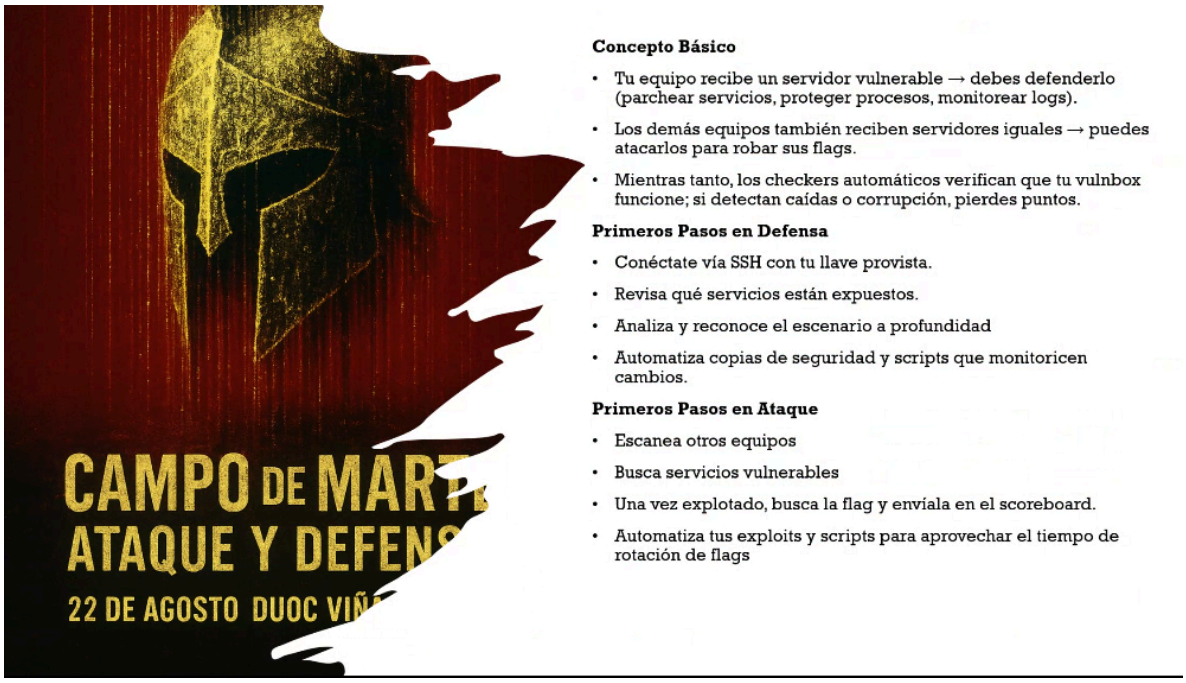


Subred desplegada en AWS y esa tiene un servidor

Esa tiene 5 desafíos corriendo con distintas dificultades.

CDR 24

Red excepto el ultimo digito se mantiene igual

10.66.IDEQUIPO.#MAQUINA

DEFENSA ES INSUMO PARA EL QUE ESTÁ ATACANDO, todos los servidores son iguales

La plataforma monitorea siempre la disponibilidad

- Todas las flags son distintas
- Cada equipo tiene una flag distinta por desafio distinto
- Para poder medir la desponiblidad. Para ver si logro atacar o defender, la plataforma divide la competencia en ticks o turnos de reloj, y hace chequeo. Por cada chequeo se hace una rotación de flags de la defensa. INGRESAR FLAG ALTOQUE porque cambian
- La idea es vulnerar las maquinas de todos los contrincantes

Llave SSH para establecer conexión a este servidor

No se puede modificar el firewall de la maquina

Infraestructura

•Cada equipo recibe una **vulnbox en AWS** provista por la organización (Debian 12).
•La infraestructura central (scoreboard, checkers, VPN y servicios comunes) está gestionada por el staff.

Acceso

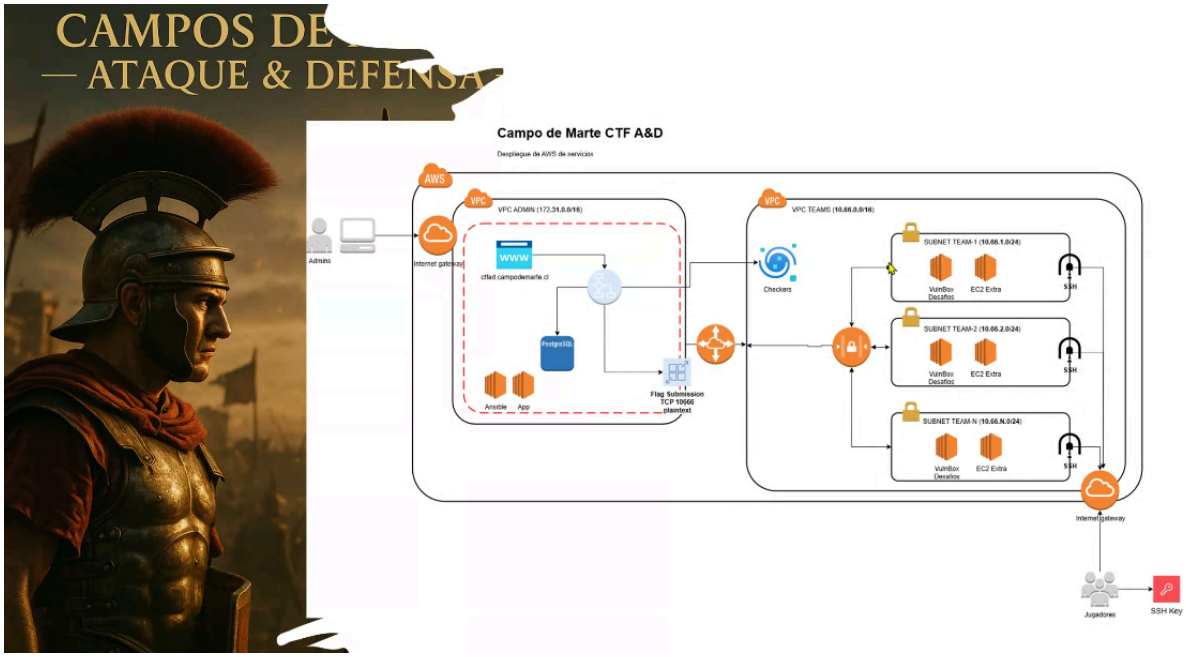
•Cada equipo recibe un **llaves SSH** exclusivas.
•El acceso es con el usuario predeterminado admin en la dirección pública asignada a la vulnbox.
•El tráfico entre equipos y vulnbox estará dentro de una **VPC privada en AWS**.

Red

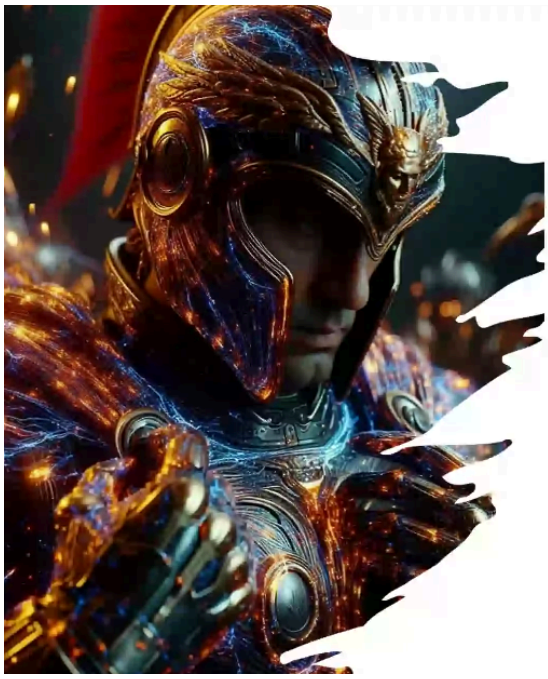
•La vulnbox de cada equipo tiene una IP privada fija (ej: 10.66.<team>.4).
•Los equipos acceden a su vulnbox desde internet mediante la llave SSH y la IP pública asignada.
•Los ataques se realizan únicamente entre las vulnbox dentro de la red privada (no se ataca a la IP pública).

Servicios

•Cada vulnbox expone servicios vulnerables en puertos definidos por el evento.
•Los servicios estarán monitoreados por los **checkers** para validar disponibilidad e integridad.



Envío de flags es a través de TCP texto plano. Telnet o nc al puerto 10166 de la ip q nos pasan, el servicio revisa si la flag es válida



Reglas Generales

1.El CTF es de modalidad **Ataque y Defensa**. Cada equipo recibe una máquina vulnerable ("vulnbox") que debe defender mientras intenta comprometer las de los demás.
2.El evento está ambientado en un escenario histórico-estratégico, pero **las reglas son estrictamente técnicas y competitivas**.
3.El uso de **DoS, DDoS, floods o ataques a la infraestructura central del evento** está estrictamente prohibido.
4.Solo está permitido atacar las **vulnbox de otros equipos** a través de los servicios habilitados y en los rangos de IP definidos.
5.Compartir o filtrar flags entre equipos está prohibido. Las flags se deben enviar únicamente a través del sistema de scoring oficial.
6.Los organizadores se reservan el derecho de aplicar penalizaciones o descalificaciones por conductas que atenten contra el espíritu del evento.
7.Esta prohibido toda manipulación de firewall de las vulnbox

Flags

•Las flags están almacenadas en los servicios de cada vulnbox y se rotan en intervalos regulares (ej: cada 2-3 minutos).
•Formato: CDM_TEXTOS_UNICO_POR_TURNO_y_EQUIPO
•Enviar la flag en el **scoreboard oficial** suma puntos de ataque, mientras que perder flags en tus servicios resta puntos de defensa.

Puntuación

•**Ataque**: puntos por cada flag válida robada a otros equipos.
•**Defensa**: puntos por cada intervalo en el que tus servicios permanecen íntegros y responden correctamente a los checkers.
•El puntaje total es la suma de ambas métricas.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

DuocUC

Brinck

inacap

OPEN H4CK

ORION

Durante el evento, el **soporte** estará disponible de dos maneras:

1.Presencialmente con los organizadores en el lugar del evento.

2.En línea a través de nuestro servidor de Discord oficial: Unirse al Discord

https://discord.gg/7tmxA3sp

Campo de Marte

SECURE DEVELOP
Seguridad por defecto, desde el diseño

DevelR0X CIBERLABS kaspersky