Day 9: Understanding Access, Its Types & Tools in Kali Linux

Date:4/07/25

Today, our session focused on the concept of **access** in the field of cybersecurity, particularly from the perspective of penetration testing and system administration using **Kali Linux**. We explored how unauthorized or authorized access plays a critical role in the security domain and learned about several tools in Kali Linux used to manage and exploit access levels.

Key Concepts Covered:

1. **What is Access?**
    - Access refers to the ability to interact with system resources (data, services, applications).
    - It can be physical (direct system access) or logical (network/system-based).
2. **Types of Access:**
    - **User Access:** Access given to general users.
    - **Administrative Access:** Full control over systems/settings.
    - **Remote Access:** Accessing systems over a network (e.g., SSH, RDP).
    - **Unauthorized Access:** Illegal/unauthorized entry into a system.
3. **Access Control Models:**
    - **MAC (Mandatory Access Control)**
    - **DAC (Discretionary Access Control)**
    - **RBAC (Role-Based Access Control)**
4. **Tools in Kali Linux for Access:**
    - **Hydra:** Password cracking tool for login services.
    - **Medusa:** Parallel login brute-forcer.
    - **Metasploit:** Framework for finding vulnerabilities and gaining access.
    - **SSH & Telnet Clients:** For accessing remote systems.
    - **Ncrack:** Network authentication cracking tool.
    - **John the Ripper:** Password cracking tool.

Day 10: Introduction to Cyber Laws

Date: 5/07/25

On Day 10, we shifted from technical skills to the **legal framework** surrounding cybersecurity. The session was focused on understanding **Cyber Laws**, their importance, and how they protect individuals, organizations, and governments in the digital world.

Key Concepts Covered:

1. **What are Cyber Laws?**
    - Laws that govern internet usage and digital communication.
    - Protects against cybercrimes like hacking, data theft, phishing, etc.
2. **Need for Cyber Laws:**
    - To protect privacy and data.
    - To define punishable offenses.
    - To regulate online business and digital transactions.
3. **Important Cyber Laws in India (as per the IT Act 2000):**
    - **Section 43:** Penalty for damage to computer system without permission.
    - **Section 66:** Hacking and identity theft.
    - **Section 67:** Publishing obscene content online.
    - **Section 69:** Government's power to intercept, monitor or decrypt data.
4. **Types of Cybercrimes:**
    - Unauthorized access
    - Cyberstalking
    - Phishing
    - Identity Theft
    - Online frauds and scams
5. **Agencies Involved in Cyber Law Enforcement:**
    - **CERT-In** (Indian Computer Emergency Response Team)
    - **Cyber Crime Cells** in Police Departments
    - **NCIIPC** (National Critical Information Infrastructure Protection Centre)