

Fundamentos de Pentest

Cassiano Peres

DIO Tech Education Analyst

 cassiano-dio

 peres-cassiano

Objetivo Geral

Nesta aula vamos explorar conceitos e práticas sobre Deep Web e Dark Web.

Pré-requisitos

Este curso abordará conceito um pouco mais avançados sobre redes de computadores, sistemas operacionais e ferramentas. Para isto é recomendado um conhecimento prévio nestes assuntos.

Percurso

Etapa 1

O que é Pentest?

Etapa 2

Fases do Pentest

Etapa 3

Definindo uma proposta de Pentest

Percurso

Etapa 4

Escrevendo um relatório de Pentest

Etapa 1

O que é Pentest?

Introdução

Nesta aula vamos falar sobre Pentest, um recurso muito utilizado para buscar e avaliar vulnerabilidades em redes e sistemas.

Pentest

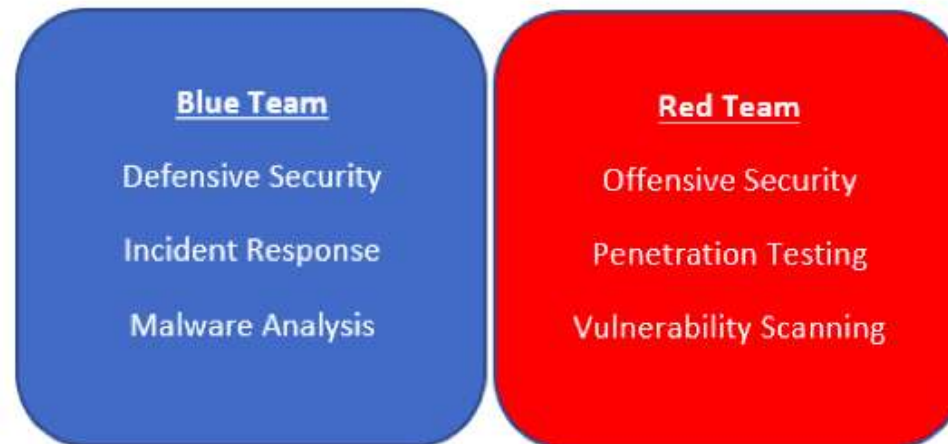
O Pentest, ou *Penetration Test*, busca detectar e explorar vulnerabilidades em um sistema, para fim de validar a eficácia dos mecanismos de segurança e melhorá-los.



Pentest

O Pentest não significa uma invasão deliberada do sistema, há um conjunto de regras definidas em contrato entre a empresa e o hacker ético.

Pentest



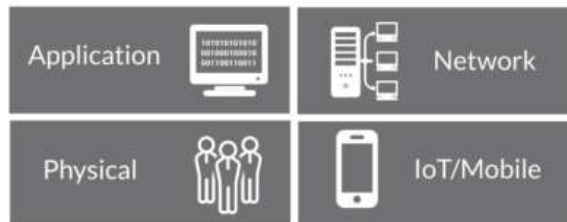
Pentest

WHAT IS A PENETRATION TEST?



An authorized attack on a computer system, network, or application to identify security vulnerabilities bad actors might exploit.

Types of Penetration Tests



The Process



Why Conduct a Penetration Test?



Identify security vulnerabilities

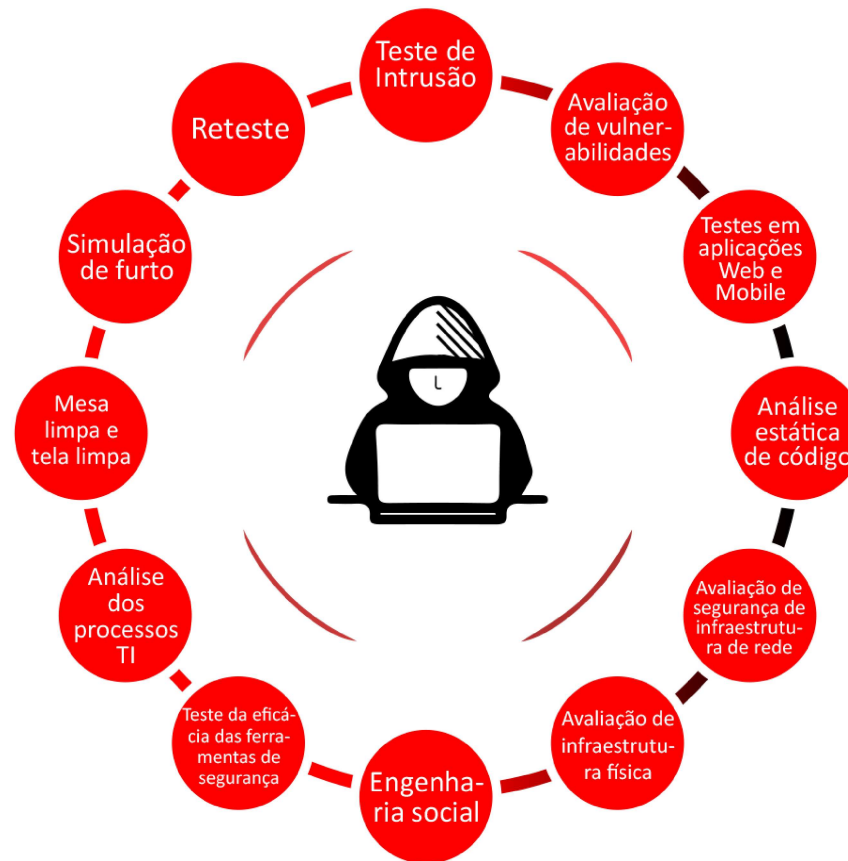


Validate compliance with policies



Evaluate effectiveness of defenses

Pentest



Tipos de Pentest

Um Pentest é classificado de acordo com o nível de conhecimento do atacante sobre o alvo.

Possui três categorias básicas:

- White Box
- Grey Box
- Black box

Tipos de Pentest

| | Black-Box <i>aka close box penetration testing</i> | Grey-Box <i>combination of black box and white box testing</i> | White-Box <i>aka open box penetration testing</i> |
|--------------|--|---|--|
| Goal | Mimic a true cyber attack | Assess an organization's vulnerability to insider threats | Simulate an attack where an attacker gains access to a privileged account |
| Access Level | Zero access or internal information | Some internal access and internal information | Complete open access to applications and systems |
| Pros | Most realistic <i>Testing is performed from point of view of attacker</i> | More efficient than black-box and saves on time and money <i>Testing is performed from point of view of attacker</i> | More comprehensive, less likely to miss a vulnerability and faster <i>Testing is performed from point of view of attacker</i> |
| Cons | Time consuming and more likely to miss a vulnerability | No real cons for this type of testing | More data (ex, source code) is required to be released to the tester and more expensive |

Vulnerabilidades buscadas

- Usuários;
- Redes;
- Configurações;
- Dispositivos;
- Softwares;
- Aplicações.

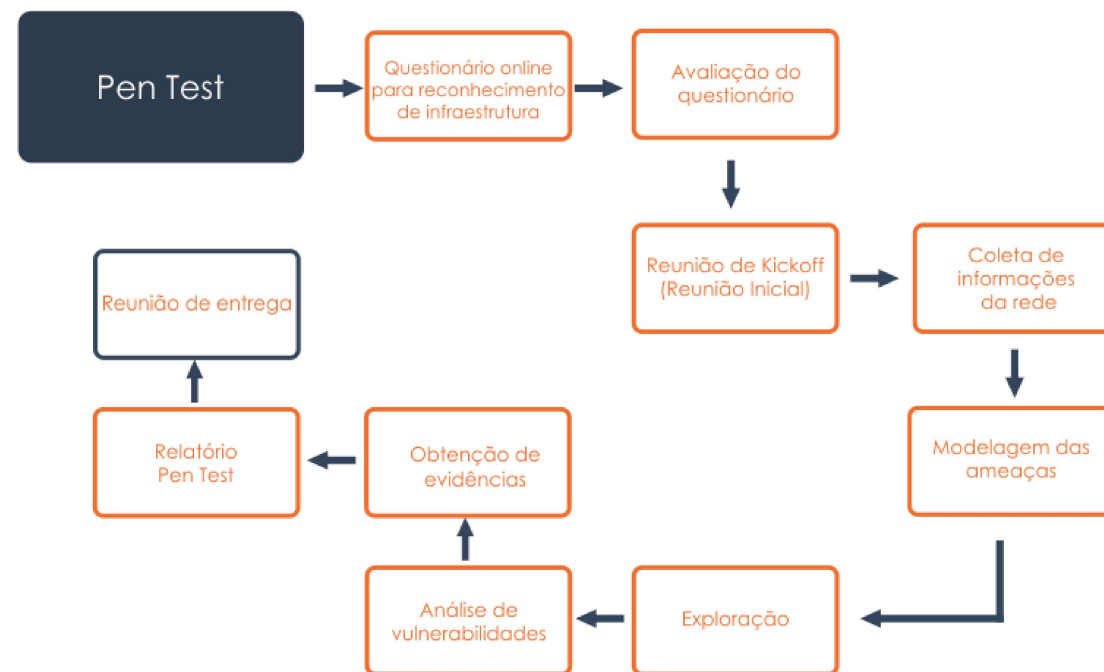
Etapa 2

Fases do Pentest

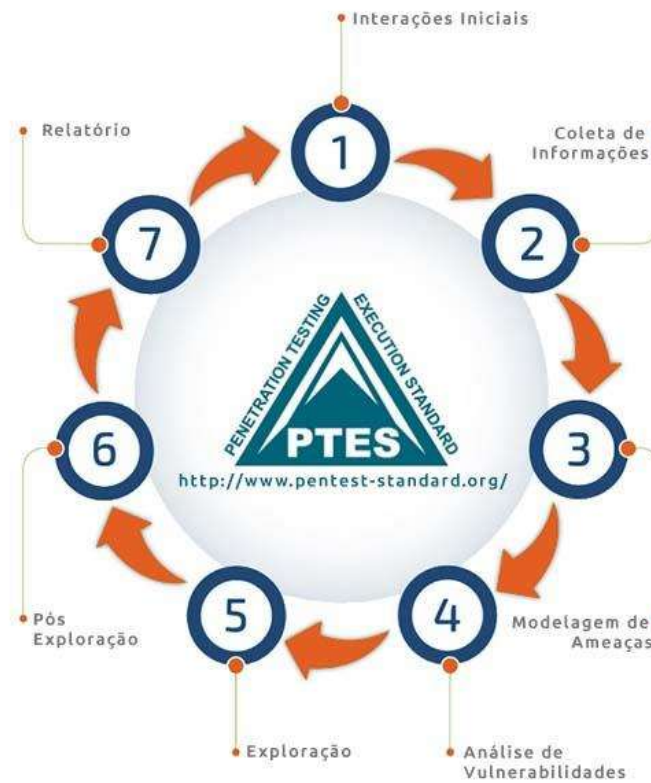
Introdução

Nesta aula vamos conhecer as etapas do Pentest e explorar cada uma delas

Introdução



Fases do Pentest



Interações iniciais

É nesta parte que a empresa contratante e o hacker ético definem o escopo, prazos, valores e os limites do teste.

Coleta de informações

Nesta etapa é feito o reconhecimento do local a ser “atacado”, coletando informações que basearão as etapas seguintes, empregando OSINT.



Modelagem das ameaças

Identifica os objetivos e vulnerabilidades para definir contramedidas visando prevenir ou mitigar os efeitos de ameaças ao sistema.

Análise de vulnerabilidades

Fase de descoberta e validação das vulnerabilidades, onde são encontrados os problemas dos sistemas.

Exploração

Aqui o testador tenta atingir a segurança do sistema de destino usando as vulnerabilidades previamente identificadas e validadas

Pós-exploração

Nesta fase o pentester mantém o controle sobre o sistema analisado e realiza a coleta de dados.

Relatório

O pentester documenta todo o processo de uma forma compreensível para o cliente, apresentando as conclusões sobre a segurança do sistema analisado.

Conclusão

Nesta aula conhecemos as fases do Pentest, baseadas no Framework PTES, que servirá de base para as aulas seguintes.

Etapa 3

Definindo uma proposta de Pentest

Introdução

Nesta aula vamos falar sobre a elaboração de uma proposta de Pentest para um possível cliente.



Proposta

Segue os moldes de uma proposta comercial para o desenvolvimento de um sistema.

Tópicos

- Descrição da empresa/profissional;
- Escopo e metodologia;
- Valores;
- Assinaturas.

Prática

Vamos explorar um exemplo de documento de proposta de Pentest.

Etapa 4

Escrevendo um relatório de Pentest

Introdução

Após a elaboração da proposta, aceite e execução do Pentest, é gerado um relatório com as vulnerabilidades da empresa contratante.

Informações importantes

- Contratante;
- Empresa/profissional pentester contratado.

Tipos de relatórios

- Técnico;
- Gerencial.

Técnico

- Introdução com detalhes técnicos;
- Informações;
- Vulnerabilidades existentes;
- Más configurações;

Técnico

- Exploração e pós-exploração
- Descrição de riscos e perdas
- Documentação

Gerencial

- Histórico de descrição do teste;
- Problemas encontrados;
- Atual postura de risco da empresa;
- Recomendações para correção e prevenção

Conclusão

É importante desenvolver um relatório com informações claras para o público alvo, se técnico ou gerencial.

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

