SY0-601

Security Roles / Controls → Lesson 1A

MCQ, Performance-Based, Drag-And-Drop

CIA – Confidentiality, Integrity, Availability

1. Confidential → Outside-In
2. Integrity < Storage / Transport
3. Availability

Non-Repudiation

SOC → Security Operations Center

DevOps → DevSecOps
- ↙ SDE
- ↓ Security
- ↘ Sys Admin

DFIR

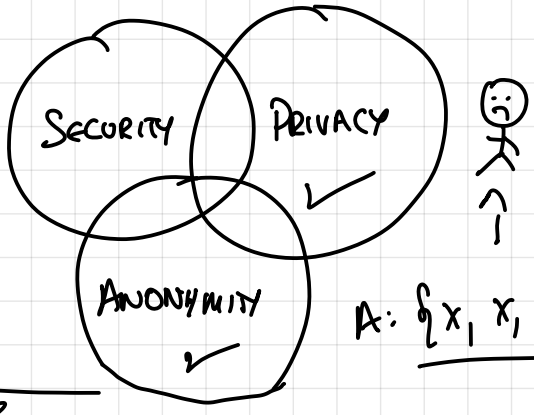
Digital Forensics / Incident Response

1B- Security Controls

Data and PPL

1. Technical – Software / Hardware Based
2. Operational – Human Based
3. Managerial – Oversight Based

Physical Security ↔ Digital Security
- Physical Security → Locks, Alarms | RFID
- Digital Security → Passwords, Crypto



A: {x, x, x, x}

Lesson 2: Threat Actors / Threat Intelligence

2A: Threat Actors.

Vuln, Threat, Risk

1. **Vuln**: Weakness, Factual, Can Exist On Its Own
2. **Threat**: Potential, Created By Vuln
3. **Risk**: Probability That Threat Becomes Real
   Considers Impact, Could Be 0

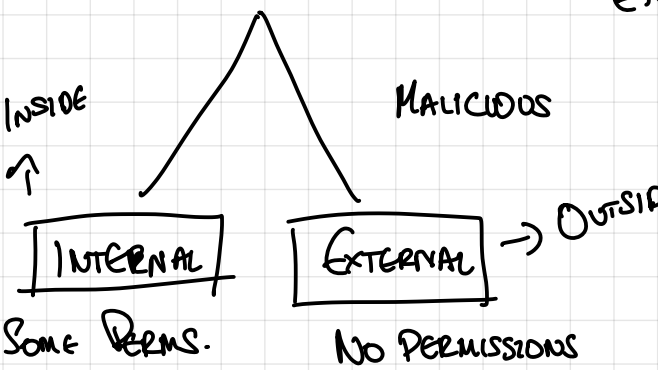
Sev 0, Sev 1, Sev 2, Sev 3

0-Day: Undiscovered Vuln.

Anna

Threat Modelling

1) Attack Vector: Method Of Exploitation.
2) Threat Actor: Intent? Malicious? Not? Etc.



SY0-601 – Student Guide

Homework 1:
Lesson 1: Read ⇒ Cybersecurity Frameworks.

Check MCQ
Credit System

Sys Bomin ⇒ System Administrator

Threat Actors

Internal	External
Some perms	No Perms
Employees Contractors	Needs To Break-In

→ Threat Actors May Not Always Be Hostile

→ **Level Of Sophistication**
- → Skids → Script Kiddie → Low Sophistication
- → Ransomware Group, Hackers → Medium Sophistication
- → Nation-State → Highly Sophisticated

→ Determines The Threat

APTs → Advanced Persistent Threat

↓ High Soph
Nation State
Advanced Tech, Motivation

Single Target Persistence

APT 1
APT 25

SSO
Special Source Operations

Attacks

→ Attack Surface: Where Do Vulnerabilities Exist Once They Have Been Identified?

A very large Attack Surface → High Risk ↑

↑ Internal Threats External Threats ↓

→ The Goal: Run Malicious Code

→ Make Attack Sfc Smaller → Minimizing Exposed Parts
- ✓ Closing Ports
- ✓ Access To Few Ppl
- ✓ Obscurity

1.5 Threat Actors, Attack Vectors

SLASHDOT

Supply Chain Attack:

Solar Winds → Attack Something The Target Is Being Supplied With

Common Types Of Attack Vectors

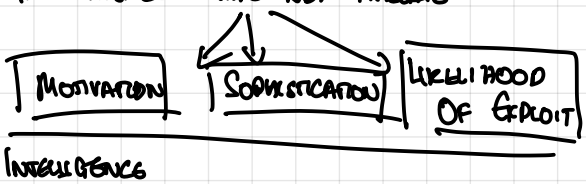
→ Direct Access: Walk Up And Access
→ Removable Media: Flash Drive (Stuxnet)

→ Email: Click On Link, Open Attachment
→ Network Vector: Send Information Wirelessly / Malicious Send Over The Network (Not Encrypted)

Send And Receive

2B Threat Intelligence

→ Threat Intelligence: Info Abt Threats



Counter Intelligence

TTPs: Tactics, Techniques, Procedures

Some Sources Only Available To Govt And Contractors

Obtaining Threat Intelligence Through
Reconnaissance (Recon)

Mandiant: Threat Intelligence Provider } Only Specific Indicators e.g. Repeated Phishing Attempts
NSA: Provides That for US Govt.

OSINT: Open-Source Intelligence
Publically Available Info. → Bellingcat
Humint: Human Intelligence → CIA
Sigint: Signals Intelligence,
↳ Electromagnetic Signals Interception

↘ Attackers Can Use These Techniques
Info Abt. Target
White Papers On Vulns.

Read Lesson 1
Read Lesson 2 !!

TTPs ⇒ SOP → Standard Operating Procedure
IoC → Indicator Of Compromise
↓
Firewall Log / Opened Port / Residual File } DFIR Specialty

Know Examples Of IOCs !!!.

→ Can Be One Thing
→ Usually Deviation From Average Behavior Of System

LESSON #3.0:

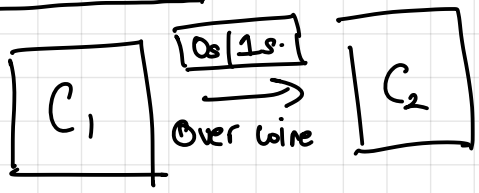
- → Basic networking ✓
- → OSI model ✓
- → TCP vs. UDP vs. ICMP ✓
- → Packet structure ✓
- → Routing

NETWORKING:

→ Wireless or wired comm. b/w 2 comp.

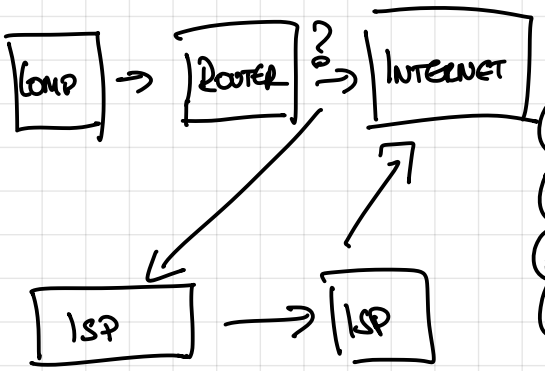
→ To exchange info. (sometimes sensitive).

DARPA
ARPANET



WIFI
↓
WIRELESS FIDELITY

INTERNET SERVICE PROVIDER



1. COMPUTER$_1$ → ROUTER (WIRELESS)
2. ROUTER → ISP. (CABLE).
3. ISP$_1$ → IXP (CABLE)
4. IXP → ISP$_2$ (CABLE)
5. ISP$_2$ → ROUTER (CABLE)
6. ROUTER → COMP$_2$ (WIRELESS).

IXPs → INTERNET EXCHANGE POINTS.

LAN → LOCAL AREA NETWORK

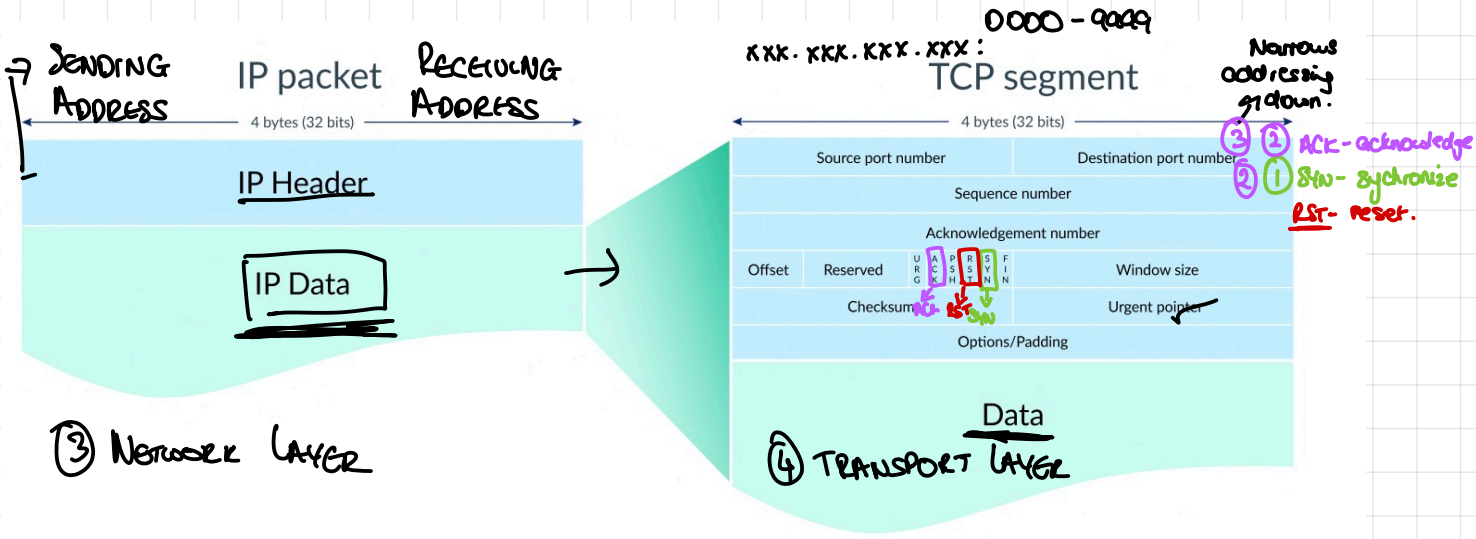
1. ADDRESS: SPECIFY DESTINATION ✓
2. PATH: OPTIMAL WAY OF GETTING TO DESTINATION.
3. EFFICIENT WAY OF TRANSFERING DATA.

OSI MODEL: OPEN SYSTEMS INTERCONNECTION MODEL
LAYERS OF ABSTRACTION FOR NETWORK DATA.

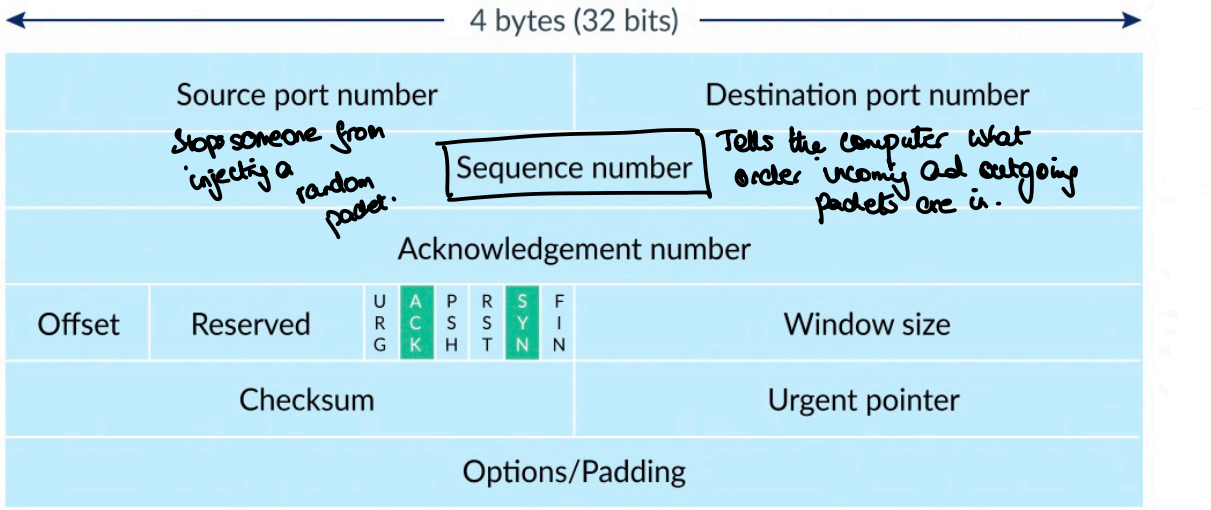
802.11 a/b/c	ETHERNET
Wi-Fi	802.3
802.11	IEEE spec.
IEEE spec.	

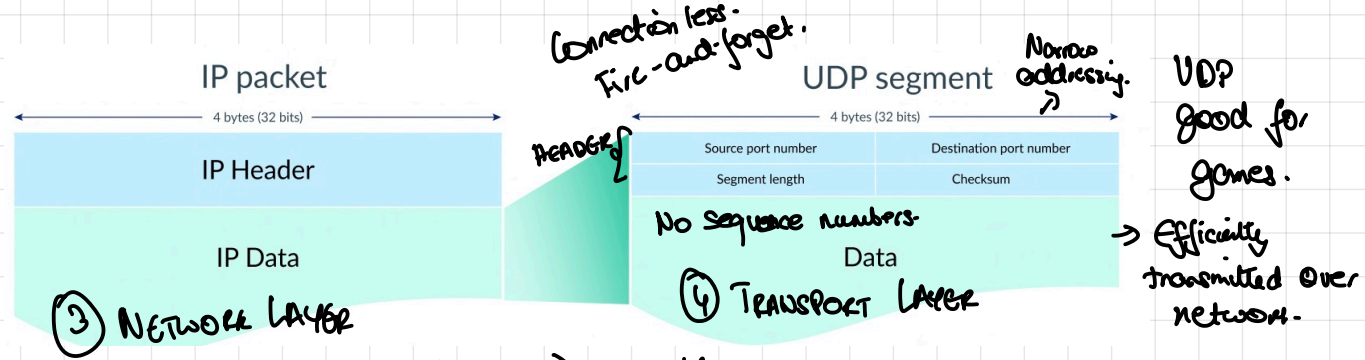
1. PHYSICAL LAYER → Link b/w bits and trans. medium e.g. radio frequency | fiber optic. (physics)
2. DATA-LINK LAYER → Ethernet | wifi standards. Link b/w info | data, converting it to binary that can be efficiently transmitted.
3. NETWORK LAYER → INTERNET PROTOCOL. (addressing system). Connectionless. (Packets).
4. TRANSPORT LAYER → TRANSMISSION CONTROL PROTOCOL. (CONNECTION-BASED). USER DATAGRAM PROTOCOL.
5. SESSION LAYER → Responsible for maintaining a session between computers. DNS → Domain Name System.
6. PRESENTATION LAYER → GOOGLE CHROME | SAFARI | FIREFOX → Presents web | internet data to the user.
7. APPLICATION LAYER. → HTTP (HYPERTEXT TRANSFER PROTOCOL). | FTP → FILE TRANSFER PROTOCOL. → The actual application you use.

1. DATA NEEDS TO BE SEQUENTIAL. ✓
2. ERROR CORRECTION. ✓

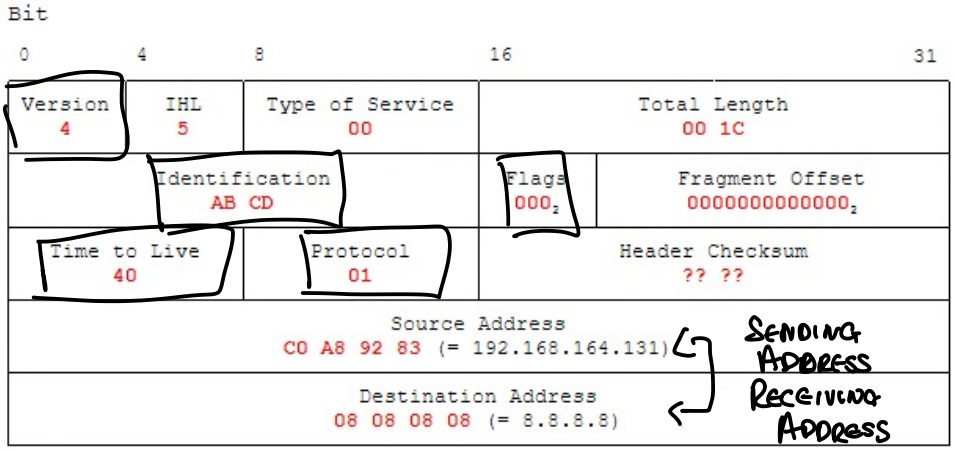


TCP PACKET HEADER





ICMP PACKET HEADER



2 NETWORK LAYER.

INTERNET CONTROL MESSAGE PROTOCOL

→ For debugging or trouble shooting purposes.

ping ⇒ SENDS OUT ICMP PACKETS BY DEFAULT

TCP | UDP packet a more common source of issues.

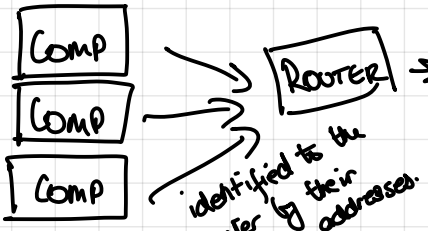
→ IP ADDRESS : xxx . xxx . xxx . xxx (IPv4) (INTERNET PROTOCOL version 4)

→ IP ADDRESS → STATIC / DYNAMIC

alphanumeric, 12 characters

xx : xx : xx : xx : xx : xx

→ MAC ADDRESS : MEDIA ACCESS CONTROL ADDRESS → hardcoded, won't change



↓ PUBLIC IP ADDRESS

172 . 253 . 122 . 104 → 32-bits → IPv6 → 64-bit address

↓ 2^{32} possible combos

limited amount of public IPv4 addresses.

(172 . 25 . xxx . 162) 2^{32}

↓ session

192, 172.

192 . 0 . 0 . 1

localhost

Poor security to block an IP address MAC Address, specific unchanging

if you block IP, someone else could get it accidentally

Lesson 3A: Network Reconnaissance

Lesson 3: Security Assessments.

Red Team	Blue Team
→ Offensive team → Actively trying to breach an organization	→ Defensive team → Trying to defend the org from attack.

→ Will do recon to find usable exploits.
→ Recon to find and patch usable exploits.

4.1) Use Tools To Assess Org Security

The Network

→ Every computer connected to other computer.
→ Form the vertexes of a graph.
→ Creates a map of the network.

footprinting: Create a network map to figure out where pts of entry are.

	Windows	MacOS / Linux	What It Do?
1	ipconfig	ifconfig	→ Configs for network interface (Wi-Fi, BT, Eth).
2	ping	ping	→ Sends ICMP packets to IP or URL. (might need to change packet type).
3	arp (Address Resolution Protocol)	arp	→ Resolves MAC address.
4	route	route	→ allows you to config local routing.
5	tracert (ICMP)	traceroute (UDP)	→ route discovery
	pathping (ping / tracert combo)	mtr (ping/traceroute combo).	

NMAP → Network Map. (SHODAN)

→ Network Reconnaissance
→ What devices are on a network (pref local)
→ What ports are open.

→ Allows you to scan the network in a lot of different ways
172.x.x.0 → 172.x.x.255

→ SYN-scanning: Sends synchronization request
→ receives SYN-ACK → no ACK back.
↓
SYN-flood. max out the connection limit

| Doesn't make sense to use UDP.

```
root@EthicalHaks:~# nmap -A 192.168.0.9

Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-23 21:49 PDT
Nmap scan report for 192.168.0.9
Host is up (0.000058s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          46044/udp  status
|_  100024  1          54793/tcp  status
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.4
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.71 seconds
```

open ports
kernel version
OS version
→ local computer → running it on their own computer.

→ OSes generate TCP sequence # in unique ways.
1 → ∞

→ Sequence Numbers → appended with random other numbers for security purposes.
↓
random info generated by the OS
→ on Linux → dev/random
→ dev/urandom.

→ TCP #s start from diff points depending on OS.
→ Nmap has fingerprinting database.

More Commands:

→ netstat : Show you all open TCP/UDP ports on your computer.
→ dig | ns lookup : pulls up DNS records.

↕ Diagnostic Tools

Saved network data is usually stored in .pcap.

Libpcap → Library Packet Capture → library
tcpdump → Built On Libpcap → command

↗ Packet Sniffing: intercepting packets

Packet sniffers use both of these ! → Wireshark ! nice frontend for libpcap | tcpdump.
Allows you to see GUI packet. Allow you to create | send packets & intercept them.

tcpreplay: replays a stream of recent TCP traffic.

NET CAT:

nc: allows you to test network connections
specifically for TCP/UDP, allows you to manipulate connections.
listen to a connection → save the output to a file.

NMAP: bunch of tools in one
NETCAT: more customization, more info.

→ Given a scenario, pick the right tool.

HOMEWORK! Read lesson 3A! → Do the Review Activities!

Do Quiz!