Proposals

Event: Black Box Breakdown

I. Event Description

Black Box Breakdown is a competitive event designed to challenge participants' analytical and logical reasoning skills through the principles of black box software testing. Contestants will conduct a systematic investigation of provided web applications without any access to the underlying source code.

The primary objective is to identify and document functional defects, logical inconsistencies, and usability issues at the user-interface level. This event requires no prior programming expertise, emphasizing methodical problem-solving and keen observational skills over technical knowledge. It serves as a practical introduction to Quality Assurance (QA) methodologies in a simulated, time-constrained environment.

II. Rules and Regulations

A. Team Composition

1. Each team must consist of two (2) to three (3) members.
2. All participants must be officially enrolled as first-year Bachelor of Technology students.

B. Technical Prerequisites

1. No specific technical or programming prerequisites are required for participation.

C. Equipment

1. This is a Bring Your Own Device (BYOD) event. Each team is required to have access to at least one laptop computer equipped with a modern web browser (e.g., Google Chrome, Mozilla Firefox, Microsoft Edge) and a stable internet connection.

D. Code of Conduct

1. All testing must be performed exclusively through the application's graphical user interface.
2. Collaboration or communication regarding the challenges with other teams is not permitted.
3. All findings must be submitted via the designated online submission portal provided by the event organizers.

III. Event Structure and Procedure

The event is structured into three progressive rounds.

Round 1: The Qualifier

- **Duration:** 30 Minutes
- **Objective:** To assess the team's fundamental ability to identify basic software defects.
- **Procedure:** All teams will be provided with a URL to a simple web application. Teams are required to identify and document a minimum of three (3) distinct, valid defects.
- **Reporting Protocol:** Each defect report must detail:

    - Steps to Reproduce
    - Expected Behavior
    - Observed Behavior
- **Progression Criteria:** Teams that successfully submit the required number of valid defects will advance to the subsequent round.

Round 2: The Gauntlet

- **Duration:** 60 Minutes
- **Objective:** To evaluate the team's ability to test a more complex system and identify defects of varying severity.
- **Procedure:** Qualifying teams will receive a URL to a multi-functional web application (e.g., an e-commerce order form). The objective is to identify and report as many unique defects as possible.
- **Reporting Protocol:** The standard reporting protocol remains in effect. Submissions will be evaluated based on both the quantity and quality of the findings.
- **Progression Criteria:** The top 4-6 teams, determined by the cumulative score of their findings, will advance to the final round.

Round 3: The Final Bug Bash

- **Duration:** 30 Minutes
- **Objective:** A real-time, competitive final stage to determine the event champion.
- **Procedure:** The final teams will assemble in a designated area. A final, previously unseen web application will be presented. Teams will compete to identify and report defects in real-time.
- **Scoring Protocol:**
    - Upon finding a defect, a team must signal an organizer for immediate verification.
    - Points will be awarded based on the defect's validity, severity, and the order of discovery.
    - A live leaderboard will display team scores.
- **Conclusion:** The team with the highest cumulative score at the conclusion of this round will be declared the winner.

IV. Judging Criteria

Submissions and performance will be evaluated based on the following criteria:

1. **Validity of Defect:** Whether the reported behavior is a genuine flaw or intended functionality.
2. **Severity and Impact:** The degree to which the defect negatively affects the application's functionality, security, or usability. Defects are categorized as High, Medium, or Low impact.
3. **Clarity and Quality of Documentation:** The precision and thoroughness of the defect report, enabling organizers to easily reproduce the issue. (Applicable to Rounds 1 & 2).
4. **Speed and Uniqueness (Final Round):** The timeliness of discovery and whether the defect was novel or previously reported by another team.

V. Grounds for Disqualification

Any team found in violation of the following rules will be subject to immediate disqualification:

- **Academic Misconduct:** Engaging in any form of cheating, including sharing information with other teams or using unauthorized external resources.
- **Unprofessional Conduct:** Any behavior deemed disruptive to the event or disrespectful towards organizers, judges, or fellow participants.

Event: Operation: Blackout

I. Event Description

Operation: Blackout - Live Threat is a real-time strategic wargame that places teams at the center of a unfolding cybersecurity crisis. As elite "IMF Cells," participants will engage in a head-to-head battle of wits, with one team orchestrating a sophisticated cyberattack on a nuclear power facility while the other mounts a desperate defense.

This is a turn-based interactive simulation. Teams will be given a limited budget of "Action Points" each round to execute offensive and defensive maneuvers from a strategic playbook. A central "Control" adjudicator will process these moves, determining their success and failure in real-time and updating the facility's status on a live dashboard. Success requires rapid thinking, resource management, and the ability to anticipate and counter your opponent's every move.

II. Rules and Regulations

A. Team Composition

1. Each participating unit, an "IMF Cell," must consist of two (2) to three (3) members.
2. All cell members must be officially enrolled as first-year Bachelor of Technology students.

B. Event Protocol

1. This is a live, turn-based strategy game. All actions are selected from a provided "Menu of Actions."
2. Internet access is permitted for research and strategic discussion.
3. Each team will be given a set number of **Action Points (AP)** per round to "purchase" their chosen maneuvers. Unspent AP does not carry over.
4. All moves are submitted secretly to "Control" at the end of each round's planning phase.
5. A live, projected dashboard will display the nuclear facility's status (e.g., Network Integrity, Power Grid Stability, Data Security), providing immediate visual feedback on the outcome of each round.

III. Event Structure and Procedure

The event is a single-elimination tournament. Each match consists of multiple, fast-paced rounds.

Phase 1: Strategic Briefing (15 Minutes)

- **Objective:** To analyze the mission dossier and formulate an initial strategy.
- **Procedure:** All teams receive the scenario details. In the tournament bracket, teams are paired and designated as either **Attack Cell** or **Defense Cell** for their first match.
- **Task:** Teams review the "Menu of Actions" and plan their opening moves.

Phase 2: Live Engagement (A Match consists of 3-5 Rounds)

- **Objective:** To achieve your cell's objective (sabotage or secure the facility) by outmaneuvering the opposition.
- **Round Structure (each round is ~10 minutes):**
    1. **Strategy Phase (5 mins):** "Control" announces the start of the round and allocates 10 Action Points to each cell. Teams secretly discuss and decide which actions to execute, noting their AP cost.
    2. **Submission Phase (1 min):** Each cell locks in their chosen actions for the round and submits them to "Control" via a provided form.
    3. **Resolution & Adjudication Phase (4 mins):**
        - "Control" reveals the actions chosen by both cells for all to see.
        - "Control" adjudicates the outcome, explaining how the moves interacted. For example: *"Attack Cell's 'Phishing Campaign' was countered by Defense Cell's 'Employee Training Drill.' However, Attack's 'Network Scan' was successful as Defense did not reinforce their firewall this round."*
        - The live dashboard is updated to reflect the new status. (e.g., "Network Integrity" might change from GREEN to YELLOW).
        - Points are awarded by "Control" based on the success of the actions.
- **Winning a Match:** The cell with the most points at the end of the final round wins the match and advances in the tournament.

Phase 3: The Final Confrontation

- **Objective:** The final match is an extended engagement with higher stakes.
- **Procedure:** The final two cells compete in a 5-round match. "Control" may introduce "live injects"—sudden scenario changes—between rounds, forcing teams to adapt on the fly. (e.g., *"A key system just received an unexpected patch, closing a vulnerability,"* or *"A solar flare is causing intermittent power surges, making the grid unstable."*)

IV. Menu of Actions (Example)

Teams choose from a list like the one below. The full list would be more extensive.

Offensive Actions (Attack Cell)	AP Cost
Conduct Phishing Campaign	3
Scan External Network for Vulnerabilities	4
Deploy Malware via Supply Chain	6
Execute Zero-Day Exploit (High Risk/Reward)	8
Initiate Denial-of-Service (DoS) Attack	5

Defensive Actions (Defense Cell)	AP Cost
Run Emergency Employee Training Drill	3
Harden External Firewall	4

Defensive Actions (Defense Cell)	AP Cost
Deploy Intrusion Detection System (IDS)	6
Isolate Critical Systems (Air Gap)	7
Patch Known Vulnerabilities	5

V. Judging Criteria

Points are awarded each round based on:

1. **Strategic Efficacy (50%):** Was the chosen action effective? Did an attack succeed, or did a defense successfully thwart an attack?
2. **Resource Management (30%):** Was the allocation of Action Points efficient? Did the team achieve a significant outcome with a low-cost move, or waste points on an ineffective one?
3. **Foresight and Counter-Play (20%):** Did the team successfully anticipate and counter the opponent's move? (e.g., choosing to run training in the same round the opponent launches a phishing attack).
4. **Adaptability (Final Round Only):** How well the team adjusts its strategy in response to live injects from "Control."

VI. Grounds for Disqualification

- **Collusion:** Sharing strategic information with any other cell.
- **Delay of Game:** Consistently failing to submit actions within the time limit.
- **Unprofessional Conduct:** Arguing with "Control's" final rulings or displaying disruptive behavior.

Event: Project: Chimera

I. Event Description

Project: Chimera is a multi-stage strategic simulation where participants, as "Handlers" of clandestine network nodes, must navigate a landscape of shifting alliances and calculated betrayals. The event is divided into distinct Acts, each with evolving rules designed to force consolidation, foster distrust, and ultimately trigger a cascade of collapsing pacts until only one Handler controls the entire network.

This is a contest of pure strategy, negotiation, and psychological acumen. Your success will be measured not by technical skill, but by your ability to manage resources, manipulate rivals, and determine the precise moment when an ally becomes a liability.

II. General Rules and Principles

A. Team Composition

1. Each team, or "Handler Cell," will consist of two (2) to three (3) members.
2. Each Handler Cell begins the game in control of one "Node."

B. Core Doctrine

1. **Zero Technical Skill:** Victory is achieved through strategic planning and negotiation alone.
2. **Secret Actions, Public Consequences:** All actions are submitted secretly to the central moderator ("Control"). The outcomes are then resolved publicly.
3. **The Unspoken Contract:** All agreements made between Handler Cells are non-binding and unenforceable by "Control." Trust is a resource to be spent or exploited.
4. **Communication Protocol:** Open negotiation is permitted only during designated phases. All inter-team communication is forbidden during Action Phases.

III. Event Structure: The Three Acts

The game progresses through three Acts, with the rules changing as the player count diminishes.

Act I: The Consolidation (From Start until 50% of Cells are Eliminated)

- **Objective:** Survive the initial chaos and form foundational power blocs.
- **Gameplay:** The rules are at their simplest. Cells use Influence Points (IP) to attack, fortify, and support one another. Alliances are essential for both offensive expansion and mutual defense. Lone wolves are highly vulnerable.

Act II: The Unraveling (From 50% of Cells until 4 Cells Remain)

- **Objective:** To navigate the increasing instability of large alliances and pursue selfish goals.
- **New Mechanics Introduced:**
    1. **Network Strain:** Alliances become costly. Any formal "Alliance" (defined as 3 or more Handler Cells who mutually supported each other in the previous round) suffers an IP tax. Each member of the Alliance must pay **2 IP** at the start of the round, before income, simply to maintain the pact. This disincentivizes the formation of a single, dominant mega-alliance.
    2. **Secret Directives:** "Control" issues a secret, unique objective to each remaining Handler Cell (e.g., "Ensure the elimination of Node 7," "Control three adjacent Nodes," "Possess 40 IP in reserve"). Completing a Directive yields a massive, one-time bonus of **20 IP**. These objectives will inevitably force Handlers into conflict with their allies' interests.

Act III: The Endgame (The Final 4 Cells)

- **Objective:** Achieve total network dominance.
- **New Mechanics Introduced:**
    1. **Alliances Dissolved:** The `SUPPORT` action is disabled. No Handler Cell may aid another. It is now a true free-for-all.
    2. **Sudden Death Cascade:** At the end of each Resolution Phase, the Node with the lowest `FORTIFY` value for that round is **immediately eliminated**, regardless of whether it was attacked. This forces aggressive spending and prevents passive, defensive play.

IV. Core Gameplay Mechanics

A. Influence Points (IP)

- The sole resource for all actions. IP is gained through income and completing Directives. Unspent IP is saved.

B. Round Cycle

1. **Income Phase:** Each Cell receives a base of **5 IP**, plus **3 IP** for each additional Node they control.
2. **Negotiation Phase (10 mins):** Open-floor diplomacy and deal-making.
3. **Action Phase (5 mins):** Secret internal deliberation and submission of actions to "Control."
4. **Resolution Phase:** "Control" publicly reveals actions and resolves outcomes.

C. Menu of Actions

Action	IP Cost	Description
FORTIFY	Variable	Allocate IP to this Node's defense value for the round.
ATTACK	Variable	Allocate IP to an offensive action against a single target Node. If multiple Cells attack the same target, the Cell that contributed the most IP to the successful attack gains control of the Node.
SUPPORT	Variable	Allocate IP to bolster another Cell's `ATTACK` or `FORTIFY` action. (Disabled in Act III).
SUBVERT	10 IP	**The Betrayal Mechanic.** Target a Handler Cell you provided `SUPPORT` to in the previous round. If successful, you steal 50% of their current unspent IP (rounded down). This action is resolved before all others and is a powerful tool for crippling an unsuspecting ally.

V. Victory Conditions

The game concludes when only one Handler Cell remains. This Cell is declared the victor.

VI. Grounds for Disqualification

A Handler Cell will be immediately removed from the game for:

- **Violating Communication Protocols:** Communicating with other teams outside of the Negotiation Phase.
- **Cheating:** Viewing another team's Action Form or engaging in any activity that compromises the integrity of the secret action system.
- **Unprofessional Conduct:** Arguing with "Control's" final rulings or displaying behavior that is disruptive to the event. "Control's" adjudication is final.