Cyber Security & Ethical Hacking Internship

Task-1: Threat Intelligence Report (2024–2025)

Prepared by: Your Name

1. Introduction to Cybersecurity

Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks. It is essential for individuals and organizations because modern life depends heavily on digital platforms, cloud computing, online banking, and AI-powered systems. As cyber crimes increase globally, businesses face risks such as financial loss, reputational damage, and operational downtime. With AI-driven threats emerging, proactive cybersecurity strategies are more important than ever.

AI-Powered Phishing Attacks

AI-driven phishing uses deepfake voice, realistic emails, and social engineering to trick victims into sharing credentials or money. Example: Deepfake CEO scam cases (2024). Prevention: MFA, employee awareness training, email filtering.

Ransomware-as-a-Service (RaaS)

RaaS allows criminals to buy ransomware kits. Example: WannaCry & LockBit campaigns. Impact includes data encryption and financial extortion. Prevention: Regular backups, patch management, endpoint security.

Cloud Security Misconfiguration

Improper cloud settings expose sensitive data. Example: Capital One breach (2019). Prevention: IAM best practices, encryption, cloud audits.

IoT Vulnerabilities

Smart devices often lack security updates. Example: Mirai Botnet attack. Prevention: Firmware updates, network segmentation, strong passwords.

Zero-Day Exploits

Unpatched vulnerabilities exploited before fixes are released. Example: SolarWinds supply chain attack. Prevention: Zero Trust model, rapid patching, IDS/IPS monitoring.

6. Conclusion & Future Scope

Cyber threats continue to evolve rapidly with advancements in AI and cloud technologies. Organizations must adopt proactive security strategies including Zero Trust architecture, continuous monitoring, employee training, and strong governance policies. Continuous learning and staying updated with threat intelligence reports are essential for cybersecurity professionals.