

[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

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 tethdump for investigations

Tools

Wireshark

- * most powerful & free GUI-based network protocol analyzer

- ↳ tshark: CLI alternative

- * nvi - 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 core: 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

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

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., email)

(VI) Presentation Layer

ensure data is in useable format & where data encryption occurs

ex. useable format for email: plain text, rich text format (RTF), HTML

(V) Session Layer

* maintains connections (ex., to SMTP); server connections made here

* responsible for establishing ports & sessions; session encryption via SSL/TLS

(IV) Transport Layer

* breaks down content into packets (Ethernet payload size: 1500 bytes)

↳ WiFi 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

(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)

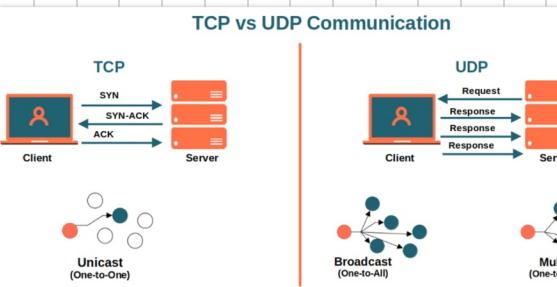
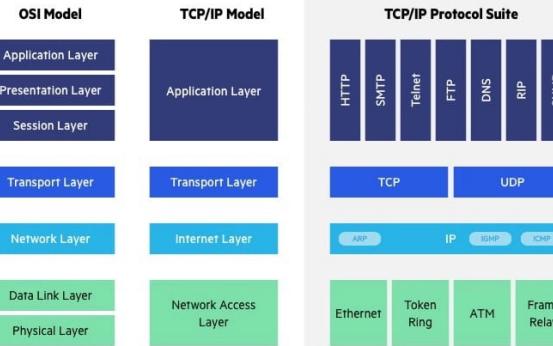
over physical medium ↳ network card → access pt. , or

host → host (via cable)

Layer 7 → 1: **Multiplexing** → technique used to combine & transmit

Layer 1 → 7: **Demultiplexing** multiple signals from multiple srcs

over a single communication/physical line



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

↳ **Private IP Addr. Ranges**

↳ Class A: 10.0.0.[7]0 ~ 10.255.255[7]255

B: 172.16.0.[7]0 ~ 172.31.255[7]255

C: 192.168.0.[7]0 ~ 192.168.255[7]255

Common Ports

COMMON PORTS	
TCP/UDP Port Numbers	
7 Echo	554 RTSP
19 Chargen	546-547 DHCPv6
20-21 FTP	560 rmonitor
22 SSH/SSCP	563 NNTP over SSL
23 Telnet	587 SMTP
25 SMTP	591 FileMaker
42 WINS Replication	593 Microsoft DCOM
43 WHOIS	631 Internet Printing
49 TACACS	636 LDAP over SSL
53 DNS	639 MSDP (PIM)
67-68 DHCP/BOOTP	646 LDP (MPLS)
69 TFTP	691 MX Exchange
70 Gopher	860 iSCSI
79 Finger	873 rsync
80 HTTP	902 VMware Server
88 Kerberos	989-990 FTP over SSL
102 MS Exchange	993 IMAP4 over SSL
110 POP3	995 POP3 over SSL
113 ident	1025 Microsoft RPC
119 NNTP (Usenet)	1026-1029 Windows Messenger
123 NTP	1080 SOCKS Proxy
135 Microsoft RPC	1080 MyDoom
137-139 NetBIOS	1194 OpenVPN
143 IMAP4	1214 Kazaa
161-162 SNMP	1241 Nessus
177 DMDP	1311 Dell OpenManage
179 BGP	1337 WASTE
201 AppleTalk	1433-1434 Microsoft SQL
264 BGMP	1512 WINS
318 TSP	1589 Cisco VQP
389 LDAP	1701 L2TP
411-412 Direct Connect	1723 MS PPTP
443 HTTP over SSL	1725 Steam
445 Microsoft DS	1741 Cisco Workbooks 2000
464 Kerberos	1755 Cisco Media Server
465 SMTP over SSL	1812-1813 RADIUS
497 Retrospect	1863 MSN
500 ISAKMP	1985 Cisco HSRP
512 rexec	2000 Cisco SCCP
513 rlogin	2002 Cisco ACS
514 syslog	2049 NFS
515 LPD/LPR	2100 Oracle XDB
520 RIP	2222 DirectAdmin
521 RIPv2 (IPV6)	2302 Halo
540 UUCP	2483-2484 Oracle DB
IANA port assignments published at http://www.iana.org/assignments/port-numbers	

packetlife.net

v1.1

by Jeremy Stretch

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

-port-numbers/

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 and UDP	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>