Cyber Clash Competition: Official Rule Book

1. Introduction

Welcome to the **Cyber Clash Competition**! This event is designed to test participants' cybersecurity skills in a simulated attack-and-defense scenario. Teams will take on both offensive and defensive roles, identifying vulnerabilities and protecting critical systems. The competition aims to assess participants' knowledge in ethical hacking, penetration testing, and defensive cybersecurity strategies.

2. Event Details

- **Event Dates**: October 12-13, 2024
- **Location**: Expo Center, Karachi
- **Competition Duration**: 4 hours total
- **Schedule**:
  - **Round 1**: Red Team attacks, Blue Team defends (1.5 hours)
  - **Break/Role Switch**: 30 minutes
  - **Round 2**: Blue Team attacks, Red Team defends (1.5 hours)
  - **Briefing Session**: 30 minutes before the competition

3. Objectives

Participants will be divided into Red Teams (Attackers) and Blue Teams (Defenders) and will:

1. Simulate real-world attack-and-defense cybersecurity scenarios.
2. As Red Team, attempt to exploit vulnerabilities in the system.
3. As Blue Team, protect and defend a network infrastructure against attacks.
4. Gain points based on their success in exploiting or defending the system during the competition.
5. Learn and apply tools and techniques used in cybersecurity fields such as penetration testing, network defense, and ethical hacking.

4. Eligibility

1. **Participants**: Open to teams of 4 members, including students, professionals, or cybersecurity enthusiasts.
2. **Affiliations**: No restrictions based on academic or professional background.
3. **Knowledge Requirements**: Basic understanding of cybersecurity, ethical hacking, and penetration testing.

5. Tools and Deliverables

1. **Tools Allowed**:
   - **Red Team (Attackers)**: Tools like Nmap, Metasploit, Wireshark, Burp Suite, John the Ripper, etc.
   - **Blue Team (Defenders)**: Tools like Snort, Splunk, ELK Stack, OSSEC, Wireshark, Fail2Ban, etc.
   - Additional tools can be approved by the organizers if necessary.
2. **Environment**:
   - A virtual environment simulating a network with various security levels will be provided.
   - Teams will connect remotely via their own laptops to the virtual infrastructure.
3. **Deliverables**:
   - Attack/defense plans and strategies for each round.
   - Performance reports and documentation summarizing the team’s approach, results, and lessons learned from the competition.

6. Competition Format

1. **Round 1**: Red Team attacks, Blue Team defends (1.5 hours)
   - The Red Team will attempt to exploit the vulnerabilities in the system, while the Blue Team will defend the infrastructure.
2. **Break and Role Switch**: 30 minutes
   - Teams will switch roles, allowing the Blue Team to become attackers and the Red Team to defend.
3. **Round 2**: Blue Team attacks, Red Team defends (1.5 hours)
   - Teams will switch roles, and the new Red Team will attack while the new Blue Team defends.

7. Judging Criteria

1. **Red Team (Attackers)**:
   - Points for discovering and successfully exploiting system vulnerabilities.
   - Bonus points for advanced exploits such as privilege escalation and accessing deeper layers of the infrastructure.
2. **Blue Team (Defenders)**:
   - Points for detecting and preventing attacks.
   - Points for timely and effective incident response.
   - Bonus points for creative and innovative defense mechanisms.
3. **Penalties**:
   - **Red Team**: Points deducted for being detected or using unauthorized tools.
   - **Blue Team**: Points deducted for failure to detect or delay in responding to attacks.
4. **Ethical Violations**:
   - Any team caught using unethical tools or harmful tactics (e.g., malware, DoS attacks) will face immediate disqualification.

8. Code of Conduct

1. **Fair Play**: Participants must adhere to ethical standards and professionalism.
2. **Respect**: Respect all participants, judges, and organizers throughout the event.
3. **Collaboration**: Each team member must actively contribute to their team's success.

9. Resources and Support

1. **Hardware**: Participants must bring their own laptops capable of running cybersecurity tools.
2. **Software**: A virtual environment will be provided for attack/defense simulation.
3. **Support**: On-site technical assistance will be available for any issues during the competition.

10. Prizes and Recognition

1. **Awards**: Prizes will be awarded to the top 3 teams based on their final scores.
2. **Recognition**: Winners will be highlighted on the event's official platforms and may receive certificates or trophies.

11. Disqualification and Appeals

1. **Disqualification**: Teams will be disqualified for any form of cheating, using unauthorized tools, or violating competition rules.
2. **Appeals**: Teams may appeal decisions by submitting a formal request to the competition committee, whose decision will be final.

12. Important Dates

- **Competition Dates**: October 12-13, 2024

13. Contact Information

For questions or further details, please contact us at:

- **Email**: contact@teknofestpakistan.com
- **Website**: www.teknofestpakistan.com
- **Phone:** +92 315 8508658 | +92 336 8285328

Good luck to all participants! We look forward to seeing your cybersecurity skills in action