EDH TALKS – 1RA EDICIÓN

CTFs para aprender hacking

By Alpra_tdm

Resuelve tus primeros CTFs - No se necesita ser un experto para empezar, se necesita saber aprender

¡Hola! ¿Te gustaría embarcarte en un emocionante viaje de aprendizaje en el mundo del hacking ético? Te presentamos "Grand Line", nuestro exclusivo curso diseñado para brindarte las habilidades fundamentales necesarias en seguridad informática. Durante 3 meses, te sumergirás en módulos especializados que abarcan desde los conceptos básicos hasta el Pentesting. Aprenderás sobre redes, Linux, programación y técnicas de Pentesting, todo de manera amigable y accesible. Nuestro enfoque práctico y didáctico te permitirá adquirir los conocimientos necesarios para proteger sistemas y descubrir vulnerabilidades. Únete a nosotros en esta aventura educativa y desata tu potencial en el hacking ético. ¡Te esperamos en "Grand Line"!

https://alpra-tdm.com

Contenido

Historia

Los retos CTF (Capture The Flag) tienen sus raíces en ejercicios de entrenamiento militar y juegos de estrategia. A medida que la seguridad informática se convirtió en un tema cada vez más relevante, los CTF evolucionaron para convertirse en una forma de desafío y aprendizaje en el ámbito de la ciberseguridad.

Aunque no hay una historia precisa y definida de los CTF, se cree que los primeros retos similares a los CTF modernos surgieron en la década de 1990 en el entorno de los grupos de hackers y entusiastas de la seguridad informática. Estos grupos organizaron competiciones en las que los participantes debían resolver desafíos técnicos y encontrar banderas (flags) para demostrar su habilidad y conocimiento.

A medida que la popularidad de los CTF creció, también lo hizo la diversidad de los desafíos. Los retos empezaron a abarcar diferentes áreas de la seguridad informática, como la criptografía, la ingeniería inversa, la explotación de vulnerabilidades, el análisis forense digital, la web y más.

En la actualidad, los CTF se han convertido en una práctica común en la comunidad de seguridad informática. Se llevan a cabo en eventos y conferencias, en línea a través de plataformas especializadas y en entornos educativos. Además, se han establecido competiciones internacionales y ligas, como DEF CON CTF y PlaidCTF, que atraen a participantes de todo el mundo.

La popularidad de los CTF se debe a su capacidad para proporcionar un entorno práctico y desafiante para mejorar las habilidades técnicas, fomentar la colaboración y promover la innovación en el campo de la ciberseguridad. Los CTF continúan evolucionando y adaptándose a medida que surgen nuevas técnicas y tecnologías, y siguen siendo una parte integral de la comunidad de seguridad informática.

Beneficios

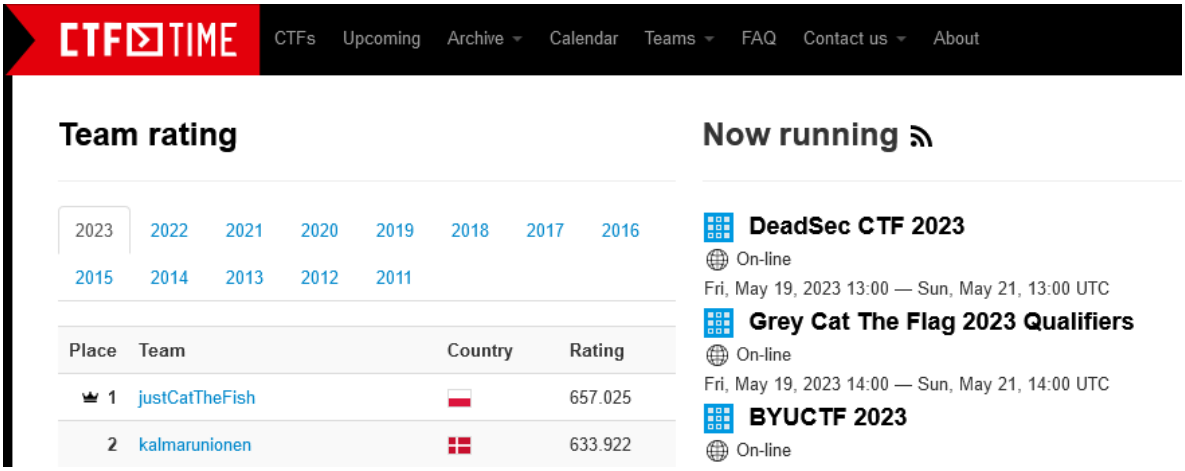
1. Entrenamiento de habilidades: Los CTF ofrecen un entorno controlado y realista para que los militares practiquen y mejoren sus habilidades en áreas como la ciberseguridad, la resolución de problemas técnicos y la defensa de sistemas. Los desafíos de CTF ayudan a fortalecer sus capacidades y prepararlos para enfrentar amenazas y ataques en el campo de batalla digital.
2. Evaluación de capacidades: Los retos de CTF permiten evaluar las habilidades y el conocimiento de los militares en tiempo real. Los participantes se enfrentan a desafíos prácticos y se les mide en términos de su capacidad para resolver problemas, trabajar en equipo y aplicar técnicas específicas de ciberseguridad.
3. Fomento de la competitividad y el espíritu de equipo: Los retos de CTF crean un ambiente competitivo donde los militares pueden demostrar sus habilidades y competir entre sí. Esto promueve la camaradería, el espíritu de equipo y el sentido de logro al trabajar juntos para alcanzar un objetivo común.
4. Actualización constante: Los desafíos de CTF ayudan a los militares a mantenerse al día con las últimas tendencias, técnicas y vulnerabilidades en el campo de la ciberseguridad. Estos retos brindan una oportunidad para practicar y aprender nuevas estrategias de defensa y ataque, y adaptarse a un entorno de amenazas en constante evolución.
5. Preparación para escenarios reales: Los CTF pueden simular situaciones y escenarios de la vida real, lo que permite a los militares desarrollar habilidades y estrategias que pueden aplicar en el campo de batalla digital. Esto incluye la identificación y mitigación de amenazas, la respuesta a incidentes y la protección de infraestructuras críticas.

Desventajas

1. Estrés y presión: Los CTF pueden generar un ambiente altamente competitivo y estresante, especialmente en competiciones de alto nivel. La presión de resolver desafíos en un tiempo limitado y superar a otros participantes puede generar estrés y ansiedad.
2. Enfoque en la competición en lugar del aprendizaje: En algunos casos, el enfoque excesivo en ganar la competición puede hacer que los participantes se centren más en obtener puntos y superar a los demás en lugar de enfocarse en el aprendizaje y la mejora de habilidades.
3. Posible falta de diversidad de desafíos: Algunos CTF pueden tender a repetir ciertos tipos de desafíos o centrarse en áreas específicas de la seguridad informática, lo que puede limitar la exposición a diferentes aspectos y dificultades.
4. Exclusividad y barreras de entrada: Algunas competiciones de CTF pueden ser de acceso limitado o requerir conocimientos y habilidades técnicas avanzadas, lo que puede excluir a aquellos que son nuevos en el campo o que no tienen experiencia previa en seguridad informática.
5. Énfasis en la explotación en lugar de la defensa: Aunque los CTF pueden abarcar tanto la explotación como la defensa, a veces existe una tendencia a centrarse en la parte ofensiva. Esto puede llevar a una falta de enfoque en las habilidades de defensa y protección de sistemas, que también son fundamentales en el campo de la ciberseguridad.

Es importante tener en cuenta que estos puntos negativos no aplican necesariamente a todos los CTF y pueden variar según las circunstancias y la organización de cada competición. Los CTF siguen siendo una herramienta valiosa para el aprendizaje y el desarrollo de habilidades en seguridad informática, siempre y cuando se aborden de manera equilibrada y se fomente un enfoque constructivo y colaborativo.

https://ctftime.org/



Una plataforma en línea dedicada a rastrear y mostrar información sobre competiciones de Capture The Flag (CTF) en todo el mundo. Es una referencia centralizada para aquellos interesados en participar en CTFs y mantenerse al tanto de los eventos y resultados de las competiciones.

1. Calendario de eventos: CTFtime proporciona un calendario completo de competiciones de CTF que se llevarán a cabo en diversas fechas y lugares. Los usuarios pueden consultar esta información para planificar su participación en futuros CTFs.
2. Información detallada sobre competiciones: La plataforma ofrece detalles específicos sobre cada competición de CTF, como la descripción del evento, el formato, las fechas, los requisitos de inscripción, las reglas y las categorías de desafíos.
3. Clasificación de equipos: CTFtime muestra las clasificaciones de los equipos participantes en diferentes competiciones, lo que permite a los usuarios conocer a los equipos más exitosos y reconocidos en el ámbito de los CTFs.
4. Estadísticas e historial de competiciones: La plataforma recopila datos y estadísticas sobre competiciones pasadas, incluyendo la cantidad de equipos participantes, el nivel de dificultad de los desafíos y los premios otorgados. Esto ayuda a los usuarios a tener una idea de la complejidad y el alcance de cada competición.
5. Perfiles de equipos y jugadores: CTFtime permite a los equipos y jugadores registrarse y crear perfiles para mostrar su participación en competiciones de CTF, sus logros y sus habilidades. Esto ayuda a construir una comunidad y facilita la interacción entre los participantes.

5 consejos para CTFs

No importa el nivel o rama, empieza por las bases, hay un CTF que lo explica

Es fundamental comenzar por las bases y adquirir conocimientos y habilidades en diferentes áreas de la seguridad informática. Hay varios CTFs que están diseñados para ayudar a los principiantes a aprender y practicar conceptos fundamentales. Uno de los ejemplos populares es:

1. "PicoCTF" (https://picoctf.org/): PicoCTF es un CTF en línea diseñado para principiantes en seguridad informática. Proporciona una serie de desafíos en áreas como criptografía, forense digital, ingeniería inversa, explotación de vulnerabilidades web y más. Además de los desafíos, PicoCTF también ofrece recursos educativos y tutoriales para ayudar a los participantes a aprender los conceptos necesarios para resolver los desafíos.

PicoCTF es solo uno de los muchos CTFs que se enfocan en proporcionar una introducción a los conceptos básicos del hacking ético. Otros CTFs y plataformas en línea, como Hack The Box (https://www.hackthebox.eu/) y OverTheWire (https://overthewire.org/wargames/), también ofrecen desafíos graduados en dificultad y están diseñados para ayudar a los principiantes a desarrollar sus habilidades.

Es importante recordar que, en el hacking ético, es esencial seguir los principios éticos y legales, así como obtener el consentimiento adecuado antes de realizar cualquier prueba o actividad de seguridad. Los CTFs pueden ser una excelente manera de aprender y practicar, siempre y cuando se realicen de manera responsable y dentro de los límites legales y éticos.

Aprender es el fin, no comprometas la experiencia

1. Enfócate en el aprendizaje: Participa en los CTFs con la mentalidad de aprender y adquirir experiencia. Utiliza cada desafío como una oportunidad para ampliar tus conocimientos y explorar nuevas técnicas y enfoques en seguridad informática.
2. Experimenta y sé creativo: Los CTFs te brindan la libertad de probar enfoques y soluciones creativas. No te límites a una sola forma de resolver los desafíos, sino que experimenta, investiga y prueba diferentes enfoques para ampliar tu conocimiento y habilidades.
3. Colabora con otros: Los CTFs suelen ser una excelente oportunidad para colaborar con otros participantes. Únete a un equipo o busca oportunidades para trabajar junto con otros jugadores. Esto fomentará el intercambio de conocimientos y experiencias, y te permitirá aprender de otros expertos en el campo.
4. Aprovecha los recursos disponibles: Utiliza los recursos proporcionados por los organizadores del CTF, como tutoriales, foros y documentación.

Aprovecha estos recursos para ampliar tus conocimientos y abordar desafíos más complejos.

5. Aprende de tus errores: No te desanimes si no logras resolver todos los desafíos en un CTF. Utiliza los desafíos no resueltos como oportunidades de aprendizaje. Analiza tus errores, busca soluciones y comprende los conceptos detrás de los desafíos que te resultaron más difíciles.

Práctica tu metodología - Try Harder

Establece una metodología clara y estructurada para abordar los desafíos del CTF. Esto puede incluir pasos como el análisis de requisitos, la recopilación de información, la identificación de vulnerabilidades, la explotación, la documentación y la presentación de resultados. Adaptar y refinar tu metodología te ayudará a ser más eficiente y efectivo en tus intentos.

Falla rápido

Identifica y reconoce rápidamente los errores o las ideas que no funcionan, para poder ajustar el enfoque y pivotar hacia una mejor solución.

No hay plataformas inseguras, hay retos de blue team

Las plataformas donde practiques puede que tengan problemas de seguridad, toma esto como una razón para no usarlas o como un reto a tus habilidades defensivas.

https://twitter.com/laprovittera/status/1623698975730593794