# Ethical Hacking & Cyber Security Workshop

By Techgyan Technologies

## Introduction to the Workshop

Welcome to the Ethical Hacking & Cyber Security Workshop presented by Techgyan Technologies. This workshop is designed to immerse participants into the dynamic world of cybersecurity and ethical hacking, providing a thorough grounding in fundamental and advanced topics. Our experienced facilitators will guide you through a series of interactive sessions that include both theoretical foundations and practical hands-on exercises. Prepare to engage with other cybersecurity enthusiasts and professionals, enhancing your understanding and skills in protecting digital assets against ever-evolving threats.

## Who Should Attend This Workshop

This workshop is tailored for a diverse audience, including:

- **IT Professionals**: System administrators, network engineers, and other IT staff who are responsible for protecting organizational IT infrastructure.
- **Aspiring Security Professionals**: Individuals looking to start or transition their career into cybersecurity.
- **Students**: Those studying in IT, computer science, or related fields who want a practical, real-world understanding of cybersecurity challenges and solutions.
- **Business Managers**: Decision-makers who need to understand the implications of cybersecurity on their business operations and how to implement effective security policies.

## Workshop Curriculum

### Welcome & Introduction (10 minutes)

- Introduction to the workshop, facilitators, and participants.
- Discussion of workshop objectives and expected outcomes.
- Icebreaker activity to share experiences with cybersecurity challenges.

### The Basics of Cybersecurity (20 mins)

- Introduction to the CIA Triad: Confidentiality, Integrity, and Availability.
- Risk management strategies in digital environments.
- Developing and adhering to robust security policies.

### Phases of Hacking (30 mins)

- Reconnaissance: Techniques such as footprinting, social engineering, and OSINT.
- Scanning: Using tools like Nmap and Nessus to identify vulnerabilities.
- Hands-on activity to practice reconnaissance on a set target.

### Reconnaissance Techniques (30 mins)

- Deep dive into the Google Hacking Database and Google Dorks.
- Exploring other tools like Shodan and Maltego.
- Practical exercise using GHDB to locate vulnerable systems.

### Scanning and Enumeration (30 mins)

- Advanced scanning techniques and network enumeration.
- Demonstrations of different Nmap scans.
- Hands-on scanning exercise and result analysis.

### System Hacking (90 minutes)

- Exploring vulnerabilities in Windows and Linux systems.
- Hands-on password cracking and backdoor utilization.

### Social Engineering (30 mins)

- Social engineering techniques and psychological tactics.
- Developing defensive strategies against social engineering.
- Hands-on phishing simulation.
- Discussion on ethical dilemmas and legal boundaries.

### Web Application Security (120 minutes)

- Understanding common web vulnerabilities: SQL injection, XSS, CSRF.
- Manual testing and exploitation of web applications.
- Hands-on session exploiting a vulnerable web application.

## Outcomes of the Workshop

By the end of this workshop, participants will be able to:

1. **Understand the Core Principles of Cybersecurity**: Grasp the essential concepts of the CIA Triad—Confidentiality, Integrity, and Availability—and how they form the foundation of any security strategy.
2. **Identify and Mitigate Risks**: Learn to use tools like Nmap and Nessus for vulnerability scanning and develop strategies for risk management in digital environments.
3. **Execute Effective Reconnaissance**: Master techniques in footprinting, social engineering, and using advanced tools such as the Google Hacking Database and Shodan.
4. **Gain Practical Hacking Skills**: Perform hands-on hacking exercises, including system hacking, password cracking, and exploiting web applications to understand the hacker mindset and methodology.
5. **Defend Against Social Engineering Attacks**: Develop strategies to counteract psychological tactics employed by social engineers and conduct a phishing simulation.
6. **Navigate Ethical and Legal Boundaries**: Discuss the ethical dilemmas and legal aspects of hacking to ensure responsible use of the skills learned.

## How to Continue Learning in the Future

To further your journey in ethical hacking and cybersecurity, consider the following avenues:

- **Certifications**: Pursue certifications like Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), or CompTIA Security+ to validate your skills and advance in your career.
- **Online Platforms**: Engage with online learning platforms that offer advanced courses and up-to-date materials on cybersecurity trends and tools.
- **Communities and Forums**: Join cybersecurity forums and online communities to stay connected with like-minded professionals and keep abreast of the latest threats and defenses.
- **Practice Labs**: Utilize platforms such as Hack The Box or OverTheWire to practice your skills in a safe and legal environment.
- **Conferences and Seminars**: Attend industry conferences and seminars to network with other professionals and learn from experts in the field.