Cyber Security: Threat Analysis and Mitigation

Page 1 – Cover Page - **Project Title:** Cyber Security: Threat Analysis and Mitigation - **Subtitle:** A Professional Corporate-Style Project - **Author:** Vadde Adikesava - **Organization:** TCS-style - **Date:** December 2025 - **Logo:** [Placeholder]

Page 2 – Certificate / Acknowledgement This is to certify that the project entitled "Cyber Security: Threat Analysis and Mitigation" has been completed under guidance and supervision and is submitted for professional evaluation.

Acknowledgements to mentors, team members, and tools used for project implementation.

Page 3 – Abstract / Executive Summary Cyber Security is essential in protecting systems, networks, and data from digital threats. This project explores the types of cyber attacks, demonstrates practical mitigation strategies using tools like Wireshark, Nmap, and Python scripts, and provides analysis of potential vulnerabilities in network systems.

Page 4 – Introduction Cyber Security involves protecting digital assets against unauthorized access, theft, or damage. Key areas include network security, application security, information security, endpoint security, and cloud security.

The project emphasizes real-world impact and demonstrates practical approaches to prevent cyber threats.

Page 5 – Objectives of the Project 1. Identify common cyber threats. 2. Analyze system and network vulnerabilities. 3. Demonstrate mitigation strategies. 4. Provide practical examples using tools and scripts.

Page 6 – Methodology Steps Followed: 1. Data collection and threat scenario analysis. 2. Network/ system scanning. 3. Vulnerability analysis. 4. Threat mitigation demonstrations.

Tools Used: - Wireshark (Network traffic analysis) - Nmap (Network scanning) - Metasploit (Penetration testing) - Python scripts (Automation and analysis)

Page 7 – Implementation / Practical Examples Python Script Example:

```python
import socket

target = '127.0.0.1'
ports = [22, 80, 443]
```

```
for port in ports:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1)
    result = sock.connect_ex((target, port))
    if result == 0:
        print(f'Port {port} is open')
    else:
        print(f'Port {port} is closed')
    sock.close()
```

Diagram Example: - Include a network topology diagram showing monitored devices and firewalls.

Page 8 – Graphs & Analysis Example Graphs: 1. Pie chart showing distribution of cyber attack types. 2. Bar graph showing frequency of vulnerabilities discovered.

(Use matplotlib in Python to generate graphs for PDF)

Page 9 – Conclusion & Future Scope - Summary: Project highlights the importance of Cyber Security and demonstrates practical mitigation strategies. - Future Scope: Incorporate AI-based threat detection, focus on cloud security, automate vulnerability scanning.

Page 10 – References / Bibliography 1. Stallings, William. *Cybersecurity Essentials*, Pearson, 2021. 2. https://owasp.org 3. https://www.cisa.gov/cybersecurity 4. Tool documentation: Wireshark, Nmap, Metasploit, Python libraries

---

Note: This content is ready to be converted into a professional 10-page PDF with diagrams and code snippets included.