An introduction to Network Analyzers

Dr. Farid Farahmand
9/15/2016
Network Analysis and Sniffing

- Process of capturing, decoding, and analyzing network traffic
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes

- Also known as
  - traffic analysis, protocol analysis, sniffing, packet analysis, eavesdropping*, etc.

*Listen secretly to what is said in private!
Network Analyzer

- A combination of hardware and software tools that can detect, decode, and manipulate traffic on the network
  - Passive monitoring (detection)
    - Difficult to detect
  - Active (attack)

- Available both free and commercially

- Mainly software-based (utilizing OS and NIC)
  - Also known as sniffer
  - A program that monitors the data traveling through the network passively

- Common network analyzers
  - Wireshark / Ethereal
  - Windump
  - Etherpeak
  - Dsniff
  - And much more…

Read: Basic Packet-Sniffer Construction from the Ground Up! by Chad Renfro
Checkout his program: sniff.c
Network Analyzer Components

- **Hardware**
  - Special hardware devices
    - Monitoring voltage fluctuation
    - Jitter (random timing variation)
    - Jabber (failure to handle electrical signals)
    - CRC and Parity Errors
  - NIC Card
- **Capture driver**
  - capturing the data
- **Buffer**
  - memory or disk-based
- **Real-time analysis**
  - analyzing the traffic in real time; detecting any intrusions
- **Decoder**
  - making data readable

Capturing the data is easy! The question is what to do with it!
Who Uses Network Analyzers

- **System administrators**
  - Understand system problems and performance
- **Malicious individuals (intruders)**
  - Capture cleartext data
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMTP, rlogin, HTTP, etc.
    - Capture VoIP data
  - Mapping the target network
  - Traffic pattern discovery
  - Actively break into the network (backdoor techniques)
Basic Operation

- Ethernet traffic is broadcasted to all nodes on the same segment
- Sniffer can capture all the incoming data when the NIC is in *promiscuous* mode:
  - `ifconfig eth0 promisc`
  - `ifconfig eth0 -promisc`
- Default setup is *non-promiscuous* (only receives the data destined for the NIC)
- Remember: a hub receives all the data!
- If switches are used the sniffer must perform **port spanning**
  - Also known as port *mirroring*
  - The traffic to each port is mirrored to the *sniffer*
Port Monitoring
Protecting Against Sniffers

- Spoofing the MAC is often referred to changing the MAC address (in Linux):
  - `ifconfig eth0 down`
  - `ifconfig eth0 hw ether 00:01:02:03:04:05`
  - `ifconfig eth0 up`
  - Register the new MAC address by broadcasting it
    - `ping -c 1 -b 192.168.1.1`

- To detect a sniffer (Linux)
  - Download `Promisc.c`
  - `ifconfig -a` (search for `promisc`)
  - `ip link` (search for `promisc`)

- To detect a sniffer (Windows)
  - Download PromiscDetect

Remember: 00:01:02:03:04:05
MAC address (HWaddr)=
Vender Address + Unique NIC #
Protecting Against Sniffers

- Using switches can help
- Use encryption
  - Making the intercepted data unreadable
  - Note: in many protocols the packet headers are cleartext!
- VPN uses encryption and authorization for secure communications
  - VPN Methods
    - Secure Shell (SSH): headers are not encrypted
    - Secure Sockets Layer (SSL): high network level packet security; headers are not encrypted
    - IPsec: Encrypted headers but does not use TCP or UDP

Remember: Never use unauthorized Sniffers at wok!
What is Wireshark?

- Formerly called **Ethereal**
- An open source program
  - free with many features
- Decodes over 750 protocols
- Compatible with many other sniffers
- Plenty of online resources are available
- Supports command-line and GUI interfaces
  - TSHARK (offers command line interface) has three components
    - Editcap (similar to Save as..to translate the format of captured packets)
    - Mergecap (combine multiple saved captured files)
    - Text2pcap (ASCII Hexdump captures and write the data into a libpcap output file)

**Remember:** You must have a good understanding of the network before you use Sniffers effectively!
Installing Wireshark

- Download the program from
  - www.wireshark.org/download.html

- Capture drivers include (monitor ports and capture all traveling packets)
  - Linux: libpcap
  - Windows: winpcap (www.winpcap.org)

- In Ubuntu
  - Use software Center
    https://www.youtube.com/watch?v=T3-3H9Bs5Nc
  - Or just open a terminal (Ctrl + Alt + T) and type `sudo apt-get install <package name>`.
Installing Wireshark – Command Line

```
mperrin@mperrin-Vostro-400:~$ sudo apt-get install -y wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  wireshark
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 0 B/821 kB of archives.
After this operation, 2,189 kB of additional disk space will be used.
Selecting previously unselected package wireshark.
(Reading database ... 201939 files and directories currently installed.)
Unpacking wireshark (from .../wireshark_1.6.7-1_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for desktop-file-utils ...
Processing triggers for gnome-menus ...
Processing triggers for hicolor-icon-theme ...
Setting up wireshark (1.6.7-1) ...
mperrin@mperrin-Vostro-400:~$ sudo addgroup -quiet -system wireshark
mperrin@mperrin-Vostro-400:~$ sudo chown root:wireshark /usr/bin/dumpcap
mperrin@mperrin-Vostro-400:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
mperrin@mperrin-Vostro-400:~$ sudo usermod -a -G wireshark mperrin
mperrin@mperrin-Vostro-400:~$ 
```
Wireshark Window

- **Menu Bar**
- **Tool Bar**
- **Filter Bar**
- **Info Field**

**Summary Window**

**Protocol Tree Window**

**Data View Window**
Packet number 8 – BGP (Boarder Gateway Prot)

Protocol Tree Window:
Details of the selected packet (#8)

Raw data (content of packet #8)

File: C:\Users\Farid\Documents\Software\wireshark\captures\ch...
Filtering BGP packets only

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>8.004942</td>
<td>192.168.0.15</td>
<td>192.168.0.33</td>
<td>BGP</td>
<td>OPEN Message</td>
</tr>
<tr>
<td>10</td>
<td>8.337997</td>
<td>192.168.0.33</td>
<td>192.168.0.15</td>
<td>BGP</td>
<td>OPEN Message</td>
</tr>
<tr>
<td>12</td>
<td>8.338115</td>
<td>192.168.0.15</td>
<td>192.168.0.15</td>
<td>BGP</td>
<td>KEEPALIVE Message</td>
</tr>
<tr>
<td>13</td>
<td>8.342206</td>
<td>192.168.0.33</td>
<td>192.168.0.15</td>
<td>BGP</td>
<td>KEEPALIVE Message</td>
</tr>
<tr>
<td>16</td>
<td>8.544149</td>
<td>192.168.0.15</td>
<td>192.168.0.33</td>
<td>BGP</td>
<td>KEEPALIVE Message, UPDATE Message, UPDATE Message</td>
</tr>
<tr>
<td>17</td>
<td>8.549476</td>
<td>192.168.0.33</td>
<td>192.168.0.15</td>
<td>BGP</td>
<td>UPDATE Message</td>
</tr>
<tr>
<td>19</td>
<td>8.562733</td>
<td>192.168.0.33</td>
<td>192.168.0.15</td>
<td>BGP</td>
<td>KEEPALIVE Message</td>
</tr>
</tbody>
</table>
We continue in the lab....

- Download the following files and copy them in your HW:
  - bgp_test
  - tcp_stream_analysis
  - follow_tcp_stream
Remember....

- Protocols are standard for communications
- Ethernet is the most popular protocol standard to enable computer communication
  - Based on shared medium and broadcasting
- Ethernet address is called MAC address
  - 48 bit HW address coded in the RON of the NIC card
  - The first 12 bits represent the vendor
  - The second 12 bits represent the serial number
  - Use: `arp -a`
- Remember: IP address is logical addressing
  - Network layer is in charge of routing
  - Use: `ipconfig`

```
C:\Documents and Settings\farid>arp -a
Interface: 130.157.158.211 --- 0x3
  Internet Address     Physical Address     Type
130.157.158.7         00-00-0c-07-ac-00    dynamic
```