,F)
- Window size — how much data that can be buffered before receiving an ACK
- TCP checksum — used to verify header and data integrity
- Urgent pointer — points to data which should be passed quickly
- TCP options — rarely used and normally padded with zeros
sam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096
<mss 1024>
- The actual payload, the data of the packet, follows