

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

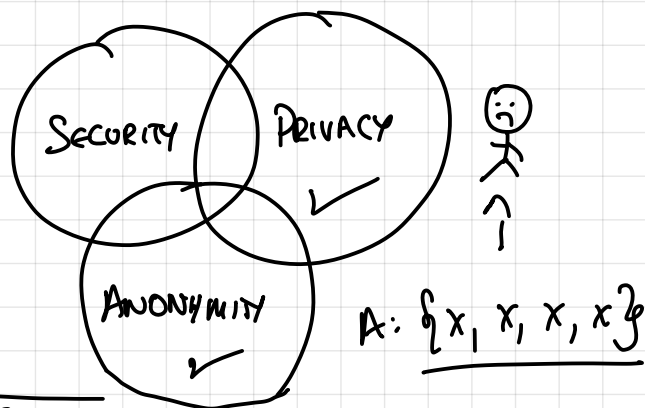
DIGITAL FORENSICS |  
INCIDENT RESPONSE

2B- 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

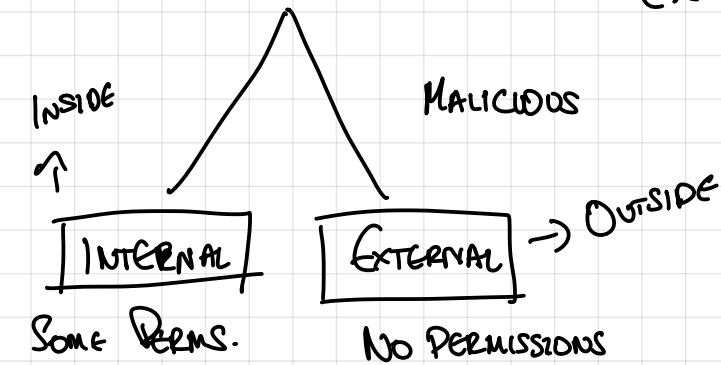
0-DAY: UNDISCOVERED VULN.

Anna

### THREAT MODELLING

① ATTACK VECTOR: METHOD OF EXPLOITATION.

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



SP0-601 - STUDENT GUIDE

HOMEWORK 1:

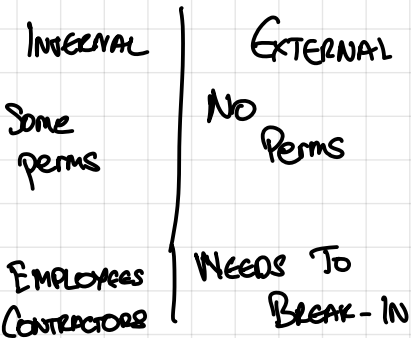
LESSON 1: READ

→ CYBERSECURITY  
FRAMEWORKS.

CHECK MCS  
CHECK SYSTEM

Sys Admin  
→ SYSTEM  
ADMINISTRATOR

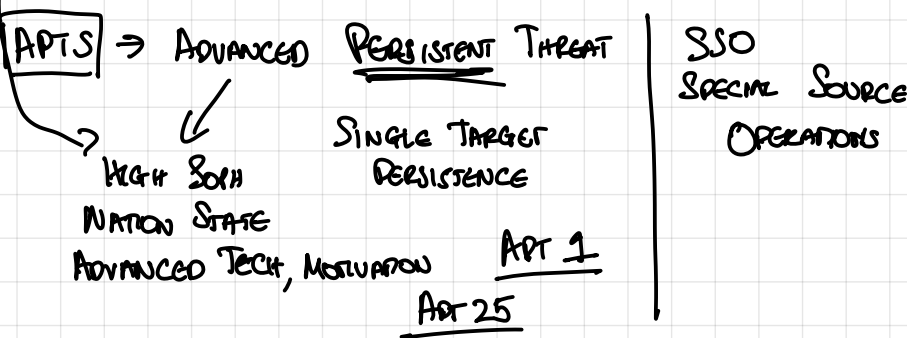
# THREAT ACTORS



→ THREAT ACTORS MAY NOT ALWAYS BE HOSTILE

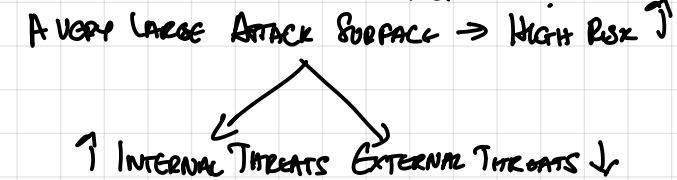
## Level Of Sophistication

- 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?



→ THE GOAL: RUN MALICIOUS CODE

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

## COMMON TYPES OF ATTACK VECTORS

- DIRECT ACCESS: WALK UP AND ACCESS
- REMOVABLE MEDIA: FLASH DRIVE (STORAGE)

1.5 THREAT ACTORS, ATTACK VECTORS

## SLASHDOT

### SUPPLY CHAIN ATTACK:

SOLAR WINDS → ATTACK SOMETHING THE  
TARGET IS BEING SUPPLIED  
WITH

→ 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

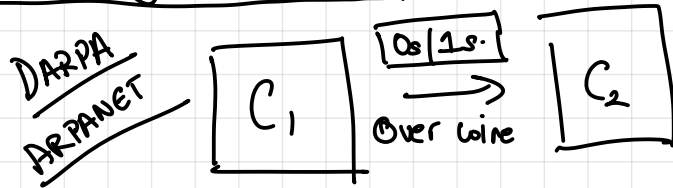
→ USUALLY DEVIATION FROM AVERAGE BEHAVIOR OF SYSTEM

# LESSON #13.0:

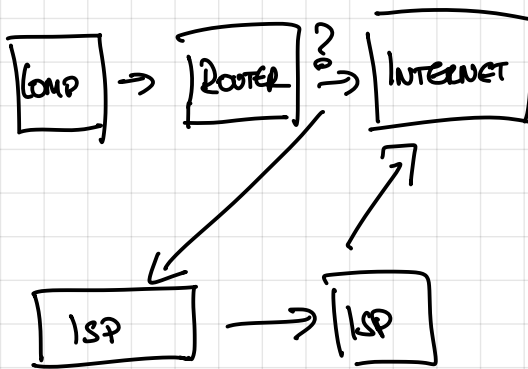
- Basic networking
- OSI model
- TCP vs. UDP vs. ICMP
- Packet structure
- Routing

## Networking:

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



WIFI  
↓  
Wireless Fidelity  
Internet Service Provider



- 1) Computer<sub>1</sub> → Router (Wireless)
- 2) Router → ISP. (Cable).
- 3) ISP<sub>1</sub> → IXP (Cable)
- 4) IXP → ISP<sub>2</sub> (Cable)
- 5) ISP<sub>2</sub> → Router (Cable)
- 6) Router → Computer<sub>2</sub> (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.

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

802.11 Q/b/c

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 | Wi-Fi 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. ✓

