AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

Teste de Intrusão em Aplicações Web

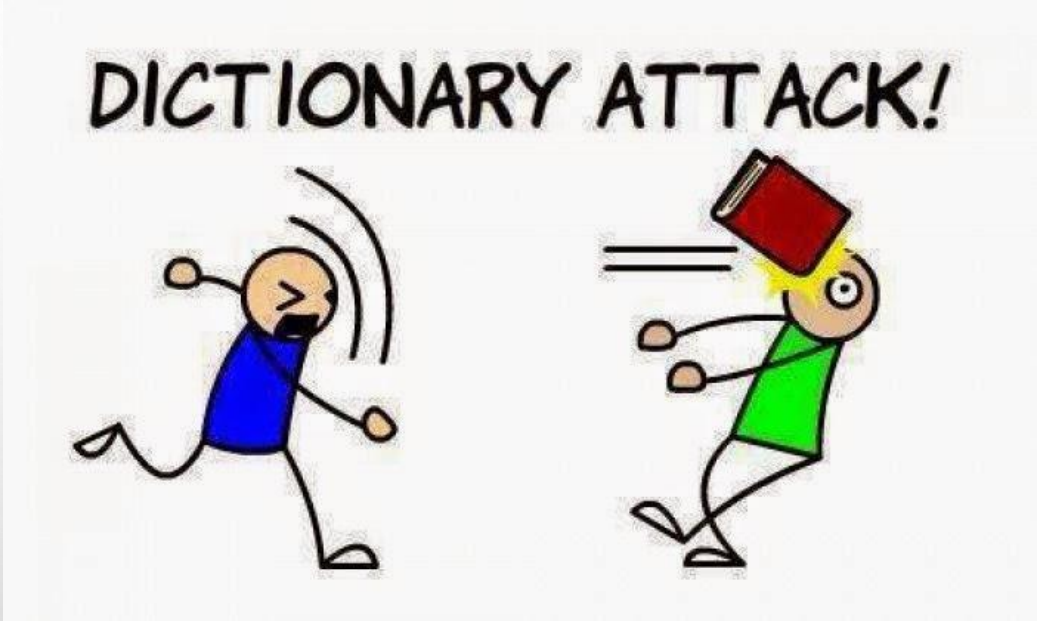
Projeto de Pentest

TESTE DE SEGURANÇA É

HACKING PENTEST AUDITORIA

E o objetivo é...?

TERMINOLOGIA ESSENCIAL



TERMINOLOGIA ESSENCIAL

White Hats – especialistas em segurança

Black hats - conhecimento para atividades ilegais

Script kids – sem habilidades de hacking, usa ferramentas de terceiros

TERMINOLOGIA ESSENCIAL

Crackers- Ganho pessoal

Phreaks – invasão de redes telefônicas

Insiders – do lado de dentro. <=50%

-Não é Hacking, foco no pentest

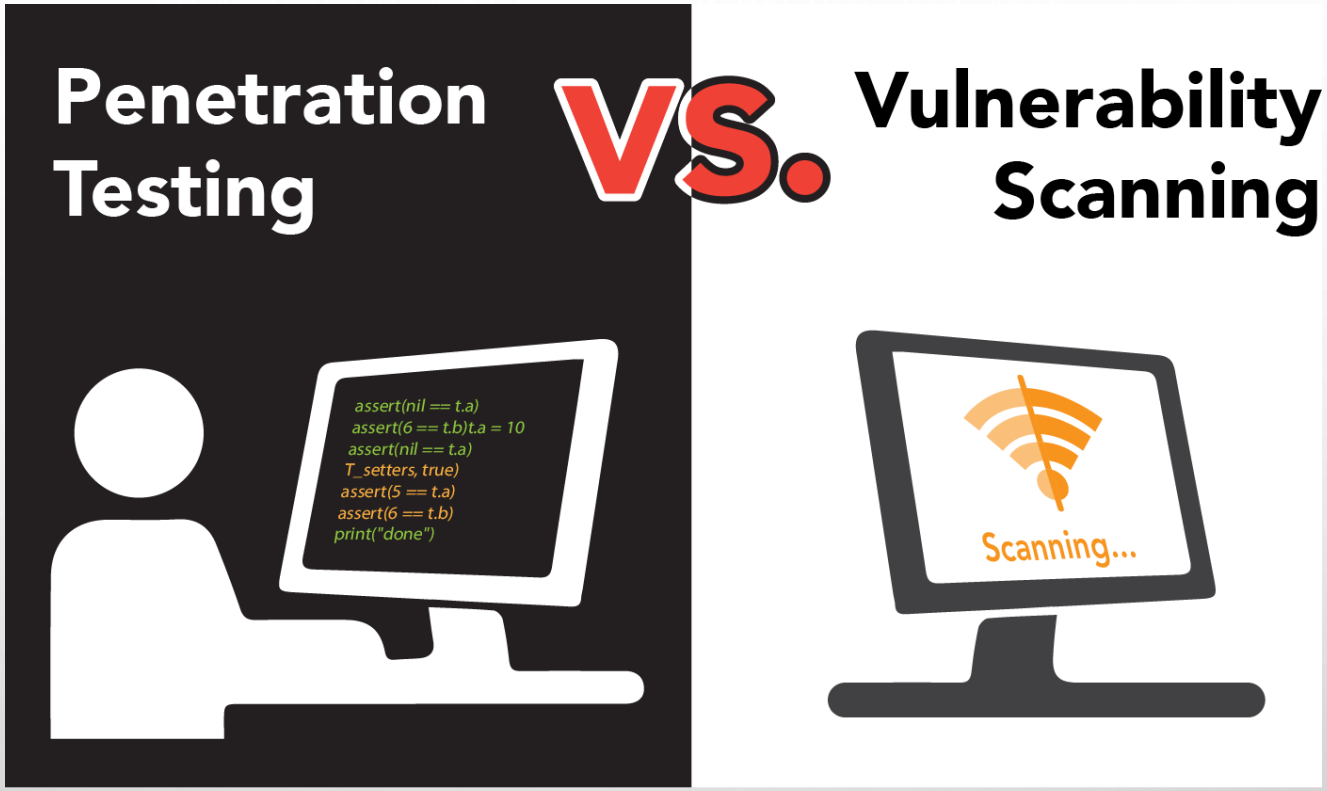
-Só iniciam teste após autorização legal

-Conduzido de maneira estruturada e organizada

-Confidencialidade de informações

-Há a concordância do cliente com os testes: DOS, etc

ANÁLISE DE VULNERABILIDADE X PENTEST



Ambos buscam brechas ou vulnerabilidades

ANÁLISE DE VULNERABILIDADE

-Podem ser feitas com analisadores de vulnerabilidades e podem necessitar testes manuais

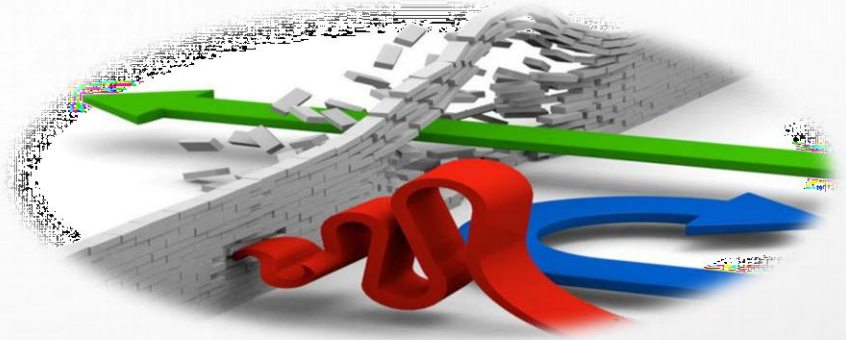
-O processo é identificar, quantificar e priorizar as vulnerabilidades em um sistema

Criatividade e conhecimento são fatores de sucesso

-Permite ao negócio entender se as estratégias de mitigação empregadas estão funcionando conforme o esperado

-**Explora** vulnerabilidades com objetivo de ganhar acesso ao sistemas e dados.

PENTEST



Exige maior nível de habilidade do que é necessário para a análise de vulnerabilidade.

Isso significa que o *preço de um teste de invasão (tempo x recursos)* será *maior que a de uma análise de vulnerabilidade*.

Atenção voltada às vulnerabilidades que possam conduzir a uma significativa perda de receitas, a menos que sejam tratadas

COMO ENCONTRAR EQUILÍBRIO?

Varredura

Quão rápido e amplamente posso analisar a superfície?

Exploratório (Pentest)

-Que tipos de ataques são relevantes?

-Qual a parte mais importante a ser protegida: **mais impacto, maior risco ao negócio?**

COMO ENCONTRAR EQUILÍBRIO? VALOR X PRODUTIVIDADE

Explorar pentest + varredura = done

Teste continuo+Sprint pequeno +
Restropectivas+ muito feedback+
envolva o time

ABORDAGENS DE PENTEST

Quanto a execução:

-Manual, automatizado, combinação

Quanto ao conhecimento sobre o sistema:

-Black-box, Grey-box, White-box

ABORDAGENS DE PENTEST

Quanto ao conhecimento sobre o sistema:

Black Box

Gray Box

White Box

Black Box

ABORDAGENS DE PENTEST

- -SEM INFORMAÇÕES PRÉVIAS,
- MUITAS VARIÁVEIS DESCONHECIDAS (BLIND TESTING)
- -DEMANDA MUITO MAIS TEMPO
- -CENÁRIO REALÍSTICO PORÉM VASTO

ABORDAGENS DE PENTEST

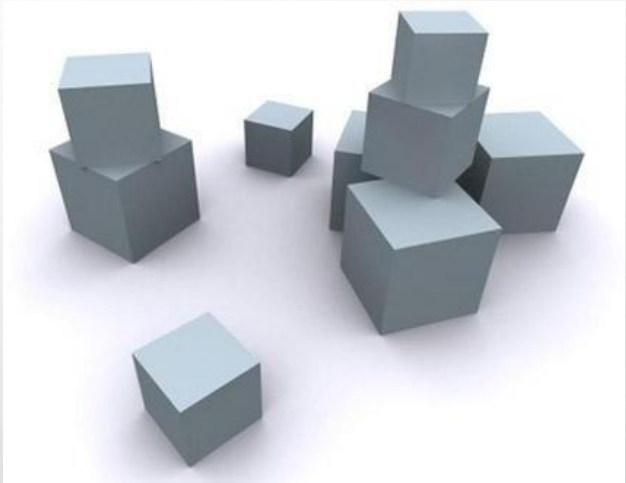
- "FULL DISCLOSURE" TESTING: IP, CÓDIGO FONTE, PROTOCOLOS, RNS,
- FUNCIONALIDADES, ETC

- RISCO DE CENÁRIO NÃO REALÍSTICO
- É MAIS DETERMINÍSTICO PORQUE O PENTESTER TEM INFORMAÇÕES PRIVILEGIADAS E PODE EXECUTAR TESTES MAIS RIGOROSOS E ABRANGENTES

- -MAIS EFICIENTE EM CUSTO X BENEFÍCIO QUE O CAIXA PRETA POIS N GASTA TEMPO COM ESCONDE-ESCONDE.
- -PODE INCLUIR ÁREAS DE ANÁLISE DE CÓDIGO, MANEIRA E EFICAZ D ENCONTRAR VULNERABILIDADES ORIGINARIAS DE CÓDIGO

ABORDAGENS DE PENTEST

Gray Box



-Conhece detalhes parciais

-Incorpora elementos de ambos

FERRAMENTAS PARA TESTADORES E DESENVOLVEDORES

SAST (Static Application Security Testing)

OWASP LAPSE + JAVA EE
https://www.owasp.org/index.php/OWASP_LAPSE_Project

FxCop .NET
https://www.owasp.org/index.php/FxCop

RIPS PHP
http://sourceforge.net/projects/rips-scanner/

GRAUDIT
Suporta: php, asp, perl e python
http://www.justanotherhacker.com/projects/graudit/download.html

O PLANO DE TESTE: FASES E ESCOPO

FASES DE UM PENTEST

-Modelagem de ameaças
-Interações pré- noivado (escopo, objetivo, reuniões)
-Coleta de informação (analisadores, eng. Social, etc)
-Análise de Vulnerabilidade
-Exploitation (explorar para tirar vantagem)
-Pós Exploitation (mais analise e decisão)
-Relatórios

O PLANO DE TESTE NO ESCOPO DA SEGURANÇA

Antes de começar...

-Qual é a finalidade do teste?

-Quem tem a autoridade para autorizar o teste?

-Qual é o prazo proposto para o teste?

-Há alguma restrição sobre quando o teste pode ser executado?

-O seu cliente percebe a diferença entre teste de invasão de análise de vulnerabilidade?

-Necessitará cooperação de outros times?

O PLANO DE TESTE NO ESCOPO DA SEGURANÇA

Antes de começar...

-É permitido engenharia social e negação de serviço?

-Terá acesso a informações de tecnologia: bd, redes, servidores, tecnologia app servidor?

-Há restrição de range de IP para teste?

-Se o objetivo for alcançado no começo dos teste, continua ou para?

O PLANO DE TESTE NO ESCOPO DA SEGURANÇA

Antes de começar...

-Existem implicações legais: sistemas de países diferentes? Plug-ins de terceiros?

-Precisa de permissões ou usuários adicionais para o teste?

É possível realizar transações no Bd durante o teste?

Usabilidade é essencial nas recomendações de segurança?

O time de DevOP é Ágil? Entrega continua, integração continua, incremental

IDENTIFIQUE CENÁRIOS DE RISCOS, SEMPRE!!!

Se não sabe onde olhar, como encontrar valor?