

SYO-601

SECURITY ROLES / CONTROLS → LESSON 1A

MCCQ, 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
↓
SDG SECURITY Sys Admin

DFIR

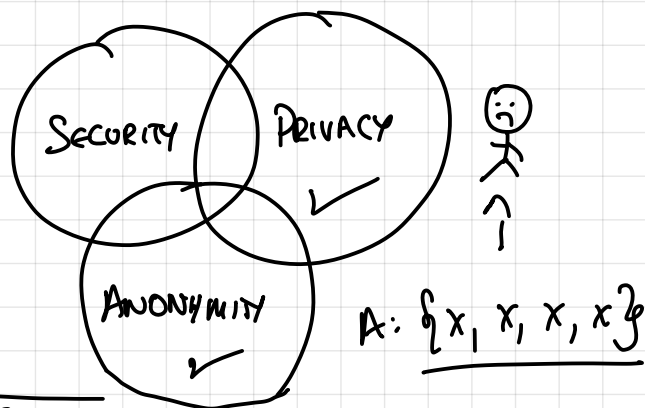
DIGITAL FORENSICS |
INCIDENT RESPONSE

7B- SECURITY CONTROLS

DATA AND PPL

1. TECHNICAL - SOFTWARE / HARDWARE BASED
2. OPERATIONAL - HUMAN BASED
3. MANAGERIAL - OVERSIGHT BASED

PHYSICAL SECURITY ↔ DIGITAL SECURITY
↓ ↓
LOCKS, ALARMS | RFID | PASSWORDS, CRYPTO



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 }
(CONSIDERE IMPACT, COULD BE 0)

Sev 0, Sev 1, Sev 2, Sev 3

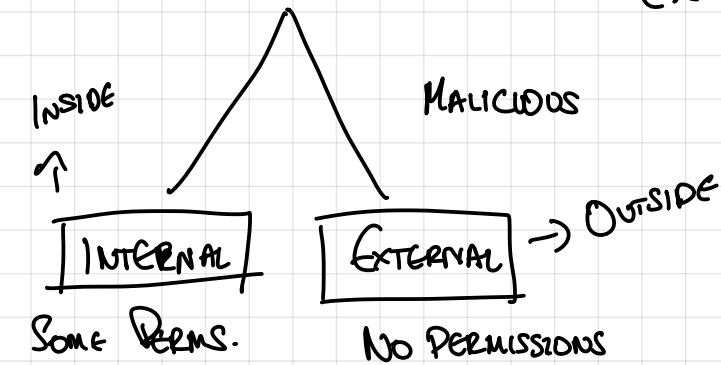
0-DAY: UNDISCOVERED VULN.

Anna

THREAT MODELLING

① ATTACK VECTOR: METHOD OF EXPLOITATION.

② THREAT ACTOR: INTENT? MALICIOUS? NOT?
ETC.



SP0-601 - STUDENT GUIDE

HOMEWORK 1:

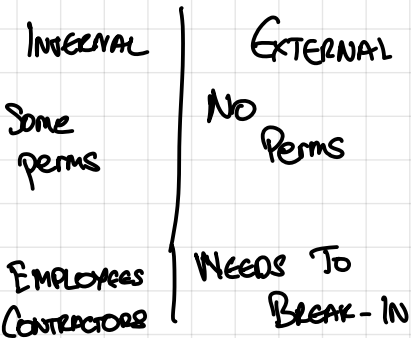
LESSON 1: READ

→ CYBERSECURITY
FRAMEWORKS.

CHECK MCS
CHECK SYSTEM

Sys Admin
→ SYSTEM
ADMINISTRATOR

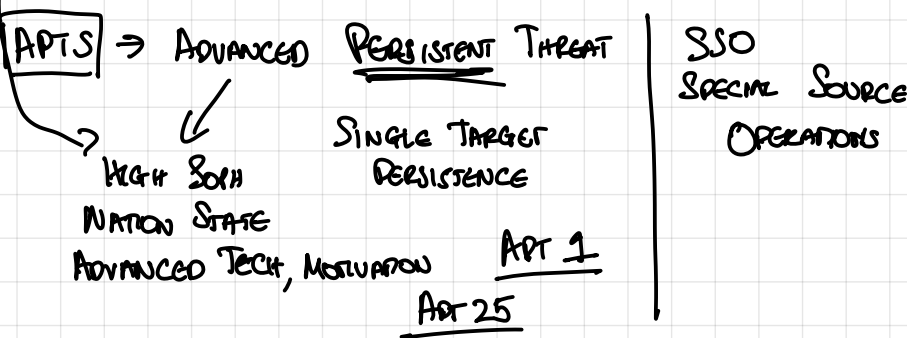
THREAT ACTORS



→ THREAT ACTORS MAY NOT ALWAYS BE HOSTILE

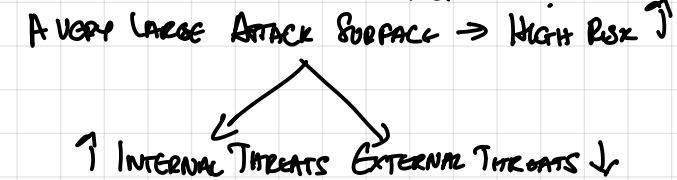
Level Of Sophistication

- SKIDS → SCRIPT KIDNIE → LOW SOPHISTICATION
- RANSOMWARE GROUP, HACKERS → MEDIUM SOPHISTICATION
- NATION-STATE → HIGHLY SOPHISTICATED
- DETERMINES THE THREAT



ATTACKS

→ ATTACK SURFACE: WHERE DO VULNERABILITIES EXIST
ONCE THEY HAVE BEEN IDENTIFIED?



1.5 THREAT ACTORS, ATTACK VECTORS

→ THE GOAL: RUN MALICIOUS CODE

- MAKE ATTACK SRC SMALLER → MINIMIZING EXPOSED PARTS
- ✓ CLOSING DOORS
 - ✓ ACCESS TO FEW PPL
 - ✓ OBSCURITY

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
SPEAK 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
NSA: PROVIDES THAT FOR US GOVT. } G-G REPEATED PHISHING ATTACKS

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

WRITE 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

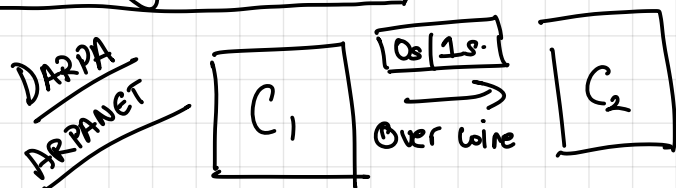
→ USUALLY DEVIATION FROM AVERAGE BEHAVIOR OF SYSTEM

LESSON #13.0:

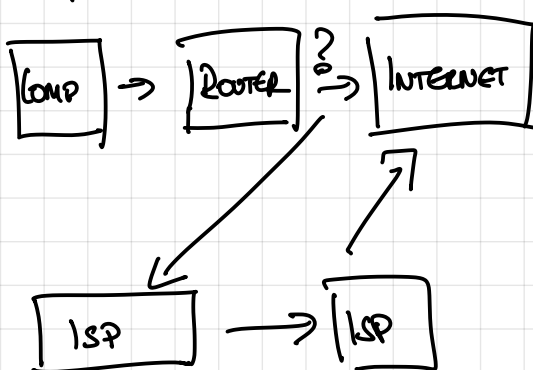
- Basic networking ✓
- OSI model ✓
- TCP vs. UDP vs. ICMP ✓
- Packet structure ✓
- Routing ✓

Networking:

- Wireless or wired comm. b/w 2 comp.
- To exchange info. (sometimes sensitive).



WIFI
↓
Wireless Fidelity
Internet Service Provider



- 1 Computer₁ → Router (Wireless)
- 2 Router → ISP. (Cable).
- 3 ISP₁ → IXP (Cable)
- 4 IXP → ISP₂ (Cable)
- 5 ISP₂ → Router (Cable)
- 6 Router → Computer₂ (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 Transferring Data. 2

OSI Model: Open Systems Interconnection Model
Layers Of Abstraction For Network Data.

802.11 a/b/g

Wi-Fi

802.11
IEEE spec.

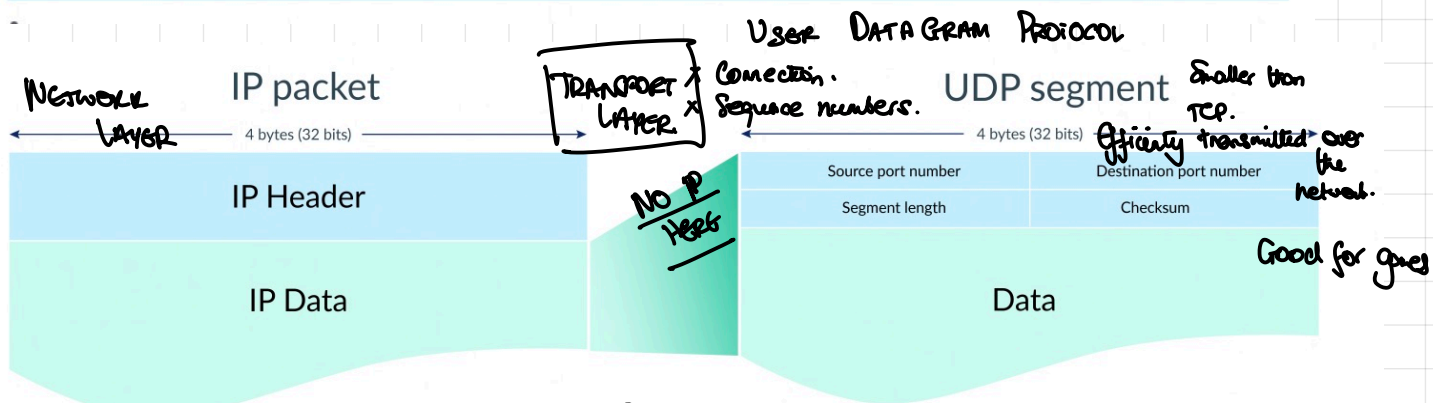
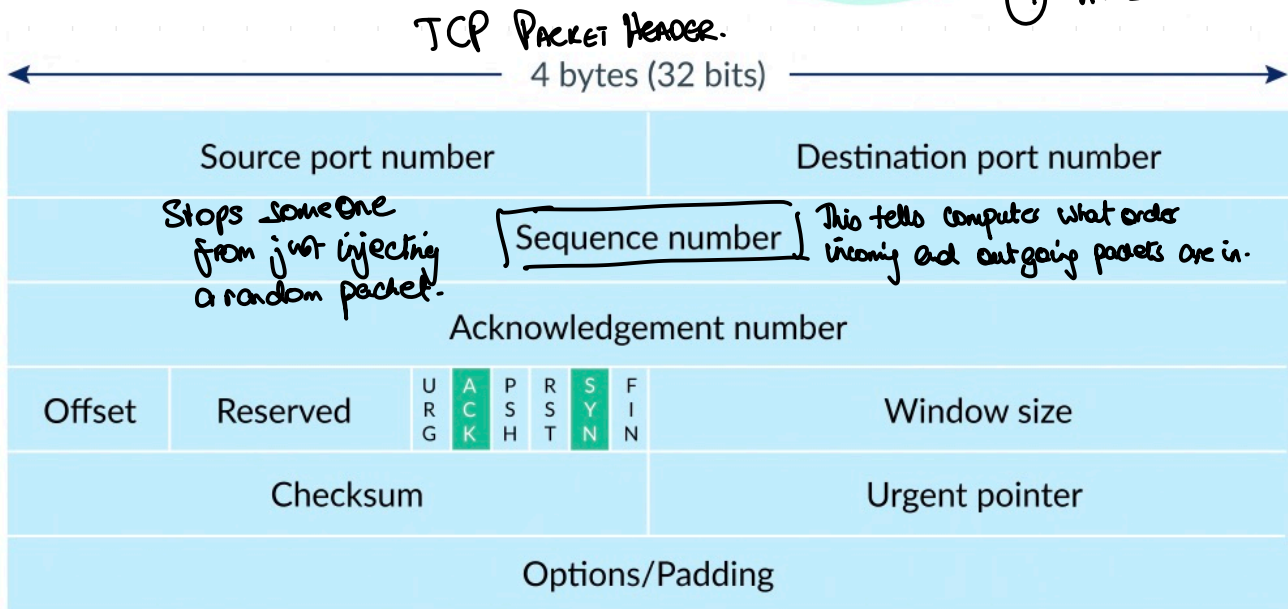
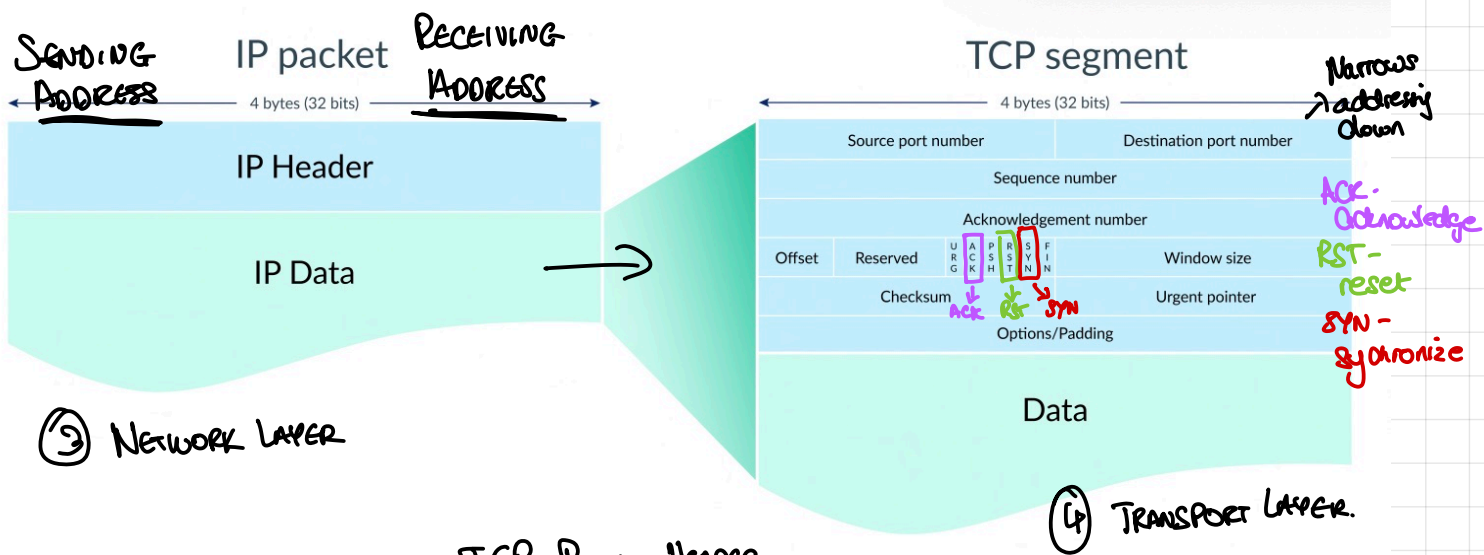
Ethernet

802.3
IEEE spec.

- 1 Physical Layer → Link b/w bits and trans. medium
e.g. radio frequency | fiber opti. (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. ✓



ICMP Packet

0	4	8	16	31
Version 4	IHL 5	Type of Service 00	Total Length 00 1C	
Identification AB CD		Flags 000 ₂	Fragment Offset 000000000000 ₂	
Time to Live 40	Protocol 01		Header Checksum ?? ??	
Source Address C0 A8 92 83 (= 192.168.164.131)				
Destination Address 08 08 08 08 (= 8.8.8.8)				

Handwritten notes:

- ICMP → Network Layer**
- Internet Control Message Protocol**
- For debugging or troubleshooting purposes.**
- Source IP Address** (next to Source Address)
- Destination IP Address** (next to Destination Address)

ping → SENDS OUT ICMP PACKETS BY DEFAULT

TCP / UDP packet a more common source of issues.

IP ADDRESS ✓ $xxx.xxx.xxx.xxx$
MAC ADDRESS : Media Access Control Address $xx:xx:xx:xx:xx:xx$
↓
hard coded → it won't change.
→ IP ADDRESS { Static
Dynamic → might change

802.3 → ETHERNET 802.x

802.11 → Wi-Fi

802.15 → BLUETOOTH

802.x

$xxx.xxx.xxx$. 000-255

↓
Subnet.

SERVER → IP ADDRESSES

