IMERSÃO HACKER ÉTICO

BUNKER 003

GUARDIÃO HACKER

A CARREIRA MAIS COBIÇADA E POUCO FALADA

IMERSÃO HACKER ÉTICO

Bug Bounty: Transforme suas Habilidades de Ethical Hacking em Lucro

Você é um entusiasta da segurança cibernética e adora explorar sistemas em busca de vulnerabilidades? Sabia que suas habilidades podem não apenas proteger organizações, mas também gerar uma renda considerável?

Bem-vindo ao mundo do Bug Bounty, onde ethical hackers são recompensados financeiramente por descobrir falhas de segurança em plataformas online. Neste texto, vamos explorar como você pode transformar sua paixão pela segurança cibernética em um negócio lucrativo.

Bug Bounty é um programa de recompensa oferecido por empresas e organizações, que convidam ethical hackers a encontrar e relatar vulnerabilidades em seus sistemas. Essas empresas reconhecem o valor de ter especialistas externos identificando e corrigindo falhas antes que hackers mal-intencionados as explorem. Ao participar de plataformas de Bug Bounty, você tem a oportunidade de colocar suas habilidades em prática e ser recompensado financeiramente por isso.

Existem várias plataformas de Bug Bounty renomadas que atuam como intermediárias entre ethical hackers e empresas em busca de especialistas em segurança cibernética. Algumas das mais populares incluem HackerOne, Bugcrowd e Synack. Essas plataformas fornecem uma variedade de programas de recompensa, com diferentes escopos e critérios, abrangendo desde pequenas startups até grandes empresas de tecnologia.

O processo de ganhar dinheiro com Bug Bounty é relativamente simples. Primeiro, você se cadastra em uma plataforma de sua escolha e preenche seu perfil, destacando suas habilidades e experiência. Em seguida, você explora os programas disponíveis na plataforma e escolhe aqueles que estão alinhados com seus interesses e conhecimentos. Ao identificar uma vulnerabilidade, você relata à empresa por meio da plataforma, que então avalia e valida a descoberta.

IMERSÃO HACKER ÉTICO

Teste de Intrusão de Rede com Kali Linux:

Desvendando as Ferramentas Netdiscover e Nmap

Introdução:

Você já se imaginou como um verdadeiro detetive da segurança cibernética, explorando redes, descobrindo dispositivos ocultos e mapeando vulnerabilidades? Se você está pronto para mergulhar nesse mundo empolgante, o Kali Linux é a sua ferramenta indispensável. Neste tutorial, vamos explorar as poderosas ferramentas Netdiscover e Nmap, que irão levá-lo a um novo patamar no teste de intrusão de rede.

Passo 1:

O Kali Linux é uma distribuição Linux projetada especialmente para testes de segurança e hacking ético. Com uma vasta gama de ferramentas pré-instaladas, ele se tornou a escolha número um para profissionais de segurança cibernética em todo o mundo. Vamos focar nas ferramentas Netdiscover e Nmap, que são fundamentais para mapear e analisar redes em busca de possíveis vulnerabilidades.

Passo 2:

Começaremos com o Netdiscover, uma ferramenta de descoberta de hosts em uma rede. O Netdiscover permite identificar dispositivos ativos na rede, inclusive aqueles que podem estar ocultos ou mascarados. Ao executar o Netdiscover no Kali Linux, você terá uma visão abrangente da topologia da rede, descobrindo endereços IP, MACs e outros detalhes importantes dos dispositivos conectados.

IMERSÃO HACKER ÉTICO

Passo 3:

Agora que temos uma lista de dispositivos ativos na rede, é hora de aprofundar nossa análise usando o Nmap. O Nmap é uma ferramenta de mapeamento de redes poderosa e versátil. Ele permite verificar os serviços em execução nos dispositivos, identificar portas abertas, detectar sistemas operacionais e até mesmo encontrar possíveis vulnerabilidades. Com o Nmap, você terá uma visão detalhada do estado de segurança da rede.

Passo 4:

Vamos colocar o conhecimento em prática! Primeiro, execute o Netdiscover para descobrir os dispositivos ativos na rede. Observe cuidadosamente os endereços IP e MAC dos dispositivos identificados. Em seguida, use o Nmap para realizar uma análise mais aprofundada dos dispositivos e serviços. Utilize opções como -sS (scan TCP SYN), -sV (deteção de versão do serviço) e -O (detecção de sistema operacional) para obter informações valiosas.

Passo 5:

À medida que você ganha experiência, pode explorar ainda mais recursos do Netdiscover e Nmap. O Netdiscover, por exemplo, permite usar filtros para refinar a busca por dispositivos específicos. O Nmap possui uma ampla variedade de opções e scripts personalizados que podem ser usados para testes de segurança mais avançados. Explore e experimente essas opções para aprimorar suas habilidades.

Conclusão:

O teste de intrusão de rede com o Kali Linux e as ferramentas Netdiscover e Nmap abre as portas para o mundo da segurança cibernética. Ao dominar essas ferramentas, você se tornará um especialista em mapeamento de redes, descobrindo vulnerabilidades ocultas

Acesse o https://idhacker.com.br para aprender muito mais