CYBERSECURITY DAILY DIARY

DAY-11
DATE- 3 July, 2025

Topics Covered:

- Routing basics: static vs dynamic routing
- Inspect routing tables and perform traceroute analysis.

What did I learn:

Today I explored the core concepts of **routing**, which determine how packets travel across networks. Understanding both static and dynamic routing helped me see how devices make forwarding decisions and how I can trace those paths.

🔹 **Static vs Dynamic Routing**

- **Static Routing**: Manually configured routes that don't change unless edited. Great for small, predictable networks like my lab setup.
- **Dynamic Routing**: Uses protocols like **RIP, OSPF, and BGP** to automatically discover and update routes. Ideal for large, complex networks where paths may change frequently.

🔹 **Inspecting Routing Tables**

- I used commands like `route -n` and `ip route show` to view the routing table on my VM.
- Each entry shows:
  - **Destination network**
  - **Gateway**
  - **Interface**
  - **Metric** (cost of the route)
- This helped me understand how the system decides which path to use for outbound traffic.

🔹 **Traceroute Analysis**

- I ran `traceroute google.com` to observe how packets hop from my machine to the destination.
- Each line showed:
  - The IP of the router at that hop
  - Round-trip time (RTT)
  - Potential delays or unreachable nodes

- This tool is powerful for diagnosing routing issues, identifying bottlenecks, and visualizing how data flows across the internet.

Routing is the nervous system of networking. Now I can interpret routing decisions, simulate static routes in my lab, and use traceroute to analyze real-world traffic paths—skills that will be crucial for my cybersecurity project and threat detection work.