"CyberSec 100: MasteringCybersecurity in 100 Days"aa

“CyberSec 100: Mastering Cybersecurity in 100 Days”

Introduction to Cybersecurity (Days 1-10)

Day 1-2: Cybersecurity Fundamentals

Introduction to Cybersecurity:

- Definition and importance of cybersecurity
- Overview of the evolving cyber threat landscape

Cybersecurity Principles:

- CIA Triad (Confidentiality, Integrity, Availability)
- Defense-in-Depth strategy
- Least Privilege and Need-to-Know principles

Common Cyber Threats:

- Malware:
    - Definition and types (viruses, worms, trojans, ransomware)
    - How malware infects and spreads
- Social Engineering:
    - Types of social engineering attacks (phishing, pretexting, tailgating, etc.)
    - Manipulation of human psychology
- Hacking and Exploits:
    - Types of hackers (black hat, white hat, gray hat)
    - Exploiting vulnerabilities (zero-day exploits, backdoors)
- Denial-of-Service (DoS) Attacks:
    - DoS vs. DDoS attacks
    - Overloading systems to disrupt services
- Insider Threats:
    - Types of insider threats (malicious, unintentional)
    - Protecting against insider attacks

Security Measures and Technologies: