



PYTHON **para Pentest**

novatec

Daniel Moreno

Resumo de Python Para Pentest

Python é a linguagem preferida dos profissionais de segurança da informação. Fácil de aprender, multiplataforma, e com uma enorme variedade de bibliotecas que podem ser aproveitadas em pentest de redes, aplicações web e redes sem fio.

Este livro mostra como criar ferramentas em Python para pentest, com muitos exemplos de código-fonte, que podem ser executados em qualquer versão do Kali Linux. Destina-se a profissionais de segurança da informação, com conhecimentos de Python e pentest, interessados em utilizar Python para criar suas próprias ferramentas para pentest.

O livro é dividido em quatro capítulos. O primeiro, Introdução ao Python, fornece o conhecimento básico para os capítulos posteriores. O segundo, Pentest em redes, mostra as ferramentas que podem ser usadas em um pentest de redes corporativas.

O terceiro, Pentest em aplicações web, mostra como criar ferramentas para automatização de ataques em aplicações web. E o quarto, Pentest em redes sem fio, automatiza ataques voltados às redes sem fio.

Com este livro você aprenderá a: Utilizar scripts Python encontrados na internet e criar os próprios. Criar cavalos de troia, backdoors e scripts para Windows e Linux. Automatizar o uso de exploits e controle de browsers, integrando o Python ao Metasploit e ao BEEF.

Ter controle do Internet Explorer, manipulando os dados entre o usuário e o site destino. Redirecionar portas e tunelamento de dados. Realizar ataques de pouca banda (low band), paralisando sites via DoS.

Criar interface gráfica para administração de redes zumbis em ataques DDoS. Infectar arquivos executáveis de pendrive com o payload do Metasploit. Realizar ataques de força bruta contra sites e o Facebook.

Monitorar o tráfego de redes sem fio. Utilizar processamento distribuído para a quebra de senhas WPA/WPA2 PSK.

[Acesse aqui a versão completa deste livro](#)