Diamond Model

## 📓 **Notes – Diamond Model**

**Lab Name:** Diamond Model

**Summary:**  
The **Diamond Model of Intrusion Analysis** is a framework for understanding and analyzing cybersecurity incidents by focusing on the relationships between four key elements of an intrusion: **Adversary, Capability, Infrastructure, and Victim**. It is widely used in threat intelligence and SOC investigations to structure analysis and identify attacker patterns.

**Four Core Features:**

1. **Adversary** – The threat actor or group conducting the intrusion.
2. **Capability** – The tools, malware, exploits, or techniques used.
3. **Infrastructure** – The physical or logical channels (servers, domains, IPs) used to deliver capabilities.
4. **Victim** – The target of the attack (person, organization, system).

**Additional Meta-Features:**

* **Timestamp** – When the activity occurred.
* **Phase** – Stage of the intrusion (mapped to Kill Chain/UKC).
* **Result** – Outcome of the action.
* **Direction** – Flow of the attack (e.g., inbound or outbound traffic).

**Practical Use in SOC Work:**

* Helps analysts connect indicators and understand how different parts of an attack are related.
* Assists in building threat profiles and mapping to MITRE TTPs.
* Allows defenders to disrupt the attack by targeting multiple elements (e.g., blocking infrastructure, detecting capabilities).

**Example:**

* **Adversary:** APT28
* **Capability:** Spear-phishing with malicious Excel macro
* **Infrastructure:** Compromised email server, C2 domain
* **Victim:** Financial department of a corporation

**Tools/Commands Used:**

* None in this lab; conceptual framework learning.

