Definition: Examining network packets to determine network-level activities and to diagnose errors.
Network Packet Analysis: Overview

- Network Packet Analysis
  - Network Topology
  - Capture Issues
- Wireshark features
- Wireshark capture and filters
- Exercises
Network Packet Analysis: Why packet analysis?

- Network packet analysis is very useful
  - For finding network errors (malformed packets, runts, collisions, significant retransmissions, etc)
  - Analyzing network throughput and load
  - Finding rogue network systems
  - Finding the source of significant network traffic (systems spewing packets, scanning, P2P, etc)
  - Analyzing 802.11 systems for crowded channels, rogue access points, hidden SSIDs
Network Packet Analysis: Understanding TCP/IP

- Network packet analysis requires an understanding of low-level protocols
  - 802.11 (WLAN), 802.3 (Ethernet)
  - IP, TCP, UDP, ICMP, IGMP
  - HTTP, SMTP, SNMP, Telnet, SSH, SMB, etc
Network Packet Analysis: Where to listen

- On network switches, you can see packets to/from your system and broadcast packets
- To see all packets you need to connect to a “mirroring” port on the switch
  - SPAN = Switched Port Analyzer (Cisco)
  - RAP = Roving Analysis Port (3com)
- Transparent bridge mode
  - Require two interfaces and OS support for bridge
  - May require dedicated machine
- Ethernet Hub can be used as well
Network Packet Analysis:
Regular Port
Network Packet Analysis: SPAN Port
Network Packet Analysis: Firewall Port
Network Packet Analysis: Transparent bridge
Network Packet Analysis: Where to wirelessly listen

- On wireless networks, you can see packets on the network you associate with, not other networks.
- You can also enter a wireless monitor mode and listen 802.11 link layer packets:
  - Requires driver and card support
  - WinPcap (Windows) has limited support
  - Most Mac wireless cards work well
Network Packet Analysis: Associated Wireless
Network Packet Analysis: Monitor Mode Wireless
Network Packet Analysis:
Software that interferes

- Some software on your Wireshark system may interfere with packet capture and interface selection
  - Software firewalls and antivirus tools
  - VPN Software
Network Packet Analysis: Performance issues

- Capturing packets can impact performance
- Packets may be dropped from capture file

Solutions:
- Stop other programs that may use CPU
- A faster machine or more efficient interface card
- Use a capture-only tool (tcpdump, dumpcap)
- Optimize software settings
Network Packet Analysis:
Tools Available

- Wireshark
- Network Packet Analyzer CAPSA
  - Javvin Technologies, Inc.
- NetScout Network Packet Analysis
- Fluke Network Analyzers
Network Packet Analysis: Wireshark features

- Works on most platforms (Windows, Mac, Linux, UNIX systems)
- Live capture or offline analysis
- GUI or command-line interface
- VoIP analysis capabilities
- Colorization of packets and types
- Output packet data to various formats
- Capture filters
- Analysis and Statistics tools
Network Packet Analysis: Wireshark capture

- Select “Capture” -> “Interfaces...”
- Determine which interface on which you want to listen and select “Start” or “Options”
Network Packet Analysis: Wireshark capture options

Capture

Interface: en0
IP address: fe80::216:cbff:fed1:4d49, 192.168.1.50
Link-layer header type: Ethernet
Capture packets in promiscuous mode
Capture packets in pcap-ng format (experimental)
Limit each packet to 1 byte

Capture Filter:

Capture File(s)
File: [Browse...]
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)

Stop Capture...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)

Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog

Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution

Help
Cancel
Start
Network Packet Analysis: Wireshark capture filters

- Select the preset capture filter
- Create a new filter
## Network Packet Analysis: Wireshark main window

![Wireshark main window](image)

### Format: 
- **Network Interface**: en1
- **Capture Mode**: Capturing - Wireshark

### Table: Network Packets

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source ADD</th>
<th>Destination ADD</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>571</td>
<td>449.0740429</td>
<td>192.168.1.50</td>
<td>74.125.95.19</td>
<td>TCP</td>
<td>49643 &gt; https [ACK] Seq=12224 Ack=4539 Win=524288 Len=0 TSV=317659249</td>
</tr>
<tr>
<td>573</td>
<td>463.229387</td>
<td>192.168.1.50</td>
<td>74.125.95.19</td>
<td>HTTP</td>
<td>POST /rtm.rtm HTTP/1.1 (application/x-www-form-urlencoded)</td>
</tr>
<tr>
<td>574</td>
<td>463.334332</td>
<td>192.168.1.50</td>
<td>192.168.1.49</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
<tr>
<td>575</td>
<td>463.368631</td>
<td>192.168.1.50</td>
<td>174.17.41.33</td>
<td>TLSv1</td>
<td>8443 &gt; https [ACK] Seq=12224 Ack=4539 Win=524288 Len=0 TSV=317659249</td>
</tr>
<tr>
<td>576</td>
<td>464.123661</td>
<td>192.168.1.36</td>
<td>192.168.1.255</td>
<td>TiVoConn</td>
<td>Discovery Beacon Bedroom (540000178725248)</td>
</tr>
<tr>
<td>577</td>
<td>464.845138</td>
<td>192.168.1.48</td>
<td>192.168.1.255</td>
<td>BROWSER</td>
<td>Local Master Announcement GART, Workstation, Server, Print Queue Serv</td>
</tr>
<tr>
<td>578</td>
<td>464.847763</td>
<td>192.168.1.48</td>
<td>192.168.1.255</td>
<td>BROWSER</td>
<td>Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum</td>
</tr>
<tr>
<td>579</td>
<td>474.875147</td>
<td>74.125.95.19</td>
<td>192.168.1.50</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>580</td>
<td>474.879395</td>
<td>192.168.1.50</td>
<td>74.125.95.19</td>
<td>TCP</td>
<td>49643 &gt; https [ACK] Seq=12224 Ack=4539 Win=524288 Len=0 TSV=317659249</td>
</tr>
<tr>
<td>581</td>
<td>483.901465</td>
<td>192.168.1.50</td>
<td>174.17.41.33</td>
<td>TLSv1</td>
<td>8443 &gt; https [ACK] Seq=12224 Ack=4539 Win=524288 Len=0 TSV=317659249</td>
</tr>
<tr>
<td>583</td>
<td>488.906800</td>
<td>192.168.1.50</td>
<td>74.125.95.19</td>
<td>HTTP</td>
<td>POST /rtm.rtm HTTP/1.1 (application/x-www-form-urlencoded)</td>
</tr>
<tr>
<td>584</td>
<td>488.907624</td>
<td>192.168.1.50</td>
<td>74.125.95.19</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
</tbody>
</table>

### Details:
- **Frame 570**: (66 bytes on wire, 66 bytes captured)
- **Ethernet II**: Src: AppleCom_40:c2:f7 (00:17:2f:40:00:0f) Dst: 0licom_ca:51:e5 (08:00:24:ca:51:e5)
- **Transmission Control Protocol**: Src Port: 49638 (49638), Dst Port: http (80), Seq: 20040, Ack: 11912, Len: 0

### Hexadecimal Representation:
```
0000 00 00 24 ca 51 e5 00 17 f2 40 c2 f7 08 00 45 00 ...
0010 00 34 b8 c3 40 00 04 06 f9 9e c0 a8 01 32 ae 25 ...
0020 45 62 c1 e6 00 50 5c 1d 71 b3 99 f7 f1 ef 80 10 ...
0030 ff ff e9 20 00 00 01 01 08 0a 1e da db 00 64 a2 ...
```

**Interface Status:** en1: <live capture in progress>  Packets: 1812 Displayed: 1812 Marked: 0  Profile: Default
Network Packet Analysis: Filter expression tool

- Filter expression tool can create specific filters based on known protocols.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Relation</th>
<th>Value (unsigned, 2 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP - Transmission Control Prot</td>
<td>is present</td>
<td>80</td>
</tr>
<tr>
<td>tcp.srcport - Source Port</td>
<td>==</td>
<td></td>
</tr>
<tr>
<td>tcp.dstport - Destination Port</td>
<td>!=</td>
<td></td>
</tr>
<tr>
<td>tcp.port - Source or Destination</td>
<td>&gt;</td>
<td></td>
</tr>
<tr>
<td>tcp.stream - Stream index</td>
<td>&lt;</td>
<td></td>
</tr>
<tr>
<td>tcp.seq - Sequence number</td>
<td>&gt;=</td>
<td></td>
</tr>
<tr>
<td>tcp.nxtseq - Next sequence number</td>
<td>&lt;=</td>
<td></td>
</tr>
<tr>
<td>tcp.ack - Acknowledgement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp.hdr_len - Header Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tcp.flags - Flags</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Predefined values:
Network Packet Analysis: Wireshark security issues

- Wireshark has had security issues due to programmer errors
- Captured packets can overflow buffers and lead to denial of service or remote execution of code
- You should always run the latest versions of Wireshark, WinPcap, and libpcap
- Avoid running Wireshark with admin privileges
Network Packet Analysis: Privileges & permissions

- **WinPcap driver must loaded to capture**
  - Loaded at Wireshark start, needs Admin privileges
  - Loaded at boot time
  - Loaded and unloaded manually
  - Wireshark can as user once WinPcap is loaded

- **Mac OS X**
  - ChmodBBF tool will set /dev/bpf read permissions
  - Wireshark can run as user

- **Linux**
  - Must run with root privileges to capture packets
Network Packet Analysis: Wireshark performance

- Wireshark can use a lot of CPU attempting to capture packets
  - Packets may be dropped from the capture file

- Solutions:
  - See previous performance slide
  - Use capture filters that select packets you want
  - Don’t “Update Packets in Real Time”
  - Don’t use read filters (command line option -R)
  - Disable coloring rules
  - Use smaller capture files
  - Disable DNS and Transport Layer lookups
Network Packet Analysis:
Exercise notes:

- The exercise wiki has links to the packet capture files for the exercises
  - [http://192.168.1.10/](http://192.168.1.10/)
  - Go to “Exercises” section and select “Wireshark Exercises”
  - The files are labeled by exercise name
Network Packet Analysis: Exercise 1

- Download “exercise1” and open it in Wireshark
- Determine the activities from the packet data
- Determine the IP addresses of the systems involved
Network Packet Analysis: Exercise 2

- Download “exercise2” and open it in Wireshark
- Determine the activities from the packet data
- What port is open?
  - How did you determine this?
  - What is a short-cut?
Network Packet Analysis: Exercise 2 Additional Info

- The packets from the trace were from this:
  ```
  kaw@klaatu:~$ sudo nmap -sS -PN 192.168.1.10
  [sudo] password for kaw:
  
  Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-07 13:50 EST
  Interesting ports on nikto.interocitry.com (192.168.1.10):
  Not shown: 999 closed ports
  PORT   STATE SERVICE
  22/tcp open  ssh
  MAC Address: 00:B0:D0:DB:9A:69 (Dell Computer)
  
  Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
  ```
Network Packet Analysis: Exercise 3

• Download “exercise3” and open it in Wireshark
• Determine the activities from the packet data
• What’s the username involved?
• What’s the password?
• What’s the secret?
Network Packet Analysis: Exercise 4

- Download “exercise4” and open it in Wireshark
- Determine the activities from the packet data
- What web browser was used?
- What web server was used?
- What’s the URL that was accessed?
- Without going to the URL, extract the image from the packet data and save it
Network Packet Analysis: Exercise 5

- Download “exercise5” and open it in Wireshark
- This is 802.11 traffic
- Find the number of “conversations” using the “Statistics” -> “Conversation List” -> “WLAN” tool
- What percentage of packets contain data?
Network Packet Analysis: Exercise 6

- Open the “Capture” menu and select “Interfaces….”
  - Choose start for the interface on which you want to capture packets
  - Open a web browser and access the wiki
  - Start an nmap scan on one of the target systems
  - Experiment with the tools in the “Analysis” menu
End of Module 3

- Questions?