Inter College Skills Competition 2026

IMINGS	ACTIVITY
9:00	Industry Judges arrive at host sites.
9:15	Welcome speech given by guest judges / visitor
10:00	Competitions start **promptly**.
1:00 - 2:00	Lunch break/Network (provided for visiting students and judges by the host college).
2:00 - 3:00	Competition wrap-up: Judges and teaching teams share feedback with competitors.
3 – 3.30	Closing from host

Cyber Security Challenge 2025: "Defend and Attack"

Team Size: 3 participants per team
Duration: 3 hours **– 10am – 1pm.**

Objective:
Your team has been recruited as Cyber Security Consultants to investigate security breaches at CyberCorp Ltd. and propose cyber security improvements. You will conduct vulnerability assessments, penetration testing, security hardening, and policy development, culminating in a final report and presentation.

Scenario
CyberCorp Ltd. has suffered multiple cyber-attacks due to outdated security measures. These attacks have resulted in data leaks, unauthorised access, and potential financial losses. Your task is to analyse the company's security process, identify vulnerabilities, implement defensive strategies, and conduct controlled penetration testing to simulate a real-world cyber security incident.

Challenge Breakdown & Assessment Criteria
Your performance will be assessed across seven key areas, ensuring you demonstrate research, technical skills, security best practices, and communication abilities.

🔍 **Phase 1: Research & Intelligence Gathering**

- Investigate current cyber threats, real-world breaches, and industry security trends.
- Document your research, focusing on how cybercriminals exploit vulnerabilities.

🔹 **Assessment:** Teams will be judged on the depth and accuracy of their research, with strong justification for selected tools and techniques.

🛡 **Phase 2: IT Rules & Security Architecture Development**

- Define baseline and target security architectures for CyberCorp Ltd.
- Develop a minimum of 10 core IT security policies (e.g., password policies, firewall rules, user access controls).
- Justify how your architecture and policies enhance cyber security.

🔷 **Assessment:** Teams must create clear, well-structured policies with justified security improvements.

🔎 **Phase 3: Vulnerability Assessment**

- Set up your virtualized testing environment using VirtualBox/VMware, Kali Linux, and Metasploitable 2.
- Conduct a vulnerability scan using nmap.
- Identify critical weaknesses and document them with risk levels (e.g., High, Medium, Low).

🔹 **Assessment:** Teams will be marked on how well they identify vulnerabilities, categorise risks, and use appropriate scanning tools.

🔐 **Phase 4: Security Hardening & Countermeasures**

- Implement defensive measures such as:
  - Firewall configurations
  - Secure authentication methods
  - Least privilege access control
  - Encryption and patching recommendations
- Demonstrate how these measures reduce CyberCorp's risks.

🔹 **Assessment:** Teams must apply effective security measures and clearly justify their impact.

💻 **Phase 5: Ethical Hacking & Penetration Testing**

- Plan and execute an ethical hacking attempt using Metasploit and other penetration testing tools.
- Successfully exploit at least one vulnerability while documenting:
  - Attack methodology
  - Impact of the exploit
  - Steps for mitigation

Assessment: Teams are judged on how well they simulate an attack scenario, document exploits, and recommend fixes.

🔹

Defining a Successful Exploit

A "successful exploit" should demonstrate that the team has moved beyond simple vulnerability scanning and has the technical capability to leverage a weakness to gain control over the system, simulating a real-world breach.

A successful exploit requires two main components:
Execution of an attack: Successfully using an exploit module (likely via Metasploit) against one of the identified vulnerabilities.

Establishing a shell/session: Gaining an interactive command-line session (a "shell" or a Meterpreter session) on the Metasploitable 2 target.

Suggested Specific Levels of Access
To demonstrate a high level of proficiency and technical skill, the successful exploit must achieve one of the following specific levels of access on the target system. The highest level achieved should be documented in the final report:

Level of Access	Description of Success	Rationale
Minimum Success: User-Level Access	The team establishes a non-privileged shell (e.g.,	This confirms the vulnerability was

	a simple Linux terminal session) as a standard user on the target system (e.g., the *msfadmin* user).	successfully exploited and control was gained, fulfilling the base requirement to "Successfully exploit at least one vulnerability.
Target Success: Root/Administrative Access	The team establishes an elevated shell with root access (Linux) or Administrator access (if applicable) on the target system. This may require a separate privilege escalation step after gaining the initial user-level access.	Achieving root access demonstrates a deeper understanding of post-exploitation techniques and system compromise, which aligns with the highest marks in the grading rubric for penetration testing.
Advanced Success: Data Exfiltration/Persistence	The team demonstrates they can read a specific sensitive file (e.g., /etc/shadow) or implement a persistent backdoor on the system, in addition to gaining root access.	This simulates the true impact of a data leak or unauthorised access, as mentioned in the scenario, and shows a high level of mastery in the attack methodology.
The team must clearly **document** the attack methodology, the impact of the exploit, and the steps for mitigation for the vulnerability they successfully exploited. Gaining and demonstrating **Root/Administrative** access should be the key goal for top marks.		

Phase 6: Report Writing & Presentation

- Compile a professional cyber security report, including:
  - Summary of security risks
  - Findings from penetration testing
  - Security improvement recommendations
- Deliver a 5-minute presentation summarising your findings.

🔹 **Assessment:** Teams will be marked on clarity, structure, technical accuracy, and professionalism.

🤝 **Phase 7: Teamwork & Problem-Solving**

- Collaborate effectively, demonstrating clear team roles.
- Troubleshoot problems efficiently and apply logical reasoning.
- Adapt to challenges and propose innovative security solutions.

🔹 **Assessment:** Judges will evaluate communication, problem-solving strategies, and teamwork dynamics.

🏆

Scoring & Awards as Marking Grid
Category

- Research & Intelligence Gathering
- IT Rules & Security Architecture
- Vulnerability Assessment
- Security Hardening & Countermeasures
- Penetration Testing Execution
- Report Quality & Presentation
- Teamwork & Problem-Solving

🛠 Required Setup
Participants will have access to the following:

- VirtualBox 7 *(https://www.virtualbox.org/)* OR VMware Workstation 17 *(https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-nowavailable-free-for-personal-use.html)*
- Kali Linux 2024.2 *(https://www.kali.org/get-kali/#kali-installer-images)* . (nmap is included)
- Metasploitable 2 *(https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)*

SUBMISSIONS – follow close attention to the information below.

STRUCTURE OF FINAL REPORT

Maximum 15 pages for the final report, excluding appendices and cover page.

Introduction/Scope (CyberCorp Scenario)
Phase 1: Research & Intelligence Findings
Phase 2: Security Architecture & Policy Summary
Phase 3: Vulnerability Assessment Findings (with Risk Register)
Phase 4: Hardening/Countermeasure Implementation
Phase 5: Penetration Testing Methodology & Results
Phase 7: Teamwork Reflection
Conclusion & Final Recommendations

Presentation - Max 10 slides, submitted as a PPTX.

Both documents are to be zipped together and use your student ID and college name as the file name. *Example- **10235672_CollegeName**.zip.* This is to be submitted at the completion of the competition. How this is done will depend on the college but in some cases it could could be to safe cloud storage such as GDrive, OneDrive.

1. IT Rules and Security Architecture Development

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Understanding and Application of IT Rules and Requirements	Demonstrates a **deep understanding** of IT rules and requirements. Accurately defines **baseline and target architectures** with clear, valid justifications for all decisions.	Demonstrates a **good understanding** of IT rules and requirements. Defines baseline and target architectures, but justifications are limited or lack depth.	Demonstrates a **basic understanding** of IT rules. Defines baseline and target architectures with noticeable gaps or unclear justifications.	Fails to demonstrate understanding of IT rules or define appropriate architectures. Justifications are missing or invalid.
Policy Creation and Structure	Creates **10 or more policies** that are clear, well-structured, specific, and actionable. Policies directly address CyberCorp's needs and align with industry standards.	Creates **8-9 policies** that are mostly clear and actionable. Minor gaps in structure or relevance to CyberCorp's needs.	Creates **5-7 policies** that are vague, generic, or not fully actionable. Some policies may not address CyberCorp's needs.	Creates fewer than 5 policies, or policies are unclear, generic, or irrelevant.

2. Research and Intelligence Gathering

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Research Depth and Relevance	Research is **comprehensive**, addressing current cyber threats, real-world breaches, and industry trends. Provides clear examples and explanations of how vulnerabilities are exploited.	Research is detailed but not fully comprehensive. Minor gaps or lack of examples, but findings are still relevant.	Research is basic, with limited focus on current threats or breach examples. Explanations are vague or incomplete.	Minimal or no research is presented. Fails to address relevant threats or vulnerabilities.
Selection and Justification of Tools/Techniques	Selects **appropriate tools and techniques** (e.g., nmap, Metasploit) with clear, logical justifications for their relevance to the task.	Selects appropriate tools and techniques but provides limited or unclear justifications.	Selects tools/techniques that are only partially relevant or lacks meaningful justification for their use.	Fails to select appropriate tools/techniques, or no justification is provided.

3. Vulnerability Assessment

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Identifying	Conducts a **detailed**	Conducts a	Conducts a basic	Fails to conduct

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Vulnerabilities	**vulnerability scan** using tools such as nmap. Identifies all critical, high, medium, and low risks with clear documentation of impact levels.	vulnerability scan and identifies most risks. Documentation is clear but lacks depth or minor vulnerabilities are missed.	scan but identifies only a few vulnerabilities. Documentation is incomplete or lacks detail.	a meaningful scan. No vulnerabilities are identified or documented.
Categorisation and Risk Levels	Accurately categorises risks into **High, Medium, and Low** with detailed, valid justifications for each.	Categorises risks with minor inaccuracies or vague justifications.	Categorises risks inconsistently or with limited justifications.	Fails to categorise risks or provide meaningful justifications.

4. Security Hardening and Countermeasures

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Implementation of Defensive Measures	Implements **at least 4 effective measures** (e.g., firewalls, encryption, access controls) with clear evidence of reduced risks. Justifications are detailed and align with industry standards.	Implements **3 defensive measures** effectively. Minor gaps in execution or justification, but measures are generally effective.	Implements **1-2 defensive measures**, but their execution or effectiveness is limited. Justifications are unclear.	Fails to implement meaningful defensive measures. No justifications are provided.

5. Penetration Testing

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Execution and Exploitation	Successfully **exploits at least one vulnerability**, achieving root/administrative access. Provides detailed documentation, including methodology, impact, and mitigation steps.	Successfully exploits a vulnerability but achieves only user-level access. Documentation is clear but lacks advanced detail.	Fails to exploit a vulnerability or demonstrates only basic scanning. Documentation is incomplete or lacks critical details.	No successful exploit demonstrated. Documentation is missing or irrelevant.
Demonstrating Advanced Success	Achieves **root/administrative access** and demonstrates additional success (e.g., data exfiltration or persistence). Documents advanced steps in detail.	Achieves root/administrative access but fails to demonstrate additional advanced success. Documentation is clear but basic.	Achieves user-level access without advanced success. Documentation lacks detail or clarity.	Fails to achieve either user-level or root access. No meaningful documentation of attempts.

6. Report Writing and Presentation

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Report Quality	Report is **professionally written**, well-structured, and free from errors. Includes actionable recommendations and detailed findings.	Report is well-written with minor errors or omissions. Recommendations are relevant but lack depth.	Report is basic, with significant errors or missing sections. Recommendations are vague or impractical.	Report is poorly written, incomplete, or unprofessional. Recommendations are missing or irrelevant.
Presentation Delivery	Presentation is **engaging, clear, and concise**, summarising all key findings within the time limit.	Presentation is clear but lacks engagement or exceeds the time limit slightly. Findings are mostly summarised.	Presentation is unclear or incomplete, with limited explanation of key findings. Delivery is inconsistent.	Presentation is poorly delivered, unfocused, or missing key findings. Exceeds time limit significantly.

7. Teamwork and Problem-Solving

Criteria	3 Marks - Advanced	2 Marks - Proficient	1 Mark - Developing	0 Marks - Beginning
Collaboration and Role Definition	Team members work **seamlessly**, with clear roles and responsibilities. Collaboration is effective and efficient.	Team members collaborate well, but roles and responsibilities are not always clearly defined.	Team collaboration is inconsistent, with unclear roles or communication issues.	Teamwork is poor, with significant miscommunication or lack of collaboration.
Problem-Solving and Adaptability	Demonstrates **logical reasoning** and innovative solutions to challenges. Adapts effectively to unexpected issues.	Demonstrates problem-solving skills but struggles with adaptability or innovation.	Problem-solving is basic, with limited adaptability to challenges.	Fails to demonstrate effective problem-solving or adaptability.