GitHub @deezcubicdude612

VI. NETWORK FORENSICS

Network forensics

* a branch of forensics that focuses on networking-related digital evidence
  ↳ involves monitoring, recording, analyzing & interpreting network traffic
* targets info transmitted & received over network, either on-the-fly or stored capture

Tools

Wireshark

* most powerful & free GUI-based network protocol analyzer
  ↳ tshark: CLI alternative
* cmd. tool: tcpdump (the original packet capture tool in Linux)
  ↳ good for quick analysis, ✗ for advanced analysis

Snort

* free & open-source Network Intrusion Detection & Prevention System (IDPS)
* uses rule-based language; perform protocol analysis + content searching/matching
* use case: detect various atks & probes → ex., buffer overflow, stealth port scans, SMB probes, OS fingerprinting attempts, etc.

In Snort, if Home Network is 10.42.85.0/24, configure in /etc/snort/snort.conf:

```
ipvar HOME_NET 10.42.85.0/24
```

Notes:

* disable DNS resolution to ↑ speed ↓ noise the adversary may pick up on
  ∴ adversary smart enough to stand up DNS servers (acting authority for their evil domains)
  → problem if you send traffic to their monitored DNS server
  → try to use -n as often as possible when using tcpdump for investigations

Malware Analysis (✗ covered in SE6016)

* study of unique feats., objectives, srcs, potential effects of harmful software & code (src: Fortinet)
* goals
  - study malware fx & behavior
  - analyze threat actor(s)
  - facilitate incident detection & response
* network forensics useful for Discovery stage (involves malware analysis) in Detection Engineering

imperva.com/learn/application-security/osi-model/

COMPUTER NETWORKING RECAP

OSI Model

* OSI: Open Systems Interconnection
* modern Internet based on TCP/IP model,
  but OSI model still helpful for:
  - ↳ visualizing & communicating how networks operate
  - ↳ isolate & troubleshoot networking problems

OSI Layers

"A Priest Saw Ten Nuns Doing Push-ups"

(VII) Application Layer

HCI layer where apps can access network services (ex., Gmail)

(VI) Presentation Layer

ensure data is in usable format & where data encryption occurs
ex. usable format for email: plain text, rich text format (RTF), HTML

(V) Session Layer

* maintains connections (ex., to SMTP); server connections made here
* responsible for ending ports & sessions; session encryption via SSL/TLS

(IV) Transport Layer

* breaks down content into packets (Ethernet payload size: 1500 bytes)
  - ↳ Wi-Fi follows Ethernet std; most Internet connections based off Ethernet or wired connection
* transmits data using transmission protocols (ex., TCP, UDP)

(III) Network Layer

aka. IP layer
decides which physical path the data will take
physical path: src. IP addr → dest. IP addr

→ Private IP Addr. Ranges
- ↳ Class A: 10.0.0.[0] ~ 10.255.255.[255]
- B: 172.16.0.[0] ~ 172.31.255.[255]
- C: 192.168.0.[0] ~ 192.168.255.[255]

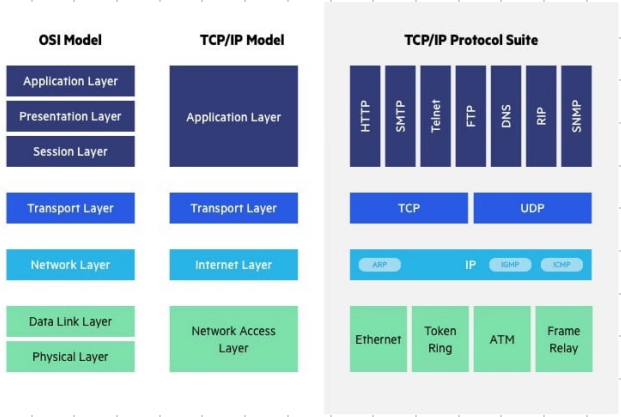
(II) Data Link Layer

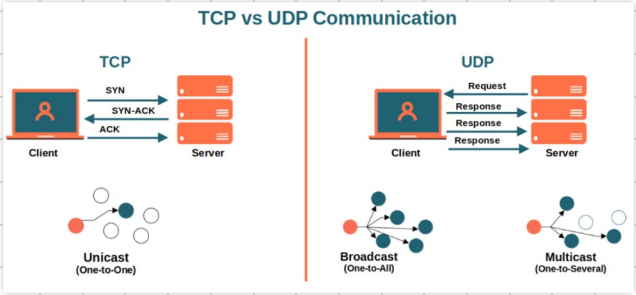
(typically closer to physical network)
defines data format on network; follow required IEEE 802.11 format

(I) Physical Layer

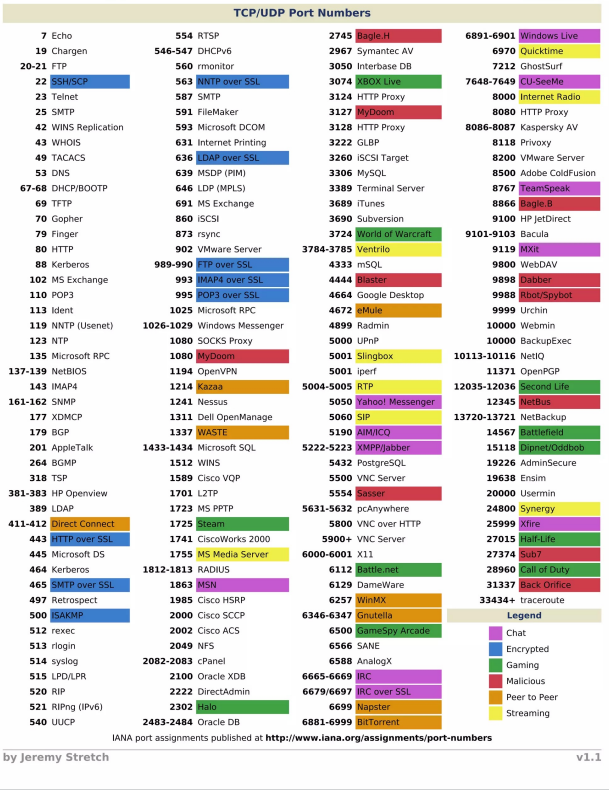
transmits raw bit stream (as physical electronic impulses)
over physical medium — network card → access pt., or
host → host (via cable)

Layer 7 → 1: [Multiplexing] → technique used to combine & transmit multiple signals for multiple srcs over a single communication/physical line
Layer 1 → 7: Demultiplexing





cheapsslsecurity.com/blog/tcp-vs-udp-how-are-they-different



ipwithease.com/common-tcp-ip-well-known-port-numbers/

Common Ports

PORT NUMBER	TRANSPORT PROTOCOL	SERVICE NAME	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

https://ipwithease.com