



# INTRODUÇÃO AO HACKING E PENTEST 2.0

Avaliações:

★★★★★ 4.9

Inicie no mundo do hacking e da segurança da informação com esse incrível curso prático e 100% gratuito.

⌚ 8 HORAS

✉ GUILHERME JUNQUEIRA · LUIZ PAULO VIANA



## CURSO GRÁTIS

[INSCREVER](#)

### VANTAGENS



Certificado de conclusão



Suporte completo e vitalício



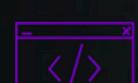
Curso referência na América Latina



Laboratórios com ambientes realísticos



Acesso em qualquer dispositivo



Aulas 100% práticas



8 horas de curso



Acesso vitalício

## O CURSO GRATUITO MAIS COMPLETO DO MERCADO!

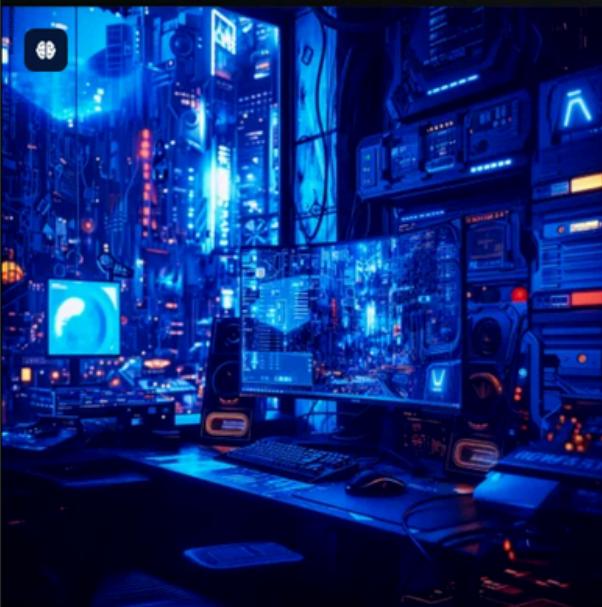
São mais de 8 horas de treinamento, com centenas de aulas e dezenas de laboratórios práticos para você se tornar um especialista em cybersecurity e se inserir de forma profissional no mercado de trabalho. Confira abaixo nossa grade de aulas:



MÓDULO 1

## COMO SER UM HACKER - O QUE É UM PENTEST?

- Blackhat e Whitehat
- As fases do pentest
- Mercado de trabalho
- Certificações
- Bug Bounty
- Qualidades e Habilidades de um hacker ético



MÓDULO 2

## INSTALANDO O SISTEMA DOS HACKERS - KALI LINUX

- Introdução ao Kali Linux
- Virtualização com VirtualBox



MÓDULO 3

## INTRODUÇÃO AO KALI LINUX

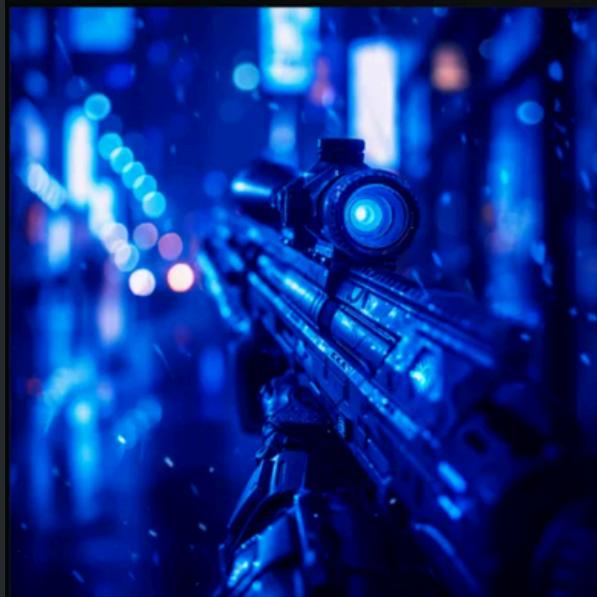
- Introdução ao sistema operacional Linux
- Permissões no Linux
- Principais comandos no terminal



MÓDULO 4

## FOOTPRINTING - COLETA DE INFORMAÇÕES

- Whois
- Enumeração DNS
- Ferramentas de enumeração DNS
- Transparéncia de certificado



MÓDULO 5

## RECONHECIMENTO COM NMAP - ANALISANDO O ALVO

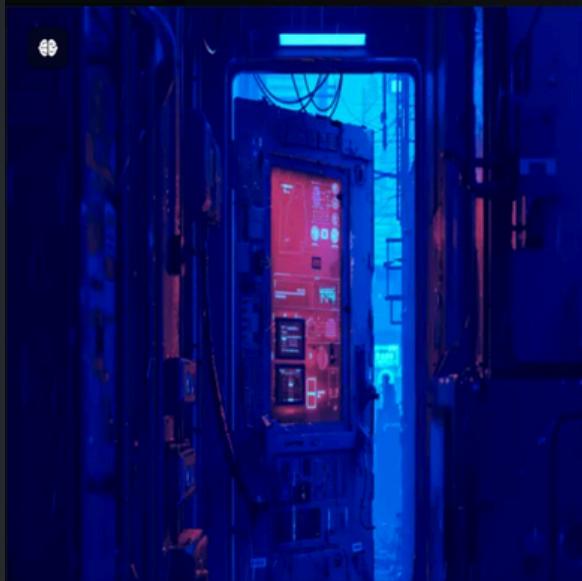
- Introdução a redes de computadores
- Netcat
- Port scanning com Nmap



MÓDULO 6

## CRIANDO SUAS PRÓPRIAS FERRAMENTAS HACKER

- Editando arquivos pelo terminal
- Introdução ao Python
- Criando um port scanner com Python
- Criando uma ferramenta de brute force de subdomínios com Python



## MÓDULO 7

# RECONHECIMENTO WEB - ENCONTRANDO VULNERABILIDADES

- Backend e Frontend
- Analise manual da aplicação web
- Wappalyzer
- Webcrawling
- Introdução ao Google Hacking
- Introdução ao protocolo HTTP
- Burlando Web Application Firewalls
- Identificando SQL Injection
- Identificando Cross Site Scripting
- Procurando por exploits

## MÓDULO 8 - SQL INJECTION - ATACANDO O SERVIDOR



## MÓDULO 8

# SQL INJECTION - ATACANDO O SERVIDOR

- Introdução ao SQL
- Entendendo o SQL Injection
- Explorando o SQL Injection manualmente
- Injetando código SQL na aplicação
- Extraíndo dados do Banco de Dados com SQLi
- Quebrando Hash MD5
- Tipos de SQL Injection
- SQL Injection com SQLMAP

## MÓDULO 9 - CROSS-SITE SCRIPTING (XSS) - ATACANDO O CLIENTE



## MÓDULO 9

# CROSS-SITE SCRIPTING (XSS) - ATACANDO O CLIENTE

- Entendendo o Cross-Site Scripting (XSS)
- Security Headers
- Roubo de sessão
- Criando exploit XSS com javascript
- Criando um link malicioso para roubar contas



MÓDULO 10

## SHELL UPLOAD - INVADINDO O SERVIDOR COM SHELL REVERSA

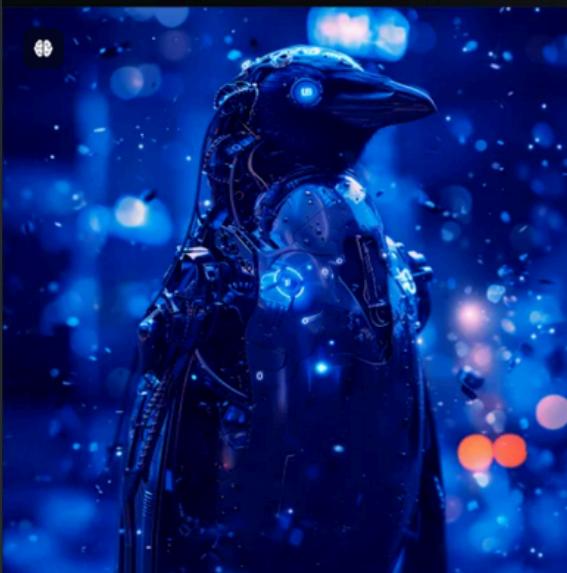
- Identificando Vulnerabilidade de Shell Upload
- Burlando restrições de upload de arquivos
- Remote Code Execution
- Criando WEB Shell em PHP
- Criando uma Shell Reversa
- Realizando ataques externos com Ngrok



MÓDULO 11

## POST EXPLOITATION, HASHING E CRIPTOGRAFIA

- Melhorando Shell Reversa
- Enumerando o sistema
- Procurando por informações sensíveis
- Fazendo dump do banco de dados
- Entendendo a criptografia
- Entendendo como as Hashs funcionam
- Ataque de força bruta em senhas com John The Ripper
- Quebrando hashes do Linux



MÓDULO 12

## LINUX PRIVILEGE ESCALATION - OBTENDO MAIORES PRIVILÉGIOS

- Criando script de reconhecimento de rede em Bashscript
- Acessando host interno por SSH
- Ferramentas de pós-exploração Linux
- Técnicas de escalação de privilégios
- Identificando programas vulneráveis
- Procurando por exploits de escalação de privilégios
- Transferência de arquivos com Netcat
- Compilando exploit em C
- Escalando privilégios para root com exploit
- Criando uma reverse shell persistente



MÓDULO 13

## PIVOTING - COMPROMETENDO TODA A REDE

- Enumerando a rede interna com Nmap
- Identificando e enumerando serviços
- Acesso anônimo FTP
- Extraíndo arquivos sensíveis pelo FTP
- Invadindo host interno pelo SSH com chave privada
- Analisando crontabs
- Privilege escalation com injeção de código malicioso em binário inseguro



MÓDULO 14

## ELEVANDO SEU NÍVEL - POR DIVERSÃO E LUCRO

- Resumo do curso
- Outras técnicas e ataques
- Próximos passos

# TRILHAS DE FORMAÇÃO SOLYD ONE



**SYCP**  
Solyd Certified Pentester  
Comprove sua expertise em todas as etapas de um Pentest Web completo



**SYWP**  
Solyd Wireless Pentester  
Comprometa redes Wi-Fi através das últimas técnicas de exploração



**SYH2**  
Solyd Hardware Hacker  
Torne-se um Hardware Hacker criando seu próprio gadget de hacking



**SYAP**  
Solyd Android Pentester  
Explore aplicações Android de utilizando as técnicas mais atuais



**SYES**  
Solyd Evasion Specialist  
Se especialize em pós-exploração e evasão de defesas avançadas