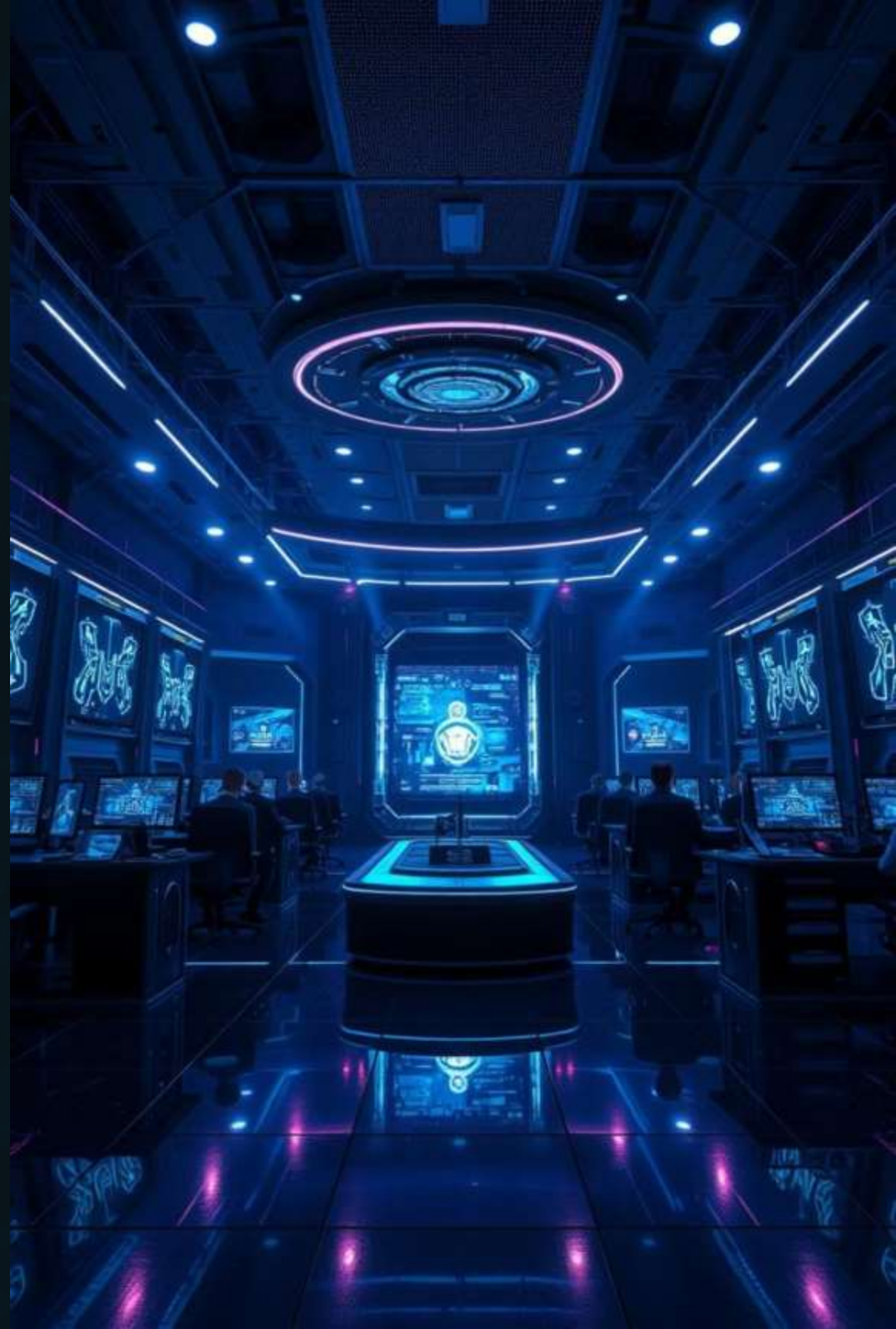
Arena SBC 2025

HUẾ

Thể thức thi đấu của Đấu trường Security Bootcamp 2025



Hình thức đấu trường

CTF

Nền tảng: CTFD

Thử thách giải đố, tìm kiếm lỗ hổng và khai thác.

Attack & Defense

Mô phỏng môi trường thực tế, vừa tấn công vừa phòng thủ.

Yêu cầu kỹ năng toàn diện.

Thể thức thi đấu của Đấu trường Security Bootcamp 2025

Điều kiện đua top và nhận giải:

- Đội thi phải khôi phục lại hệ thống hoàn chỉnh.
- Các dịch vụ trên các server được bàn giao phải hoạt động ổn định tối thiểu **10 phút**.

Về việc tiếp nhận, quản lý và quản trị server:

- Các đội sẽ tiến hành bốc thăm chọn server để tham gia cuộc thi, trong trường hợp phát sinh lỗi phải báo lại cho BTC.
- Các linh kiện thiết bị các đội tự bảo quản và bàn giao lại cho BTC sau khi thi đấu xong.
- Nghiêm cấm phá hoại, làm mất hoặc hư hại tài sản của BTC.
- Các đội phải duy trì các dịch vụ giám sát của BTC để tiến hành tính điểm.
- Các đội có thể thay đổi giải pháp dịch vụ để tăng cường bảo mật và giám sát phát hiện tấn công sớm. Danh sách dịch vụ xem thêm phần thể lệ thi đấu.

Thể lệ thi đấu: Hệ thống tính điểm

Các đội tham gia phần CTF của CyberJutsu để có thêm điểm cho đội mình.

Điểm khôi phục dịch vụ:

1000

Server K8s

Khôi phục và dịch vụ hoạt động.

500

Server

Khôi phục và dịch vụ hoạt động.

100

Máy trạm

Khôi phục và dịch vụ hoạt động.

Điểm chiếm quyền kiểm soát:

1000

ESXi/vCenter

Chiếm được của đối phương.

500

Server

Chiếm được của đối phương.

300

Thiết bị

Chiếm được của đối phương.

100

Máy trạm

Chiếm được của đối phương.

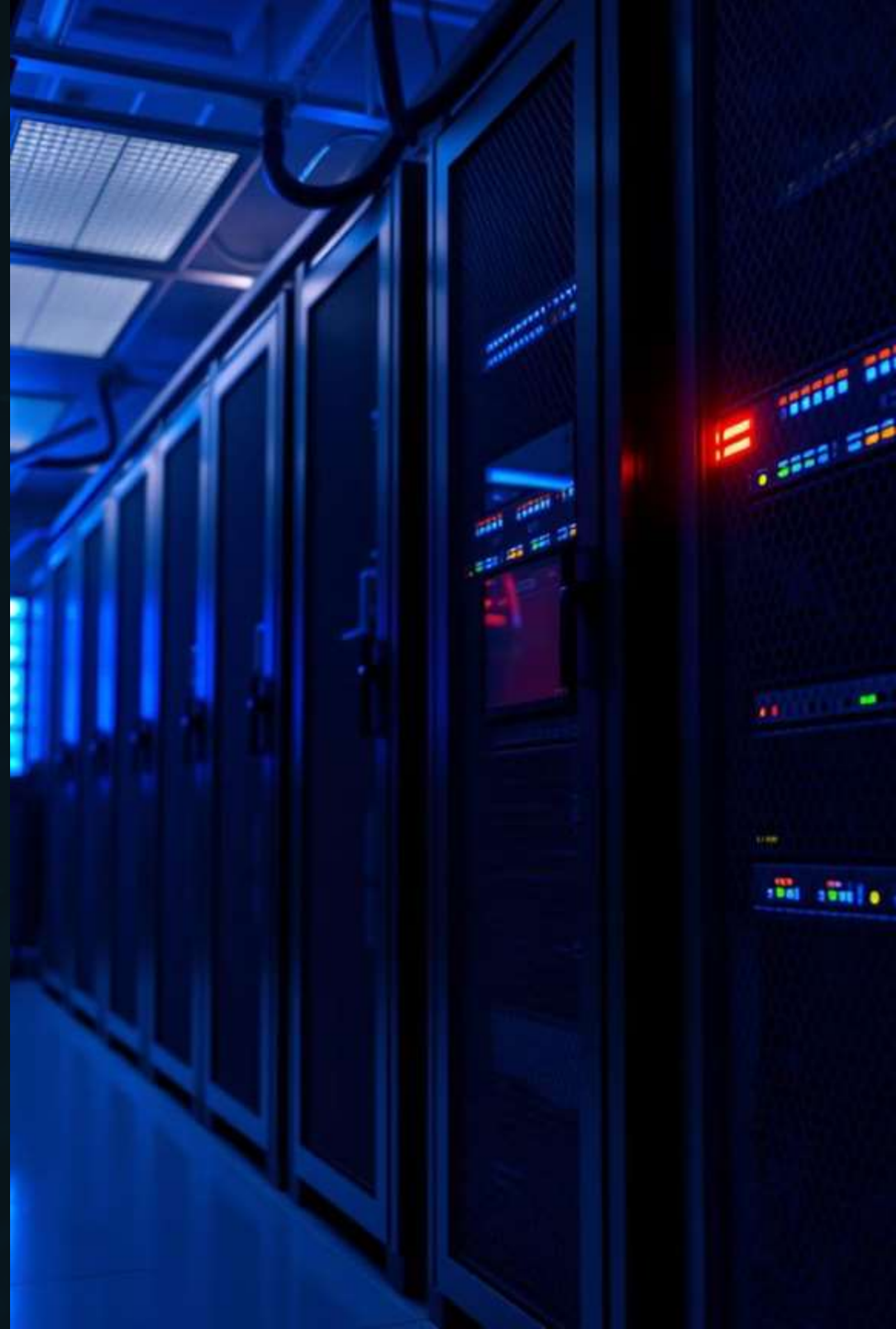
Thể lệ thi đấu: Quy định trừ điểm

Khi chiếm được server/máy trạm của đối phương mà **“không vô hiệu hoá dịch vụ”** thì đội quản trị server không bị trừ điểm.

Trừ điểm khi dịch vụ dừng quá 10 phút:

- Server: 500 điểm
- Máy trạm: 100 điểm
- ESXi: 2000 điểm

Duy trì hoạt động ổn định là chìa khóa để bảo toàn điểm số!



Thể lệ thi đấu: Các hành vi được cho phép

- Nâng cấp OS/Service
  Cập nhật hệ điều hành và các dịch vụ để tăng cường bảo mật.
- Patching hoặc workaround
  Áp dụng các bản vá hoặc giải pháp tạm thời cho lỗ hổng.
- Thay thế core firewall
  Triển khai giải pháp tường lửa mới để bảo vệ mạng.
- Thay thế giải pháp SIEM/SOAR
  Cải thiện khả năng giám sát và phản ứng sự cố.
- Bổ sung IDS/IPS hoặc Network Security Monitoring
  Tăng cường khả năng phát hiện và ngăn chặn xâm nhập.
- Bổ sung WAF
  Bảo vệ ứng dụng web khỏi các cuộc tấn công.
- Cài đặt bổ sung các giải pháp Endpoint Security
  Như sandbox, Virtual Patch, Host IDS/IPS, Honeypot, ...
- Bổ sung rule cho firewall, IDS/IPS, SOAR/SIEM, Syslog
  Tối ưu hóa quy tắc bảo mật và ghi nhật ký.

Thể lệ thi đấu: Quy định về giải pháp và báo cáo

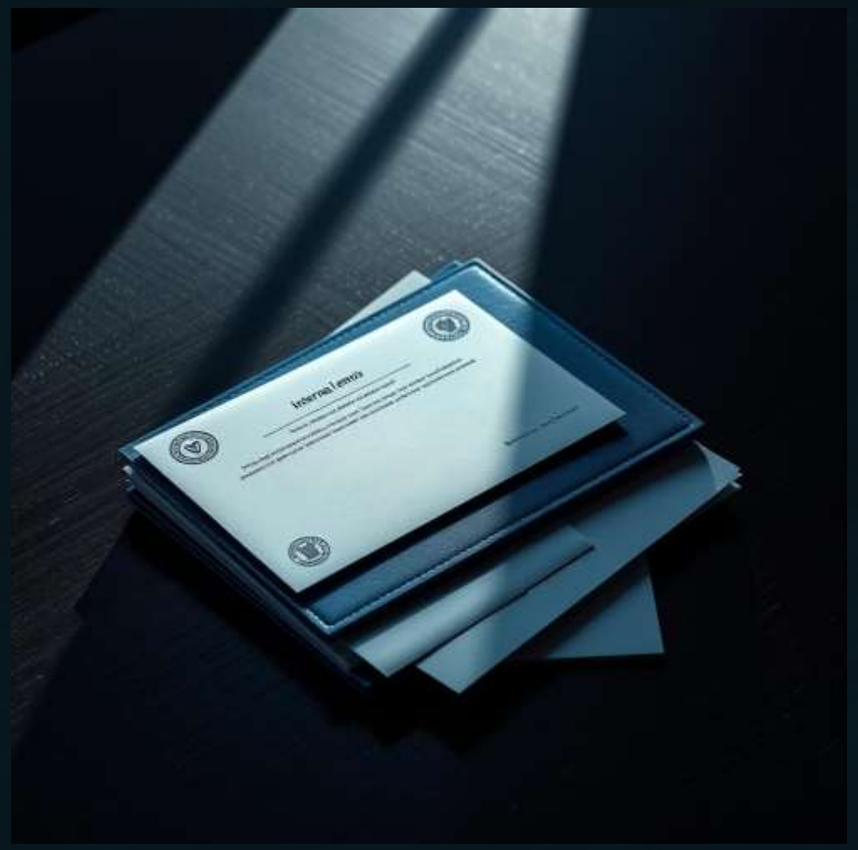
Đối với các giải pháp thay thế:

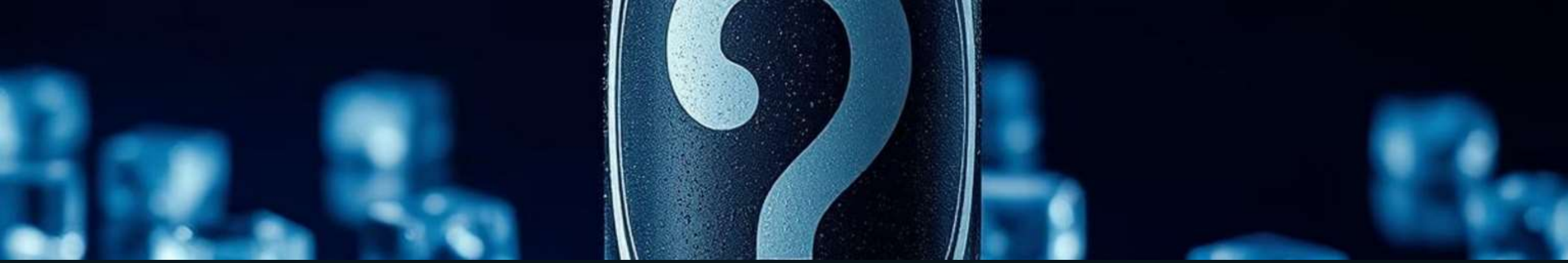
Phải đảm bảo các dịch vụ/ứng dụng khác hoạt động được theo checklist, từng tính năng dịch vụ.

=> Gửi email nội bộ thôi

Khi Owner server/máy trạm thì gửi info tính điểm:

- **Linux:** Chèn tên vào `/etc/hosts`
- **Windows:** Chèn tên vào `C:\Windows\System32\drivers\etc\hosts`
- **Các trường hợp khác:** Thông báo lại ban tổ chức





Thể lệ thi đấu: Lưu ý quan trọng

Dịch vụ bị dừng

Những dịch vụ khi bị dừng sẽ bị trừ điểm hoặc không ghi điểm.

Tấn công sau giờ làm việc

Chiếm được server hoặc tấn công làm dịch vụ của đối phương ngừng hoạt động sau giờ làm việc.

Ứng dụng quản trị bị crash

Ứng dụng quản trị bị crash nhưng vẫn cung cấp dịch vụ bình thường.

Quy tắc hỏi BTC

Đội nào không đọc kỹ hỏi BTC quá **3 lần** thì trừ **100 điểm**.

Cách hỏi BTC

Muốn hỏi gì thì cầm **Huda** lên gặp BTC.

Hỗ trợ

Các đội thi chỉ được cấp **Huda** và **đá lạnh** (không cấp nước).

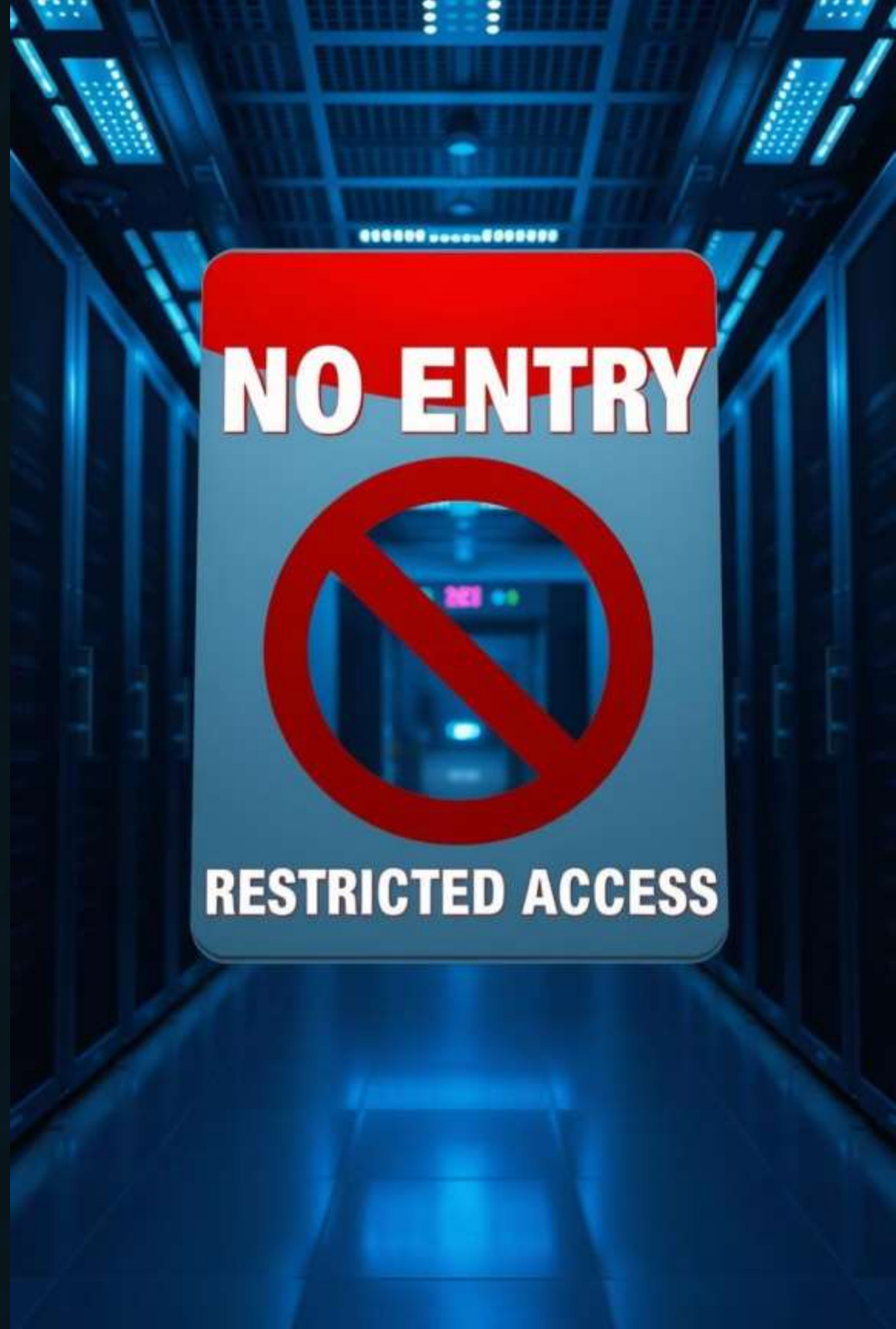
Thể lệ thi đấu: Phạm vi cấm tấn công

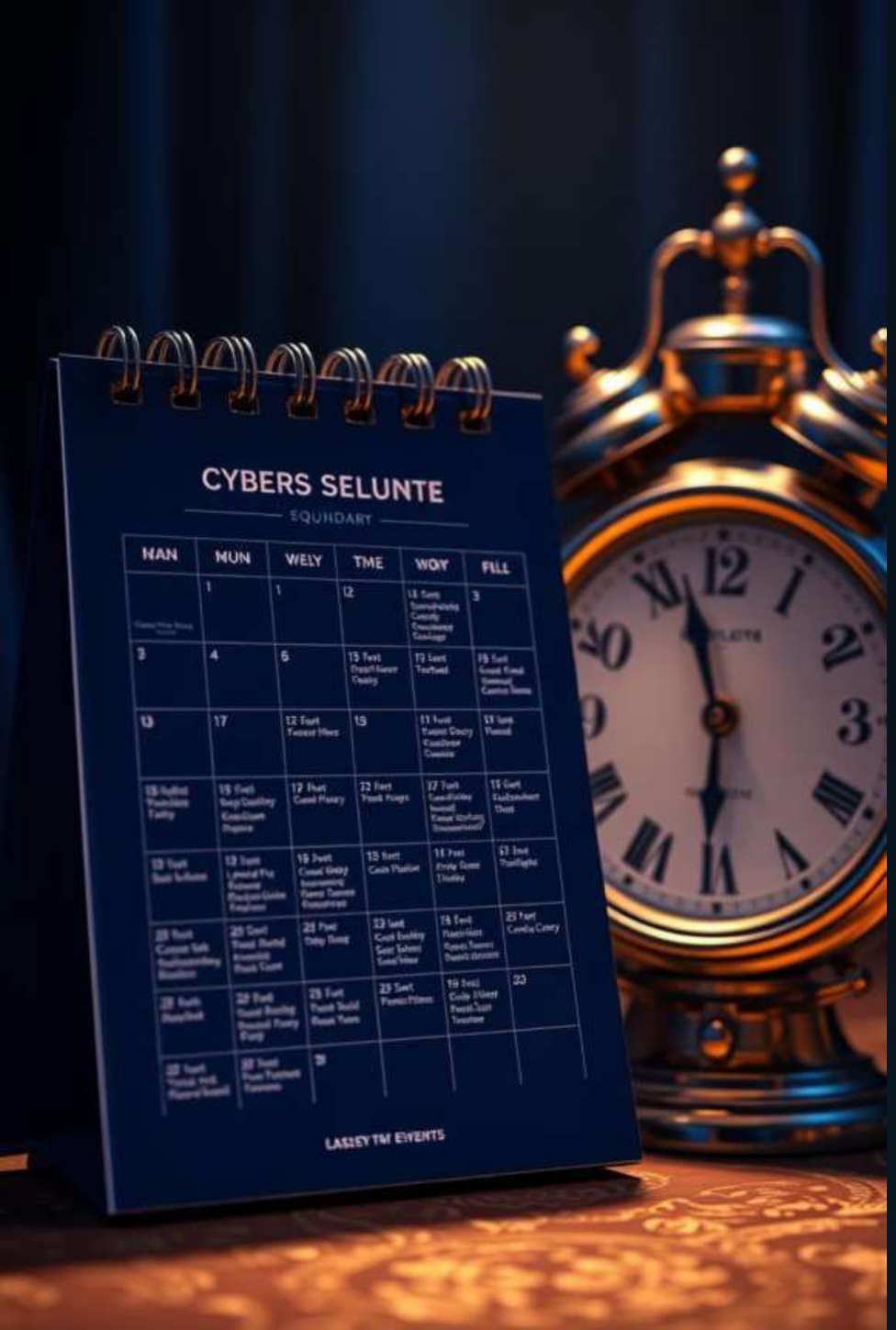
CẢNH BÁO: HÀNH VI BỊ CẤM!

Những phạm vi nếu đội nào tấn công sẽ bị loại ngay lập tức:

- Subnet 192.168.199.0/24 của BTC (nếu đội nào tấn công BTC sẽ trả thù)
  - Các range IP 10.10.10.1> 10.10.10.200

Hãy tuân thủ nghiêm ngặt các quy định để tránh bị loại khỏi cuộc thi!





Thể lệ thi đấu: Lịch trình Đấu trường

1

Bắt đầu Đấu trường

13h00 ngày 12/9/2025

Cuộc thi chính thức khởi tranh.

2

Kết thúc Đấu trường

17h00 ngày 13/9/2025

Thời gian thi đấu chính thức kết thúc.

3

Giờ nghỉ (Không tính điểm)

17h00 - 07h00 sáng hôm sau

BTC sẽ không cộng trừ điểm trong khoảng thời gian này.

4

Tấn công ngoài giờ

BTC sẽ không giới hạn việc các bạn tấn công sau giờ làm việc.

Hãy tận dụng thời gian này để gây bất ngờ cho đối thủ!

Chúc các đội thi đấu hết mình và đạt được kết quả tốt nhất!