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

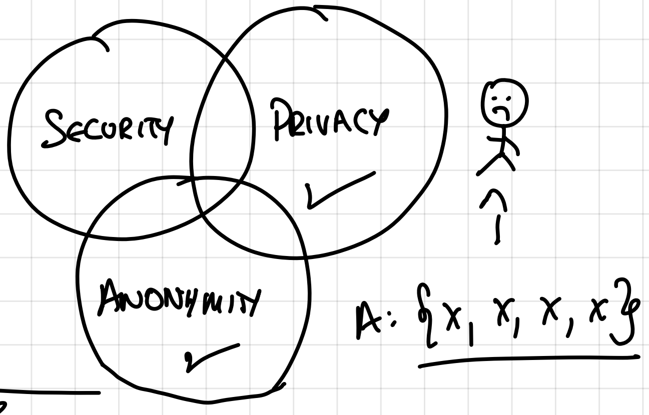
DFIR

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

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
CONSIDERS IMPACT, COULD BE 0

SEV 0, SEV 1, SEV 2, SEV3

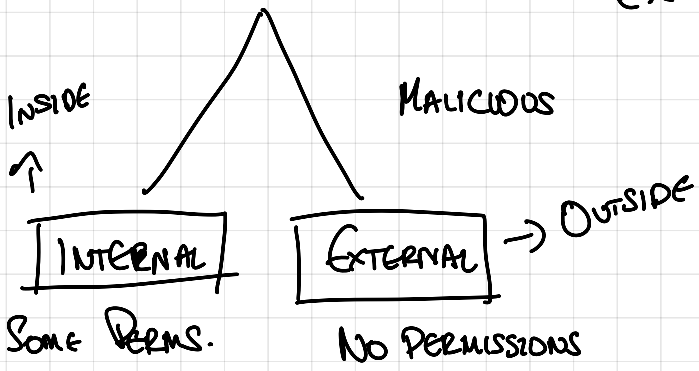
0-DAY: UNDISCOVERED VULN.

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

SYSADMIN → 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 <u>Persistent</u> Threat

High Soph
Nation State
Advanced Tech, Motivation

Single Target
Persistence

APT 1

APT 25

SSO
Special Source
Operations

Attacks

→ <u>Attack Surface</u>: 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
✓ Acess To Few PPL
✓ Obscurity

1.5 Threat Actors, Attack Vectors

<u>Slashdot</u>

<u>Supply Chain Attack</u>:

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 <u>Information</u> Wirelessly
Malicious
Steal Over The Network. (Not Encrypted)

Send And Receive

2B Threat Intelligence

→ Threat Intelligence : Info Abt Threats

Motivation | Sophistication | Likelihood Of Exploit

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

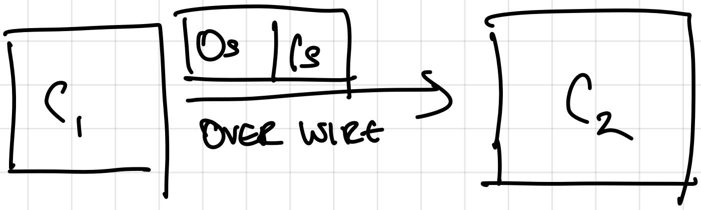
- → Basic networking ✓
- → OSI model
- → TCP vs. UDP vs. ICMP
- → Packet structure
- → Routing

Networking

→ Wireless or Wired Comm B/w Comps.

→ To Exchange Info (Sometimes Sensitive)

DARPA → ARPANET



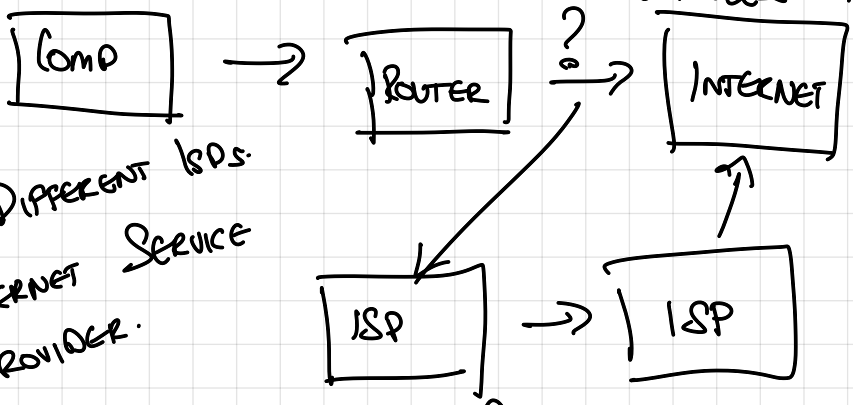
Wi-Fi | BT

↓

Wireless Fidelity

IEEE

(802.11 a/b/c. Local Area Network Wireless Standard)



Different ISPs.

Internet Service Provider.

1. Computer → Router (Wireless)
2. Router → ISP. (Cable)
3. ISP_1 → IXP (Cable)
4. IXP → ISP_2 (Cable) (Transfer)
5. ISP_2 → Router (Cable) (Recv.)
6. Router (Recv.) → Computer (R) Wireless.

IXPs → Internet Exchange Points.

802.11 | 802.3

WiFi | Ethernet

LAN: Local Area Network

1. Address?
2. Path.
3. Efficient Way Of Transferring Data.

OSI Model

→ Open Systems Interconnection Model

Layers Of Abstraction.

1. Physical Layer → Binary data trans/recv. over cables.
2. Data Link Layer → Ethernet cable / LAN cables. PPPoE
3. Network Layer → Internet Protocol connectionless.
4. Transport Layer → TCP → Transmission Control Protocol
   → UDP → User Datagram Protocol.
5. Session Layer. → DNS | SOCKS
6. Presentation Layer. → Browsers.
7. Application Layer → HTTP → Hypertext Transfer Protocol. | FTP → File Transfer Protocol.

① fiber optic cables. / copper cables / phone lines.