**Estudo Pen Test** Aula 11. 2.5 - Fases de um teste de invasão

Hacker ético = Penetration Test

**Tipos de Teste**

**Caixa Preta [Black box]** = Teste realizado em um sistema remoto, **sem nenhum conhecimento do alvo**. O invasor deve partir da estaca zero, sem informações sobre endereços IPs públicos, sistemas operacionais utilizados, tipos de roteadores e firewalls, etc. Esse teste visa demonstrar a visão de um atacante de fora da intranet da empresa.

**Caixa Cinza [Gray Box]** = Teste realizado entre departamentos ou sub-redes de uma intranet, **com conhecimento parcial da estrutura**. O objetivo desse teste é demonstrar até que ponto um funcionário consegue chegar caso ele decida tentar acessar um sistema de outro departamento ao qual ele não tem acesso legitimo. Nesse tipo de PenTest, temos conhecimento parcial da rede, como a faixa de endereços IPs utilizada na sub-rede de origem, o endereço IP do gateway do servidor DNS, etc.

**Caixa Branca [White Box]** = Teste realizado em uma intranet local, **com total conhecimento do alvo**. Nesse teste, temos o conhecimento total de como a rede opera, sabemos todos os dispositivos, endereços e sistemas operacionais utilizados. A visão de um teste White Box é a de um administrador de rede. Essa metodologia de testagem é utilizada quando desejamos conhecer até onde um administrador poderá ir caso deseje acessar dados ou obter informações, tais como conversar de MSN, senhas de usuários, e-mails alheios, etc.

**Níveis**

1 - Júnior = Iniciante

2 - Pleno = Mediano

3 - Sênior = Avançado

NDA - Termo a ser fechado com a empresa sobre a “Invasão”.

**Relatórios**

**Sumário executivo** - Este relatório é **preparado para os executivos da empresa.** Ele condensa todos os problemas de uma forma mais visual, utilizando gráficos e tabelas para sintetizar todas as vulnerabilidades detectadas e as sugestões para as correções das mesmas. Não possui informações técnicas profundas.

**Relatório Técnico** - Esse relatório é **preparado para os profissionais de segurança da empresa**. Ele explica em detalhes todas as vulnerabilidades encontradas, mostrando tela a tela o resultado da exploração de cada problema, o impacto e uma sugestão de correção. È apresentado como se fosse um “tutorial” do que foi feito.

www.pentest-standart.org

**Certificações**

Exin

CEH

GPEN

GWAPT

Offensive security OSCP

**Links para estudo**

**Livros**

Livro Teste de Invasão - jorga weidman

Wireless Hacking - Autor curso