BASES
COMPETENCIA DE CIBERSEGURIDAD “STRIKE BACK”

El día 13 y 14 de octubre de este año, se llevará a cabo el quinto Encuentro de Innovación Pública INNOVAPOLINAV, una actividad que busca generar acciones para conectar a la Armada de Chile con el ecosistema de investigación, desarrollo, innovación y emprendimiento nacional e internacional.

Por segundo año consecutivo, se incluye la ciberseguridad como materia de alto interés formativo y de participación en el quehacer nacional, por lo que, como Centro de Estudios en Ciberseguridad e Investigación en Defensa CECID, en conjunto con las siguientes organizaciones civiles: La Comunidad Level[0]Sec, la Comunidad PartyHack, la Organización Internacional ISACA Capítulo Santiago, con la Colaboración de las instituciones y empresas, Capacitación USACH, Microsoft, IT-Box, VAST.ECO, SCL Maintenance, se ha organizado el Evento de Ciberseguridad “Strike Back” cuyo objetivo principal es impulsar el desarrollo personal e incentivar la mejora en las capacidades institucionales y de la sociedad.

OBJETIVO

El objetivo de estas Bases es regular la participación de los competidores debidamente registrados en el formulario compartido y publicado en página la www.innovapolinav.cl, y en las redes sociales de las organizaciones e instituciones participantes, tanto para las competencias por equipos como Individuales, durante las actividades del evento comprendido única y exclusivamente entre los días 13 y 14 de octubre del 2022.

REQUISITOS DE PARTICIPACIÓN

La inscripción de participación implica el conocimiento y la aceptación integral de las presentes bases, así como de las bases generales que regulan la participación en las actividades del evento, por lo que, es requisito aceptar los términos de Inscripción enviados en el Formulario, de lo contrario, no se podrá inscribir como participante en las siguientes actividades.

ACTIVIDADES Y SUS RESTRICCIONES

El Encuentro de Ciberseguridad se compone de tres activades separadas e independientes entre sí, y son las que se detallan a continuación:

1. CTF ABIERTO

El primer evento es un **CTF ABIERTO** a toda la sociedad, nacional e internacional, con dos categorías, individual y por equipos con un máximo de 5 miembros y un mínimo de 3. Este evento es en modalidad Online y no presencial.

Se iniciará la competencia a las 12:00 horas del día 13 de octubre. El acceso a la plataforma será abierto y de manera continuada, para todo el evento y permanecerá activa hasta el cierre del evento, programado para las 16:00 horas del día 14 de octubre.

La competencia individual solo será para el CTF Abierto, y se rige por las mismas restricciones que la competencia por equipos. No hay requisitos mínimos de edad o localización para participar en forma individual en las competencias abiertas, exceptuando las siguientes restricciones:

- No se permite la participación en dos o más equipos.
- El competidor individual no puede participar en equipo
- No se permite la participación de docentes en cualquier área de la ciberseguridad, que ejerzan o hayan ejercido nacional e internacionalmente.
- Quien no se registre, no podrá competir, ni ser admitido fuera de plazo.
- Todo participante debe llenar el formulario de inscripción con sus datos reales.

2. RED VS BLUE FF.AA. Y DE ORDEN PRESENCIAL Y CERRADO

El segundo evento es un **CTF CERRADO** exclusivamente desarrollado para las FF.AA. y de Orden, con un escenario común y ficticio, donde, todos los equipos participantes se dividirán, por sorteo, en dos grupos, donde uno hará de Blue Team y tendrá la misión de defender la infraestructura, y el otro grupo actuará como Red Team, e intentará atacar y vulnerar la infraestructura existente dentro del ejercicio. Para esto se dispondrá de un laboratorio aislado y compuesto por maquinas virtualizadas. Los equipos estarán compuestos por un máximo de 5 participantes con un mínimo de 3, donde los equipos participantes deben pertenecer exclusivamente a las instituciones de la defensa y de orden nacionales.

Esta competencia posee dos categorías de premiación: Premio por equipo al mayor puntaje acumulativo y premio al mayor puntaje individual evaluado por cantidad de puntos generados a los equipos y al grupo, donde los puntajes sumados corresponderán a las dos jornadas, en total y por su desempeño personal, evaluado por sus pares. El Equipo de Jueces (White Team) evaluará la determinación de cada resolución.

Se entenderán como parte de la conducta obligatoria el respeto, el honor, la lealtad, el trabajo en equipo y la sana convivencia con cada uno de los competidore y se extiende a la conducta de todo el equipo, no obstante, se establecen las siguientes restricciones:

- Pueden participar miembros de diferentes ramas de las FF.AA y de Orden en el mismo equipo.
- No se permiten conductas como la entrega de flags, hint-farming, fuerza bruta para obtener flags dentro del servidor de CTF.
- No se permite la participación en dos o más equipos.
- No se permite la participación de docentes en cualquier área de la ciberseguridad, que ejerzan o hayan ejercido nacional e internacionalmente.
- No se aceptará la colusión de equipos.

3. RED VS BLUE ABIERTO

El tercer evento es un **CTF ABIERTO** desarrollado para las IES y de Formación Técnica tanto civiles como militares, con un escenario común y ficticio, donde, todos los equipos participantes se dividirán, por sorteo, en dos grupos, donde uno hará de Blue Team y tendrá la misión de defender la infraestructura, y el otro grupo actuará como Red Team, e intentará atacar y vulnerar la infraestructura existente dentro del ejercicio. Para esto se dispondrá de un laboratorio aislado y compuesto por maquinas virtualizadas.

Los equipos estarán compuestos por un máximo de 5 participantes con un mínimo de 3, donde los equipos participantes deben pertenecer exclusivamente a las instituciones de la defensa y de orden nacionales.

Esta competencia posee dos categorías de premiación: Premio por equipo al mayor puntaje acumulativo y premio al mayor puntaje individual evaluado por cantidad de puntos generados a los equipos y al grupo, donde los puntajes sumados corresponderán a las dos jornadas, en total y por su desempeño personal, evaluado por sus

pares. El Equipo de Jueces (White Team) evaluará la determinación de cada resolución.

INSCRIPCIÓN CTF ABIERTO

Se realizará mediante formulario online, publicado en redes sociales y en páginas oficiales a contar del día 5 de octubre, con fecha y hora de término de registro, para el día 12 de octubre a las 12:00 horas, como tope máximo.

Las personas inscritas recibirán el enlace a la plataforma del CTF Abierto mediante el correo proporcionado.

Para mantener el respeto mutuo entre participantes, no se aceptará el uso de lenguaje ofensivo, discriminatorio, peyorativo sobre algún sector de la sociedad civil o las instituciones del estado, sus autoridades y/o toda persona por su etnia, credo, condición, orientación y credo. El incumplimiento de esta conducta dará paso al término de la inscripción de forma inmediata y a la expulsión de la competencia.

Esta actividad es gratuita para la inscripción y la participación, ya sea individual y como equipos.

NORMAS DE PARTICIPACIÓN

En las categorías del CTF, tanto individual como por equipos, no se permiten alianzas, no se permite el intercambio de flags o el hint-farmming, quedan prohibidos los ataques de fuerza bruta. La infracción de dicha norma, atenta contra la lealtad y la ética competitiva, por lo tanto, dada la detección de estas infracciones, supondrá la inmediata descalificación del participante y, en función al tenor de la infracción, del equipo. Sin prejuicio de que, por la gravedad de la infracción o comportamiento anómalo detectado, pueda ser sujeto a posibles acciones legales por parte de los patrocinadores y organizadores.

FUNCIONAMIENTO DE LOS RETOS DEL CTF ABIERTO

Los retos abiertos se habilitarán en una plataforma de CTF de acceso público, de tipo Jeopardy. En este sentido los participantes ingresarán a la plataforma mediante el navegador web al entorno virtual de los retos.

En estas pruebas se consideran varias áreas del conocimiento y habilidades en las diferentes áreas de la seguridad de sistemas, Esto incluye las siguientes categorías:

- Sistemas Operativos >> Nivele Fácil, Medio
- Reconocimiento >> Nivele Fácil, Medio
- Ingeniería Inversa >> Nivele Fácil, Medio
- Criptografía y esteganografía >> Nivele Fácil, Medio
- Conocimientos generales de computación, redes e informática.
- Reversing>> Nivele Fácil, Medio.

BASES DE LA COMPETENCIA RED VS BLUE

La competencia Red vs Blue se realizará en las dependencias de la Academia Politécnica Naval.

En este evento, se dividirán los equipos, mediante sorteo, en dos grupos, el primero será designado como Red Team y el segundo grupo, como Blue Team, donde, los equipos se unirán en un solo Team con un solo objetivo.

- Para Blue Team la función es defender la infraestructura.
    - Utilizarán la arquitectura entregada, con los accesos y controles de sistemas facilitados por la organización.
    - El Blue Team organizará a los equipos para defender la infraestructura, entregando roles y responsabilidades a cada grupo miembro, para lo cual, se asignará tiempo para dicha tarea.
    - El BT deberá realizar análisis de Inteligencia de amenazas.
    - Deberá modelar la amenaza posible y debe configurar y operar

- Para Red Team la función es atacar la infraestructura.
    - Utilizarán sistemas operativos ofensivos propios.
    - El Red Team deberá organizar a los equipos para atacar la infraestructura, entregando roles y responsabilidades a cada grupo miembro, para lo cual, se asignará tiempo para dicha organización.
    - Se coordinarán estratégica y tácticamente para logra el acometido.
    - Todo está permitido en Red Team, con excepción de ataques de denegación de servicios y el uso de botnets,
    - El objetivo primario será poder lograr Command and Control (C2)

Se dará 1 hora para Coordinar antes del inicio de la competencia. El escenario presentado el día 13 de octubre, será el mismo que se utilizará el día 14 de octubre, sin embargo, se invertirán los roles y se renovarán las "*flags*" para todos los retos.

PUNTUACION DE LOS RETOS DE RED VS BLUE Y CTF ABIERTO

Cada prueba tiene asignado un valor en puntaje máximo en función a su dificultad y, en la medida en que se soliciten Hints (pistas), estas descontarán del valor máximo, un puntaje informado en cada casilla. Para obtener el puntaje, se debe ingresar y enviar la evidencia de éxito mediante la flag descubierta o la(s) respuesta(s) correcta(s).

CATEGORIAS PARA PREMIACIÓN

Los premios se informarán de manera oportuna y las categorías son los siguientes:

1. **CTF RVSB CERRADO FF.AA. Y DE ORDEN - INDIVIDUAL**
   - Primer Lugar Individual por Evaluación y Puntaje
   - Primer Lugar por sumatoria de puntajes dos jornadas
   - Segundo Lugar por sumatoria de puntajes dos jornadas
   - Tercer Lugar por sumatoria de puntajes dos jornadas

2. **CTF RVSB ABIERTO IES Y CFT**
   - Primer Lugar Individual por Evaluación y Puntaje
   - Primer Lugar por Equipo por sumatoria de puntajes dos jornadas
   - Segundo Lugar por Equipo por sumatoria de puntajes dos jornadas
   - Tercer Lugar por Equipo por sumatoria de puntajes dos jornadas

3. **CTF ABIERTO**
   - Primer Lugar individual y por equipo.
   - Segundo Lugar individual y por equipo.
   - Tercer Lugar individual y por equipo.

La rúbrica de valores fijará los puntajes por flag, descuentos por causales ya definidas y puntos de bonificación, la que se publicará el mismo día del evento.

La entrega de los premios en CTF Cerrado presencial, serán entregados en ceremonia de premiación a realizarse el día 14 de octubre a las 17:30 horas.

La entrega de los premios en CTF Abierto será entregado mediante comunicación directa con los ganadores, vía correo de registro.

SELECCIÓN DE LOS GANADORES

El fin de la competencia ha sido fijado para ambas modalidades de CTF Abierto y Cerrado, a las 16:00 horas del viernes 14 de octubre. La posición en

el ranking se establecerá por el número de puntos obtenidos avalados por la rúbrica y certificado por los jueces del White Team. En caso de empate de puntos entre misma modalidad y categoría de dos o más equipos o competidores individuales, se discernirá por timestamp predominando quien llegó primero a la solución.

PARTNERS Y SPONORS

Los equipos partners de las diferentes comunidades, empresas de capacitación y de servicios, nos han colaborado con profesionales capacitados de muy alto nivel, con infraestructura de alta calidad y recursos para hacer de este evento, una experiencia de aprendizaje y de formación.

DISCLAIMER

Todas las actividades que se realizarán en este evento son de carácter académico, se realizarán en ambientes controlados, los escenarios presentados son ficticios y las acciones no tiene efecto en las infraestructuras externas de ningún tipo.

Consultas al Email:

innovacion@apolinav.cl

claudio.reyes.o@usach.cl

Viña del Mar, 04 de octubre de 2022

Atentamente.

Equipo organizador.