Introdução

Este guia destina-se a entusiastas de segurança da informação e que desejam participar de CTFs.

O que são CTFs?

CTF significa Capture the Flag. No contexto de segurança da informação, são competições que envolvem diversas áreas como descoberta de vulnerabilidades, técnicas de espionagem e criação de exploits e ferramentas.

De maneira geral, nessas competições os jogadores são apresentados a problemas, programas com falhas de segurança ou sistemas para serem invadidos. Em cada problema, programa ou sistema, há uma chave secreta ou "flag". Encontrar essa flag é a prova que você resolveu o desafio e enviando no campo especificado faz seu time ganhar pontos.

Tipos de CTFs

Os CTFs são divididos em dois tipos:

Attack-defense

Todos os times recebem uma Máquina Virtual com algumas falhas de segurança. O objetivo é capturar as flags através das vulnerabilidades dos outros times e protegendo seu próprio time de invasões corrigindo suas falhas de segurança.

Jeopardy-sytle

Todos são apresentados a questões de diversas categorias, níveis de dificuldades e pontuações, também chamadas de *challenges*. As categorias variam de competição para competição, as principais são

- **Crypto:** Envolvem problemas relacionados a criptografia.
- **Stegano:** Esteganografia é a arte de esconder em plena vista e que envolve basicamente

mensagens escondidas em outras mensagens.

- **Forensics:** É uma área ampla que pode incluir análise de formato de arquivos, memory dumps e pacotes e até esteganografia.
- **Reversing:** São desafios de engenharia reversa. Envolvem encontrar vulnerabilidades de algum programa que você não possui o código.
- **Web Hacking:** Envolvem atacar vulnerabilidades comuns no ramo de tecnologia web.
- **Programming:** Testam sua habilidade de criar scripts.
- **Miscellaneous:** Problemas variados e normalmente com baixa pontuação.

Quando ocorrem os CTFs?

Esses eventos ocorrem em vários perídos e lugares, sendo organizados por pessoas diferentes. Alguns podem acontecer remotamente (on-line) ou presencialmente (on-site).

Uma ótima plataforma para acompanhar as datas das principais competições é o CTFtime.

Como se preparar para CTFs?

O melhor jeito de se preparar para essas competições é praticando.

Abaixo está uma lista de alguns sites com ótimo conteúdo para treinar.

Para auxiliar esse processo, este guia pretende abordar alguns conceitos básicos para resolver esses desafios de forma didática e rápida.

E ainda, uma ótima forma de treinar é observar resoluções (ou *write-ups*) de desafios que você não conseguiu ou quer ver outra resolução dele.

Onde treinar?

Alguns dos sites abaixo serão usados como exercício para este guia.

WeChall

Plataforma com desafios de diversas áreas e dificuldades.

OverTheWire

Site com diversos *wargames* onde é necessário conectar no respectivo servidor por meio do terminal. O desafio **Bandit** é muito recomendado para aprender comandos de Linux.

picoCTF 2018

A edição 2018 de uma competição muito famosa e voltada para estudantes. Apresenta ótimos desafios introdutórios e de diversas áreas.

Hack The Box

Plataforma voltada para invasão de máquinas, simula cenários reais de *pentest*. Possui também alguns desafios de várias áreas, como os outros, e é preciso "*hackear*" o site para conseguir o login.

Referências

CTF-BR

OpenCTF

Trail of Bits

CTFtime

Revision #4

Created Sat, Oct 6, 2018 6:21 PM by Andrew

Updated Thu, Dec 6, 2018 5:34 PM by Cainotis