# FOOTPRINTING & RECONNAISSANCE

**Presented by:**

PANKAJ SINGH

**ROLL NUMBER** :2023A7R058

**DEPARTMENT** :CSE CYBER SECURITY

# What is Footprinting?

**Footprinting** :Footprinting is the process of gathering as much information as possible about a target system, organization, or individual—often as the first step in a cyber attack or security audit.

**Purpose:**

- Understand the target's digital footprint
- Identify vulnerabilities without triggering defenses

# Real-World Scenario

**Case Study:**

An attacker uses LinkedIn to find employee roles, and Shodan to map exposed devices. They craft phishing emails based on job titles and breach the internal network through an exposed RDP port.

# Types of Reconnaissance

**1. Passive Reconnaissance:**

- No direct interaction
- Uses publicly available sources (WHOIS, Google, social media)

**2. Active Reconnaissance:**

- Directly interacts with the target (ping sweeps, port scans)
- Higher risk of detection

# Tools & Techniques

**Passive Tools:**

- Maltego, Google Hacking, Shodan

**Active Tools:**

- Nmap, Netcat,

**Techniques:**

- DNS interrogation
- WHOIS lookups
- Social engineering

# Countermeasures

## Countermeasures

- Regular audits of public data and assets
- Restrict exposure of DNS and WHOIS information
- Train staff on social engineering risks
- Use Intrusion Detection Systems (IDS)
- Monitor for abnormal scanning behaviors