

Como estudar segurança da informação?

- Introdução
- Áreas de atuação
- Material de Estudos

Introdução

Bem vindo ao guia de estudos da WikiSEC, onde tentaremos centralizar o máximo de informações possíveis para o interessado em hacking. Aqui você poderá encontrar materiais para aprender os fundamentos de segurança da informação (ou *information security*, comumente abreviada para **infosec**), ferramentas, áreas de atuação, conceitos e onde se aprofundar em cada um desses itens.

```
Account bits: 0x0214 =
[ ] Disabled          | [ ] Homedir req.    | [X] Passwd not req.  |
[ ] Temp. duplicate   | [X] Normal account  | [ ] NMS account      |
[ ] Domain trust ac   | [ ] Wks trust act.  | [ ] Srv trust act    |
[X] Pwd don't expir   | [ ] Auto lockout    | [ ] (unknown 0x08)   |
[ ] (unknown 0x10)    | [ ] (unknown 0x20)  | [ ] (unknown 0x40)   |

Failed login count: 4, while max tries is: 0
Total login count: 5026

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [probably locked now]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 
```

A primeira coisa a se ter em mente é que segurança da informação é um ramo enorme, requisitando conhecimentos avançados em diversas outras áreas, e que os maiores profissionais da área tendem a ter tido experiência em outras áreas - como administração de sistemas ou desenvolvimento de software - antes de entrar em infosec. Então não espere uma fórmula mágica para virar um grande hacker como nos filmes!

Para seus estudos com infosec, recomendamos que tenha uma familiaridade com o inglês. É possível encontrar bons conteúdos com autoria de brasileiros, mas as suas possibilidades crescem exponencialmente, tanto em quantidade quanto em qualidade, quando se consegue entender conteúdo de autores do mundo todo. E por mais óbvio que isso possa parecer, sempre vale reforçar - prática é o melhor jeito de se aprender. Na página "Material de Estudos" você encontrará canais no youtube, cursos e plataformas onde pode aprender os fundamentos e se aprofundar nos mesmos.

Áreas de atuação

Como você provavelmente pode imaginar, a Segurança está presente em diversas áreas relacionadas à Tecnologia da Informação (e nem se limita ao mundo dos computadores!). É virtualmente impossível para um único hacker se tornar um especialista em todas, mas ter familiaridade e conforto com conceitos de cada uma é muito importante, até para que o estudante possa saber em qual ou quais almeja dedicar mais do seu tempo para se aprofundar.

Segurança em aplicações Web

A segurança na Internet. Sua função mais comum envolve a testagem de sites por possíveis bugs que podem comprometer um site de uma determinada organização - Como explorar falhas no site que permitam a um atacante:

- Executar código no navegador de uma eventual vítima (e consequentemente ter acesso ao seu computador);
 - Acessar, vender ou destruir informações referentes a bancos de dados que estejam operando no site;
 - Comprometer transações financeiras que estejam mal configuradas para seu próprio benefício;
 - Executar ataques de negação de serviço (DoS) que possam acarretar em prejuízos financeiros e/ou de confiabilidade para uma empresa ou órgão público;
- Entre diversos outros.

E por todos esses aspectos, a segurança na Web é um dos setores mais rentáveis e que mais crescem em todo o hacking: *Bug Bounties* é o nome dado para programas oferecidos por algumas empresas para que profissionais testem seus sites - com permissão, obviamente - e tentem achar bugs que possam acarretar em prejuízos direta ou indiretamente caso explorados por atacantes com intenções maliciosas, e os recompensam por isso com base no impacto de seus achados.

Para mais informações:

OWASP Foundation - Fundação com ideal de manter a Web um lugar mais seguro, desenvolvendo FLOSS e com projetos educacionais.

HackerOne

- Plataforma de bug bounties com programas públicos e privados. No painel *Hacktivity* podem ser encontrados detalhes sobre bugs já encontrados, com alguns disponibilizando o relatório fornecido pelo hacker responsável e a recompensa dada pela empresa.

Bugcrowd - Plataforma de Bug Bounty semelhante ao HackerOne.

How to Shot Web - Playlist - Uma série de palestras oferecidas por Jason Haddix, famoso bug bounty hunter, onde ele compartilha suas metodologias de reconhecimento e enumeração.

Segurança em servidores - Red Team e Blue Team

Criptografia

Engenharia Social

Material de Estudos

Materiais sobre tudo relacionado à segurança da informação para buscar conhecimento fora da wiki.

Sites, revistas, autores e podcasts

Daniel Miessler

Nome com reputação na área de segurança da informação, Daniel Miessler possui excelentes guias sobre aprendizado de infosec em seu site, incluindo dicas em construção de carreira e possíveis perguntas para entrevistas. Seu podcast semanal, *Unsupervised Learning*, trata sobre ferramentas e notícias do mundo do hacking e na tecnologia em geral.

Open Source Security Podcast

Criado por Kurt Seifried e Josh Bressers, o podcast trata de diversos temas relacionados à segurança, incluindo falar sobre quaisquer novas notícias, vulnerabilidades e ferramentas que possam ter surgido durante a semana.

Ganesh Gitbook

Gitbook do Ganesh, grupo de infosec do ICMC-USP. Fornece explicações concisas e úteis sobre conteúdos como engenharia reversa, CTFs e criptografia.

Canais no youtube

John Hammond

Tutoriais de hacking e programação abrangendo diversas disciplinas.

IppSec

Writeups de CTFs e challs, como de Hack The Box e TryHackMe.

Hackersploit

Apresenta diversas ferramentas, principalmente as presentes em sistemas como o Kali Linux, explica conceitos e faz walkthroughs de CTFs de uma forma compreensível.

Papo Binário

Canal da comunidade **Mente Binária** sobre tecnologia da informação que busca formar profissionais de TI com conteúdo de qualidade em português.

As aulas deles incluem duas playlists sobre **Engenharia Reversa**, uma com o CERO - Curso de Engenharia Reversa Online e outra com conteúdos gerais; uma playlist de Programação Moderna em C; e outras sobre Binary Exploitation; Curso de Ghidra; Análise de Malware; entre muitas outras.

Null Byte

Apresenta diversas ferramentas e macetes de hacking que podem ser úteis para hackers de todos os níveis de conhecimento.

PwnFunction

Explica diversos conceitos de forma ilustrada e de fácil entendimento, principalmente voltados à área de Web Security.

LiveOverflow

Vídeos sobre diversos assuntos de TI e análises aprofundadas sobre temas de infosec.

STÖK

Caçador de Bug Bounties sueco, faz diversos vídeos sobre automação e reconhecimento para testes em aplicações web, entrevista outros Bounty Hunters e explica as metodologias de cada um, além de tratar de outros assuntos relacionados à segurança.

The Cyber Mentor

Conteúdo sobre tudo que envolve segurança da informação e outras coisas, desde falhas Web e exploração de servidores até debates sobre outros assunto e dicas de marketing pessoal.

Ganesh ICMC

Canal do youtube do grupo de segurança da informação do ICMC-USP, o Ganesh. Playlists que cobrem assuntos desde introduções básicas do Linux e redes de computadores até pwn e engenharia reversa.

Plataformas de Aprendizado

Hackaflag Academy

Plataforma brasileira que inclui laboratórios virtuais e cursos, como de programação e engenharia reversa.

Entre seus conteúdos didáticos está o CERO, ou **Curso de Engenharia Reversa Online** do canal Papo Binário.

Hacker101

Com um laboratório de CTFs e videoaulas sobre falhas em aplicações Web, o Hacker101 é a plataforma de aprendizado da empresa de Bug Bounties **HackerOne**. Note que completar as CTFs te fornece pontos para participar de programas de bug bounties privados, o que pode ser um diferencial caso tenha interesse em entrar nessa área.

Bugcrowd University

De forma análoga ao Hacker101, o Bugcrowd University é uma plataforma de aprendizagem mantida por uma empresa que oferece programas de Bug Bounty. Possui vídeos de introdução à ferramentas como o Burp Suite e bugs, e laboratórios para que você possa testar seus conhecimentos.

PortSwigger Academy

Criada pela mesma empresa que fez o Burp Suite, a Academy da PortSwigger representa um lugar imprescindível para quem planeja aprender sobre falhas para aplicações web, seus conceitos e ameaças que representam, e *bypassing* de filtros e firewalls para que essas falhas possam ser exploradas.

Hack The Box

Laboratórios para Testes de Invasão gratuitos, onde o atacante deve saber fazer o reconhecimento e enumeração de possíveis vulnerabilidades antes de buscar atacá-las. Requer a obtenção de um 'convite' para registrar uma conta, porém.

PentesterLab

Semelhante ao Hack the Box, porém o acesso aos laboratórios é pago e envolve máquinas mais realistas.

TryHackMe

VulnHub

IMPORTANTE: A utilização de plataformas como o Hack The Box envolve a utilização de uma VPN para acesso às máquinas, o que pode te deixar vulnerável - por estar na mesma rede local - aos outros usuários, que podem ter muito mais experiência que você. Use uma VM nateada, rodando

um sistema operacional Linux, para maior segurança.

Udemy

Cursos na Udemy são um excelente ponto de partida tanto para aqueles que já conhecem conceitos do ramo de software quanto para estudantes sem conhecimento prévio. As promoções promovidas pela plataforma também permitem ter acesso a um conteúdo de qualidade de forma acessível, evitando o marketing daqueles que querem pregar nos novos adeptos da área.

Fundamentos de Ethical Hacking - Curso Prático por Marcos Flávio Araújo Assunção

Ensina os fundamentos para qualquer hacker ético que planeja adentrar o mercado de trabalho, tratando de todas as etapas de um teste de invasão e apresenta ferramentas para explorar essas falhas.

Practical Ethical Hacking - The Complete Course por Heath Adams, TCM Security

Criado pelo The Cyber Mentor previamente mencionado, mostra sobre conceitos de pentesting do zero, exploração de Active Directory, e fornece exemplos práticos por meio de boxes como da Hack the Box.

Cheatsheets e Ferramentas

Thug Bounty

Ghidra

GHCQ CyberChef