3. Network Security

I. Network Security Theory

Network Layer Protocols

- IP - Internet Protocol
  - addressing
  - routing
- TCP - Transmission Control Protocol
  - Connection-oriented
  - reliable
  - 3-way handshake
  - flow and congestion control
- UDP - User Datagram Protocol
  - Connectionless
  - Lightweight, low-overhead
  - Speed > Reliability
  - VoIP, video streaming, audio streaming

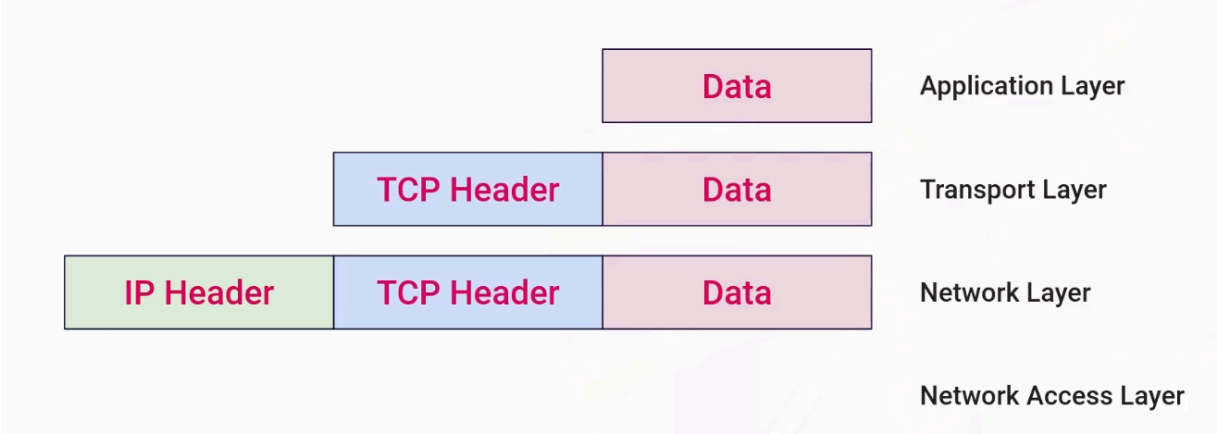
Common Ports

21 - FTP
22 - SSH
23 - Telnet
25 - SMTP
53 - DNS
80 - HTTP
110 - POP3
135 - RPC - Microsoft Remote Procedure Call
139 - NetBIOS
143 - IMAP
389 - LDAP
443 - HTTPS

445 - SMB
3389 - RDP
8080 - HTTP

II. Packet Capture and Flow Analysis

Packets



- Header
  - Contain all info about the packet
- Payload
  - Core content the packet is holding
- Trailer
  - Not always required

Packet Capture (PCAP)

- Intercepting Packets
  - Port mirroring (SPAN Ports)
  - Inline network devices
  - Network taps
- PCAP Files
  - binary file format
  - header and raw payload
  - Tcpdump, Wireshark, Tshark etc
- Advantages
  - most detailed record

    - Includes packet payload
- Disadvantages
    - Resource intensive
    - Requires significant storage space

Flow Records

- Aggregated metadata
- 5-Tuple
    - Source IP
    - Source Port
    - Destination IP
    - Destination Port
    - Transport Protocol
- Generated by devices such as firewalls
- Advantages
    - Efficient bandwidth and storage requirements
    - High level pattern and anomaly detection
    - Easier to scale
- Disadvantages
    - Lacks payload detail
    - Doesn't give the whole picture

III. Introduction to tcpdump

Installation

```
sudo apt-get install tcpdump -y
```

Setting to listen

```
tcpdump -D # Find available interfaces
sudo tcpdump -i lo
```

IV. tcpdump: Capturing Network Traffic

Using `-n` with tcpdump will prevent tcpdump from resolving domains to IPs

Adding a domain name to the command like below will filter for just example.com. This is useful for looking for a specific malicious site.

```
sudo tcpdump -i <interface> -n host example.com
```

use `src` and `dst` to specify the source and destination IP if needed.

use `net` to specify traffic to/from a specific network.

Save to a file using `-w` flag and give it the path/file.pcap name

```
sudo tcpdump -i <interface> -n -w ~/Desktop/capture.pcap
```

V. tcpdump: Analyzing Network Traffic

```
tcpdump -r capture.pcap
```

`--count` - display how many packets are in the file (can use filters to further divide the number)
`-c` - how many packets to display in output
`-t` removes timestamp
`-tt` converts timestamp to UTC
`-ttt` timestamp in millisecond since previous packet
`-tttt` hours / minutes / seconds

Advanced Searching for IP addresses:

```
tcpdump -tt -r file.pcap -n tcp | cut -d " " -f 5 | cut -d "." -f 1-4 | sort | uniq -c | sort -nr
```

VI. Wireshark: Capture and Display Filters

Capture Filters

Set before starting capture

- `host <IP address>`
- `port <port number>`
- `net <Network/CIDR range>`
- `src / dst`
- `and / or / not`
- `net`

Display Filters

Can be set at any point

- Protocols: `tcp / udp`
- Any item from field and sub items: `http.request`
- Comparisons: `== != < >`
- Contains: `http contains"login"`
- Logic: `AND OR NOT`

Advanced Filter Examples:

```
http.request.method == "GET"
http.request.uri contains "audiodg"
```

You can right click a packet and select or `Prepare as Filter > Apply as Filter`

VII. Wireshark: Statistics

Use the statistics tab to have wireshark run analysis on the pcap file.

```
Statistics > Capture File Properties
```

This page will have a lot of info about the pcap file:

- Time frame: Determine whether file covers the suspicious timeline
- Total Packets
- Filtered Packets

```
Statistics  > Resolved Addresses
```

Get a list of all IP addresses resolved to Domains

`Statistics > Protocol Hierarchy`
Displays the percentage of packets by protocol type
This tool runs display filters first before calculating percentages

`Statistics > Conversations`
Analyze the top talkers on the network
From here you can apply this as a display filter

`Statistics > HTTP`
Find quick info about HTTP packets

Follow Streams
You can select entire collections of packets that relate to each other.
Right click on packet > `Follow` > Select stream type
This will let you see an entire TCP or HTTP conversation

VIII. Wireshark: Analyzing Network Traffic

Workflow:

1. `Statistics > Capture File Properties` to find basic details about the pcap file.
    a. Time frame in question
2. `Statistics > Conversations > IPv4 > Packets A -> B` to find IP address with the most packets
    a. Note IP addresses of source and destination IPs of top talkers
    b. Consider the information flow and in what directions
3. `Statistics > Protocol Hierarchy Statistics >` to determine protocols in use
    a. http
    b. NetBIOS
4. Right Click http packet > `Follow > HTTP Stream` to search for artifacts
    a. User agents
    b. magic byte file signatures
    c. files within the pcap
5. `Statistics > HTTP > Requests` to find http requests
6. `File > Export Objects > HTTP` to find files within pcap
    a. Save to system

    b. `file <filename>` to get file information
    c. `sha256sum <filename>` to get hash
7. Search IOCs on VirusTotal to find more info on attack
    a. malware used
    b. mitre attack methodology

IX. Intrusion Detection and Prevention Systems

- Intrusion Detection Systems (IDS)
    - Passive monitoring and analysis
    - Alert generation
    - Logging
    - Out of band, not between traffic
- Intrusion Protection Systems (IPS)
    - Traffic inspection
    - Blocking and dropping packets
    - Alert generation
    - Logging
    - Inline deployment
    - Can introduce latency

- Types
    - Network based
    - Host based
- Detection Methods
    - Signature-based
    - Behavior-based
    - Rule-based

Known Knowns	Known Unknowns
Unknown Knowns	Unknown Unknowns

X. Introduction to Snort

- Security tool to analyze network traffic

- Modes:
  - Sniffer Mode
  - Packet Logger Mode
  - IDS/IPS Mode
- Operates from rules

```
sudo apt install snort -y
```

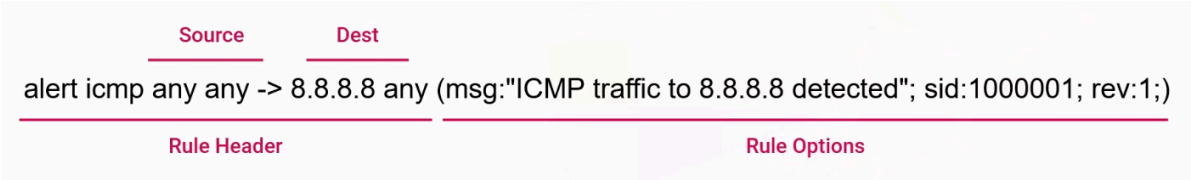
Give address range of local network
In typical organizational network the network interface must be run in promiscuous mode

Config Files:
`/etc/snort/snort.conf`
`/etc/snort/rules/`

XI. Snort: Reading and Writing Rules

http://snorpy.cyb3rs3c.net/

Anatomy of a Rule



- Action
  - `alert`
  - `log`
  - `drop`
  - `reject`
- Protocol
  - `icmp`
  - `ip`
  - `tcp`
  - `udp`
- Direction
  - `->` (source to destination)
  - `<>` (bidirectional)

- Source
  - ip
  - port
- Destination
  - ip
  - port
- Options
  - `msg` - Message included within the alert
  - `sid` - snort id number. Use a number above 1 mil (1000000)
  - `rev` - Revision number (track changes over time)

```
sudo nano /etc/snort/rules/local.rules
```

The rule can be added to this file as a new line.

```
sudo snort -A console -l /var/log/snort -i <interface> -c /etc/snort/snort.conf
-q
```

Community Rules

```
sudo mkdir /etc/snort/rules/community
cd /etc/snort/rules/community
sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz
sudo tar -xzvf community-rules.tar.gz
sudo cp community.rules /etc/snort/rules/community.rules
```

Logs

```
cd /var/log/snort/
sudo wireshark snort.log.<ID number>
```

Inline Mode

Must be running with two network interfaces on the machine

```
sudo snort -q -A console -i <interface>:<interface2> -c /etc/snort/snort.conf --daq afpacket -Q
```

XII. Snort: Intrusion Detection and Prevention