ETHICAL HACKING & CYBERSECURITY COURSE

MARUTHI TECHNOLOGIES
TRAINING STAFFING DEVELOPMENT

PREPARED BY :
Prathik Parsi

VISION AND MISSION

VISION

Empowering ethical hacking students to become pioneers in cybersecurity, fostering a safer digital world through innovation, integrity, and expertise.

MISSION

Our mission is to provide comprehensive education and practical training to aspiring ethical hackers, equipping them with the skills and knowledge needed to defend against cyber threats ethically. We aim to cultivate a community of ethical hackers committed to continuous learning, ethical conduct, and global collaboration in safeguarding digital assets and privacy.

ETHICAL HACKING COURSE SYLLABUS - 2024 EDITION

Target Audience
Individuals interested in learning the principles and practices of ethical hacking for security testing and vulnerability assessments. This syllabus is relevant for both beginners and those with some IT security knowledge.

Objectives

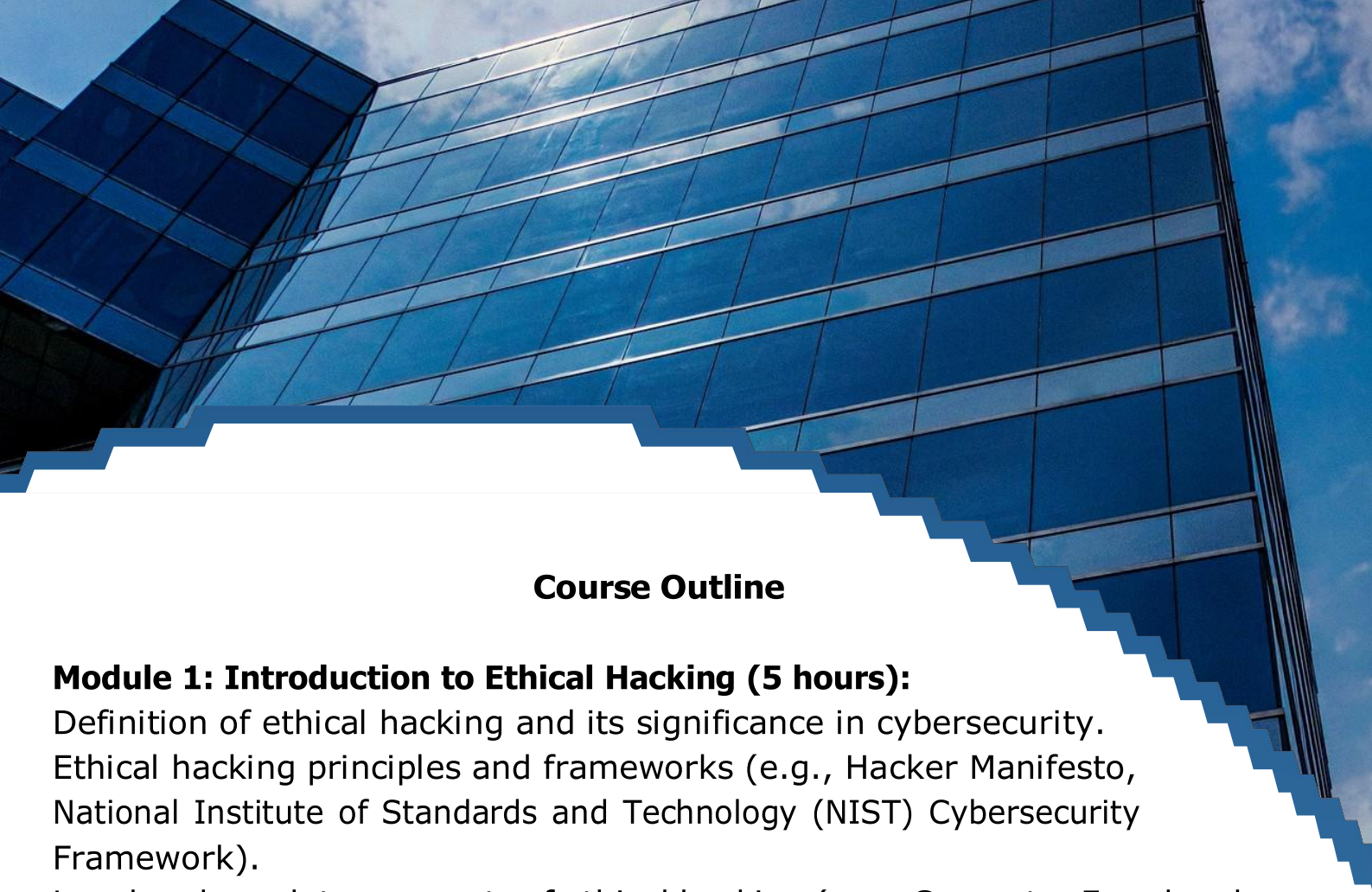
- Understand the concepts and principles of ethical hacking.
- Master essential tools and techniques used in ethical hacking.
- Learn to perform ethical hacking engagements according to industry best practices.
- Develop critical thinking and problem-solving skills for identifying and mitigating security vulnerabilities.
- Prepare for industry-recognized ethical hacking certifications like CEH or OSCP (optional).

Course Duration: 65-90 hours (adjust based on desired depth and content)

Course Overview
This course is designed to provide students with a thorough understanding of ethical hacking principles and techniques. Through a combination of theoretical knowledge and hands-on practice, students will learn how to identify vulnerabilities, exploit weaknesses, and strengthen cybersecurity defenses ethically. By the end of the course, students will be equipped with the skills necessary to pursue a career in ethical hacking and contribute positively to the cybersecurity field.

Practical Projects and Labs
Throughout the course, students will engage in hands-on labs and practical projects to reinforce their learning. Projects may include conducting penetration tests on simulated environments, developing custom tools/scripts, and performing real-world ethical hacking scenarios.

Students will be assessed through a combination of quizzes, practical assignments, lab exercises, and a final project. Participation and engagement in class discussions and activities will also be taken into consideration for grading



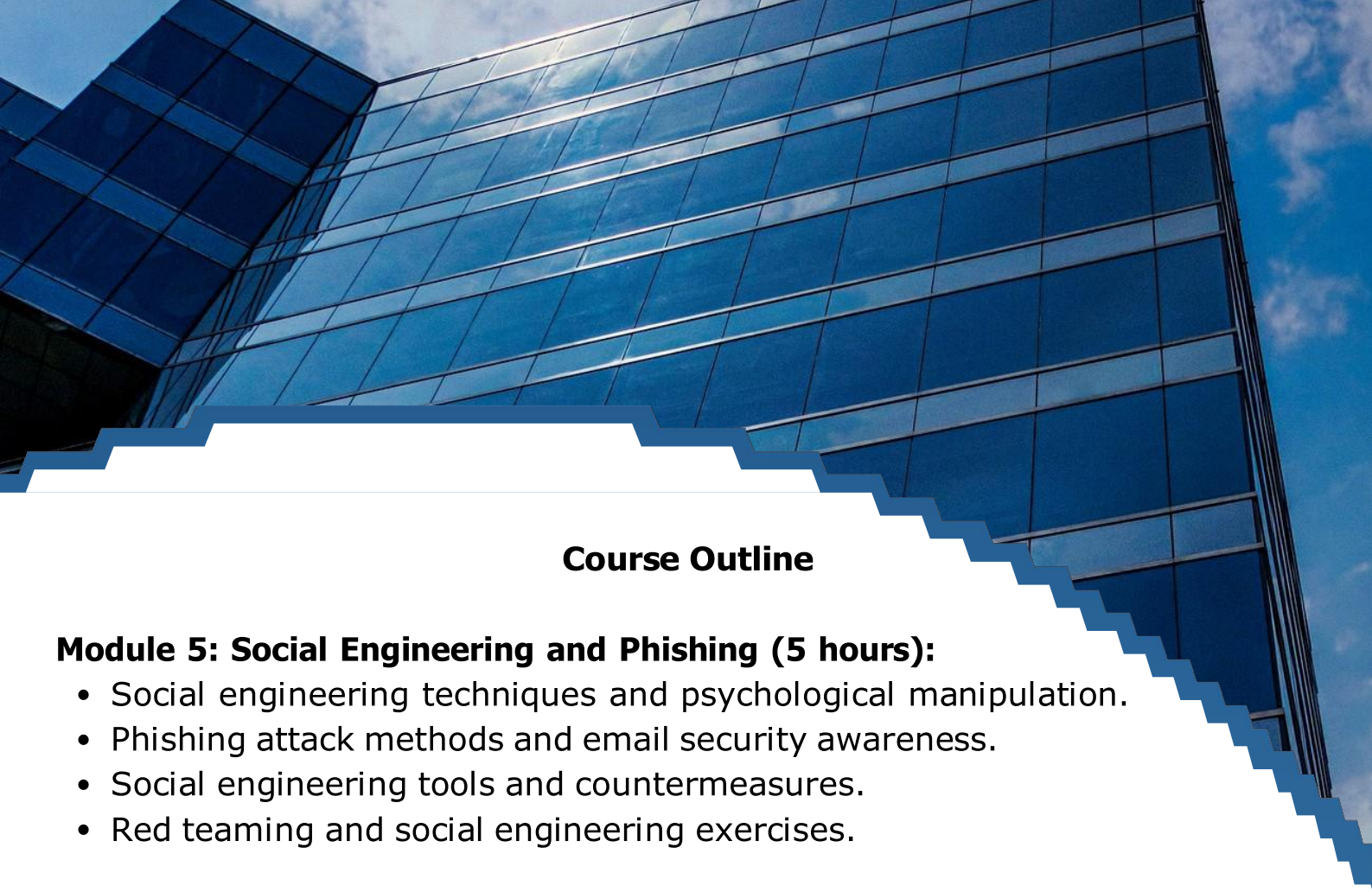
Course Outline

Module 1: Introduction to Ethical Hacking (5 hours):
Definition of ethical hacking and its significance in cybersecurity.
Ethical hacking principles and frameworks (e.g., Hacker Manifesto, National Institute of Standards and Technology (NIST) Cybersecurity Framework).
Legal and regulatory aspects of ethical hacking (e.g., Computer Fraud and Abuse Act, Digital Millennium Copyright Act).
Understanding the hacker mindset and attack methodologies.

Module 2: Network Security Fundamentals (5 hours):
OSI and TCP/IP network models.
IP addressing and subnetting.
Common network protocols and their vulnerabilities.
Network reconnaissance and scanning techniques (e.g., Nmap, Netcat).
Port scanning and vulnerability scanning.

Module 3: System Security Fundamentals (5 hours):
Operating system vulnerabilities and exploits.
Windows and Linux security concepts.
User account security and password cracking.
Privilege escalation techniques.
System hardening and mitigation strategies.

Module 4: Web Application Security (15 hours):
Common web application vulnerabilities (e.g., SQL injection, XSS, CSRF).
Web application scanning and fuzzing tools (e.g., Burp Suite, OWASP ZAP).
Manual web application penetration testing techniques.
Secure coding practices and web application firewalls.



Course Outline

Module 5: Social Engineering and Phishing (5 hours):

- Social engineering techniques and psychological manipulation.
- Phishing attack methods and email security awareness.
- Social engineering tools and countermeasures.
- Red teaming and social engineering exercises.

Module 6: Cloud Security (5 hours):

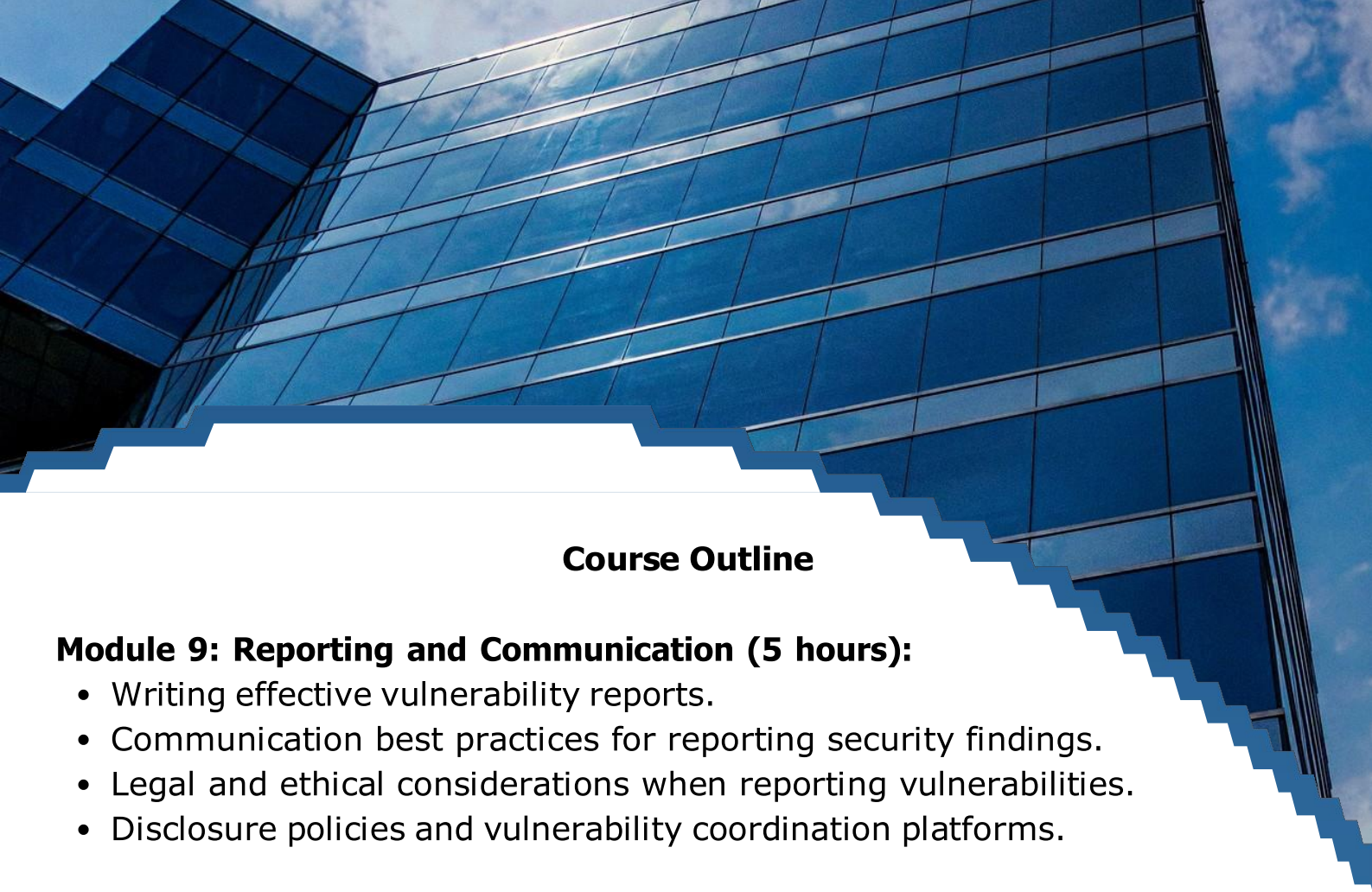
- Cloud security fundamentals and shared responsibility model.
- Common cloud security risks and vulnerabilities.
- Securing cloud workloads and storage.
- Cloud penetration testing methodologies.

Module 7: Offensive Security Tools and Techniques (15 hours):

- Introduction to scripting languages like Python for automation.
- Kali Linux as an ethical hacking platform.
- Command-line tools for network and system exploration (e.g., Metasploit, Netcat).
- Open-source intelligence (OSINT) techniques for gathering information.

Module 8: Post-Exploitation and Privilege Escalation (5 hours):

- Maintaining access and escalating privileges on compromised systems.
- Lateral movement techniques and post-exploitation frameworks.
- Covering tracks and evidence removal.
- Incident response and remediation strategies.



Course Outline

Module 9: Reporting and Communication (5 hours):

- Writing effective vulnerability reports.
- Communication best practices for reporting security findings.
- Legal and ethical considerations when reporting vulnerabilities.
- Disclosure policies and vulnerability coordination platforms.

Final Project (25 hours):

- Conduct a simulated ethical hacking engagement on a defined target system or application.
- Apply the learned techniques to identify, exploit, and document vulnerabilities.
- Provide a comprehensive report detailing the findings and recommendations.
- Present the project findings to the class and defend your methodology.

Disclaimer This syllabus is provided for informational purposes only and does not constitute a guarantee of any specific outcome. Participants are responsible for adhering to all applicable laws and regulations when practicing ethical hacking.

Additional Considerations:

Capture the Flag (CTF) exercises: Integrate CTF challenges throughout the course to provide practical application of learned skills.
Guest speakers from industry: Invite ethical hackers, security professionals, and bug bounty hunters to share their experiences.
Hands-on labs and projects: Offer additional challenges and projects beyond the core curriculum for self-driven learning.

THANK YOU

Thank you for embarking on this journey with us to explore the exciting world of ethical hacking.

We are confident that the knowledge and skills gained throughout this course will empower you to make a positive impact in the cybersecurity domain.

As we conclude this syllabus overview, we extend our sincere gratitude for your dedication and enthusiasm.

Should you have any questions or require further assistance, please do not hesitate to reach out to our support team.

We wish you all the best as you embark on this learning adventure, and we look forward to seeing you excel in the field of ethical hacking!

MARUTHI TECHNOLOGIES

TRAINING STAFFING DEVELOPMENT