INTRUSION PREVENTION SYSTEM

MODULE 2

INTRODUCTION

- An intrusion prevention system (IPS) monitors network traffic for **potential threats and automatically blocks** them by alerting the security team, terminating dangerous connections**, removing malicious content** or **triggering** other security devices.
- IPS has same **detection capabilities**, logging capabilities like IDS but it has **automated prevention** abilities which is absence in IDS.
- IPSs can help enforce network security policies by blocking unauthorized actions from legitimate users, and they can support compliance efforts.

THREAT DETECTION METHODS

- IPSs use three primary threat detection methods-

1) Signature-based detection- Signature-based detection methods **analyze network packets** for attack signatures—unique characteristics or behaviors that are associated with a specific threat. If a packet triggers a match to one of the signatures, the IPS respond.

2) Anomaly-based detection- The IPS compares ongoing **network activity** to the model and responds when it finds deviations, anomaly-based IPSs respond to any **abnormal behavior,** they can often block brand-new cyber-attacks that might evade signature-based detection. Anomaly-based IPSs may be more prone to false positives.

CONTT…

3) Policy-based detection- It is based on **security policies set by the security team**. Whenever a policy-based IPS detects an action that violates a security policy, it blocks the attempt. Eg- if an **unauthorized user tries connecting to the host**, a policy-based IPS **stops t**hem.

CONTT…

- IPS automatically takes action against the threat by using techniques such as:

a) **Blocking malicious traffic**
b) **Removing malicious content**
c) **Triggering other security devices**
d) **Enforcing security policies**

TYPES OF IPS

1) **NIPS(Network-based Intrusion Prevention System)-** installed to **monitor all network traffic** and scan for threats.
2) **HIPS(Host-based Intrusion Prevention System)-** which is installed on an endpoint and **looks at inbound/outbound** traffic from that machine only.
3) **NBA(Network Behavior Analysis)-** analyzes network traffic to detect **unusual traffic flows and spot new malware** or zero-day vulnerabilities.
4) **WIPS(Wireless Intrusion Prevention System)-** scans a **Wi-Fi network for unauthorized access** and removes any unauthorized devices.

Attacks detected and prevented by IPS:-

1) ARP Spoofing-type of attack in which a malicious actor sends falsified ARP
2) Buffer Overflow-occurs when the amount of data in the buffer exceeds its storage capacity.
3) DDoS (distributed denial-of-service (DDoS)
4) IP fragmentation
5) OS Fingerprinting

OS fingerprinting is the process a hacker goes through to determine the type of operating system being used on a targeted computer.

6)Ping of Death

disrupt a targeted machine by sending a packet larger than the maximum allowable size,

7)Port Scanning

8) Secure Socket Layer Evasion -is an encryption security protocol.

9)SYN flood- which aims to make a server unavailable to legitimate traffic

10)Smurf- which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

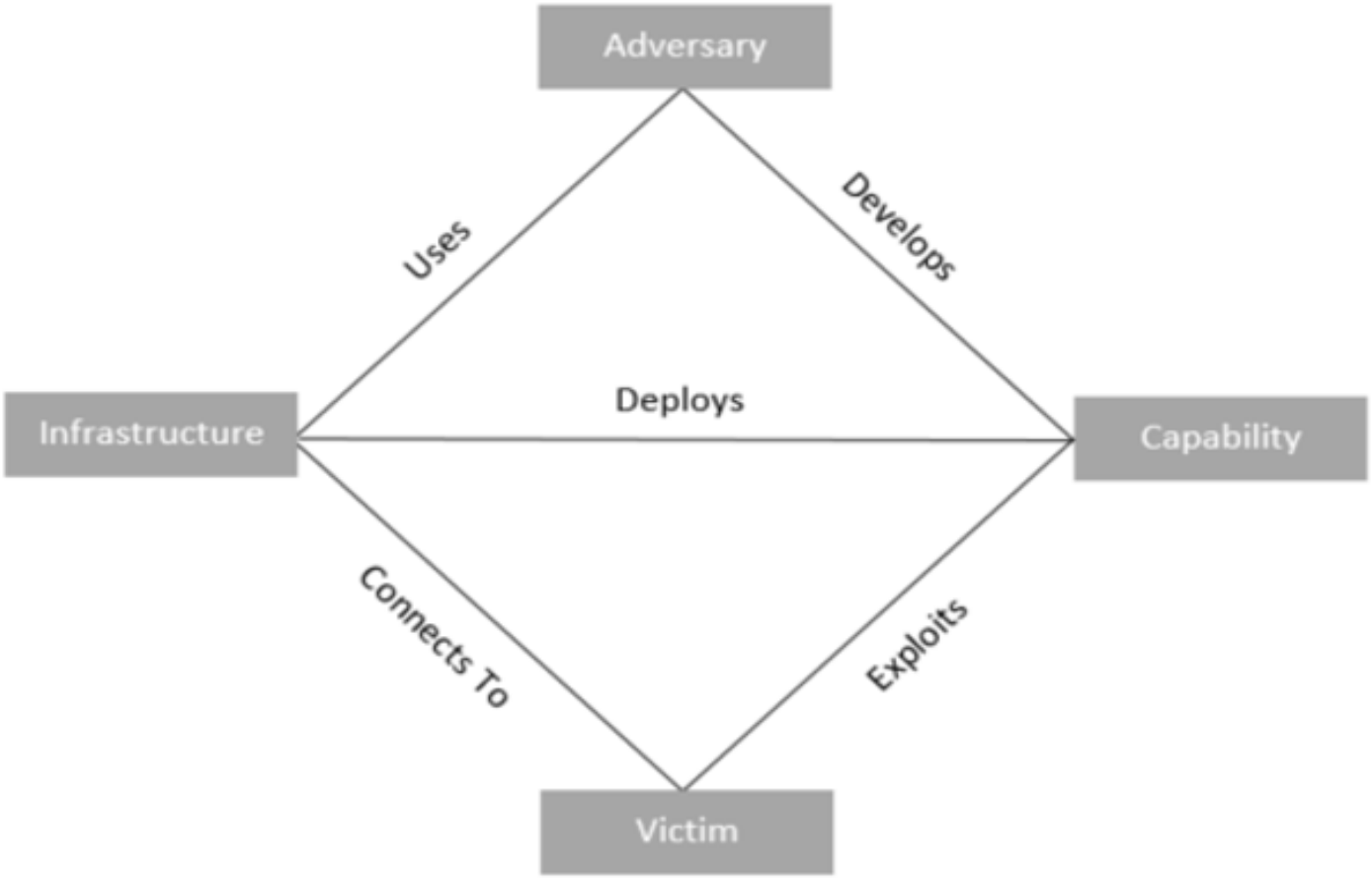
MODEL FOR INTRUSION ANALYSIS

- Any model of Intrusion Analysis is a cyber-security framework that helps organizations analyze **cyber intrusions**. The most common one is Diamond model of Intrusion Analysis.
- Main objectives are to identify specific attackers, understand the tactics, threats, and procedures they use, and more effectively respond to **cyber incidents** as they occur.
- It is simple but powerful model for intrusion analysis that fits right in between the Kill chain and Attack.
- This model is peculiar because it scrutinizes victimology and links the capabilities of the attacker to the infrastructure of the attack as well. It makes mitigation effective and the adversary's cost to operate more.

COMPONENTS OF MODEL

- Four main components of the Diamond Model of Intrusion are-

1. **Adversary:** The attacker or **group responsible** for a cyber incident.
2. **Infrastructure:** The technical resources or assets the **adversary uses during the attac**k (e.g., servers, domains, and IP addresses).
3. **Capability:** A method, tool, or technique the adversary uses during the attack (e.g., **malware or exploits**).
4. **Victim:** The **individual** or **organization** the adversary targets during the attack.



Diamond model for Intrusion Analysis

CONTT…

- There are also various relationships between components, including:

1. **Adversary-victim:** The **interaction between the attacker and target.** This relationship concerns questions such as why the attacker selected this target and **the attacker's motivations and objectives.**
2. **Adversary-infrastructure:** The attacker uses **various technical resources and assets**. This relationship concerns **how the attacker establishes and maintains its cyber operations**.
3. **Victim-infrastructure:** The target's connection to the attacker's technical resources. This relationship concerns the attacker's use of **various channels, methods, and vectors against the target.**
4. **Victim-capability:** The **target's connection to the attacker's tools and techniques**. This relationship concerns specific tactics and attack signatures used against the target.

CONTT…

- **Benefits of Using the Diamond Model:-**

The Diamond Model of Intrusion Analysis offers advantages such as:

- **Holistic understanding:** The Diamond Model examines the technical aspects of a **cyberattack and the human** and **organizational aspects**
- **Structured analysis:** The Diamond Model provides a clear, organized way for **cybersecurity experts to structure** and process data relating to **cyber threats and attacks**, making it easier to collaborate and share information.
- **Incident response and threat intelligence:** The Diamond Model offers benefits both for **threat intelligence (before an attack**) and **incident response (after an attack),** helping analysts collect and analyze valuable data.
- Particularly skillful at visualizing and understanding complex attack scenarios.

CONTT..

- The meta-features of the diamond model are listed as well-

1. **Timestamp**- Each event is notated with **a date and/or time** that it occurred
2. **Phase**- Malicious activity does not happen in a **single event** but **rather two or more.**
3. **Result**- While the results of an adversary's operations will not always be known, it is particularly useful to look across an adversary's operations to **determine their success rate** with **particular capabilities or against sets of victims**.
4. **Direction**- The direction of an event is **important for planning mitigation.** This is how the placement of detection mechanisms are planned. By knowing this adversary's activity direction over time, **better decisions can be made on which mechanism of detection** would work best to counter the adversary.

CONTT..

5. Methodology- The methodology meta-feature allows an **analyst** to describe the general **class of activity**.

6. Resources- The resources meta-feature lists one or more **external resources the event requires to be satisfied**..

7. Technology- The technology meta-feature **connects the infrastructure and capability and describes** the **technology enabling** the infrastructure and capabilities to interact effectively.