Segurança da Informação

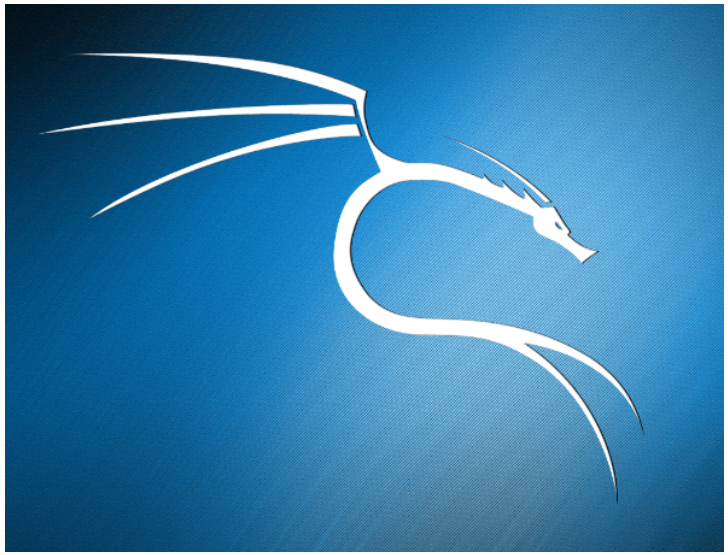
Prevenção de Ataques e Defesas
Utilização do Kali Linux

Prof. Fábio Henrique Ribeiro Machado
fabiohenriquerm@gmail.com

O que é Kali Linux

» **Kali Linux** é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança.

https://www.kali.org/



Teste de Invasão e Configuração

» Muitas organizações oferecem serviços de segurança e de uso de termos tais como auditoria de segurança,

rede ou avaliação de risco, e Penetration Test sendo a mesma coisa.

» Por definição, uma auditoria é uma avaliação técnica mensurável de um sistema (s) ou aplicativo (s).
As avaliações de segurança são as avaliações de risco, ou seja, os serviços usado para identificar vulnerabilidades em sistemas, aplicações e processos.

Teste de Invasão e Configuração

» Um teste de penetração tentaria atacar vulnerabilidades da mesma maneira como um hacker malicioso para verificar quais vulnerabilidades são genuínos reduzir a lista verdadeira das vulnerabilidades do sistema para um punhado de falhas de segurança;

» O Teste de Invasão não tornar as redes mais seguras!

Teste de Invasão e Configuração

» Posicionando um escopo adequado de trabalho é fundamental quando a venda de serviços de testes de penetração.

» O escopo do trabalho define o que os sistemas e as aplicações estão a ser alvo, bem como o que conjuntos de ferramentas podem ser usadas para comprometer vulnerabilidades que são encontradas.

Teste de Invasão e Configuração

» Melhores práticas está a trabalhar com o seu cliente durante uma sessão de design para desenvolver um escopo aceitável de trabalho que não tem impacto sobre o valor dos resultados.

» Teste de Invasão Web com Kali Linux irá fornecer-lhe passo-a-passo métodos para encontrar vulnerabilidades e exploração de aplicações web.

Teste de Invasão aplicação Web conceitos

» A aplicação web é qualquer aplicativo que usa um navegador web como um cliente.

» As aplicações web oferecem facilidade de acesso a serviços e gerenciamento centralizado de um sistema utilizado por várias partições. Requisitos para acessar um aplicativo web pode seguir padrões de cliente navegador, simplificando as expectativas, tanto do prestadores de serviços, bem como os usuários ao acessar o aplicativo.

Teste de Invasão aplicação Web conceitos

» Aplicações web de teste de penetração podem variar em escopo já que há um grande número de tipos de sistema e os casos de uso de negócios para serviços de aplicativos web.

» O núcleo das camadas web de aplicações que são servidores de hospedagem, dispositivos de acesso e depósito de dados deve ser testada, juntamente com a comunicação entre as camadas durante uma teia exercício Teste de Invasão aplicação.

Teste de Invasão aplicação Web conceitos

» Um exemplo para o desenvolvimento de um escopo para um teste de penetração de aplicações web é o teste

aplicações de um servidor Linux de hospedagem para dispositivos móveis.

» O escopo do trabalho em um mínimo deve incluir a avaliação do servidor Linux (sistema operacional, rede configuração, e assim por diante), as aplicações alojadas no servidor, como os sistemas e usuários autenticados, dispositivos clientes que acessam o servidor e a comunicação entre todos os três níveis.

Teste de Invasão aplicação Web conceitos

» Outras áreas de avaliação que podem ser incluídos no âmbito de trabalho são os dispositivos que são utilizados por funcionários, como os dispositivos são usados de fora para acessar o aplicativo, a rede (s) circundante, a manutenção dos sistemas, e os usuários dos sistemas.

» Cada escopo do trabalho deve ser personalizado em torno de objetivos de negócio do seu cliente, prazo esperado de desempenho, recursos alocados, e resultado desejado. Como afirmado anteriormente, os modelos servem como ferramentas para melhorar uma sessão de design para o desenvolvimento de um escopo de trabalho

Metodologia Teste de Invasão

» Há passos lógicos recomendados para a realização de um teste de penetração.

» O primeiro passo é identificar o status de iniciar o projeto. A terminologia mais comum definindo o estado de partida é Caixa-preta teste, Caixa branca teste, ou uma mistura entre branco e preto teste de caixa conhecido como Caixa cinza teste.

Metodologia Teste de Invasão

» Caixa preta assume o verificador da penetração não tem conhecimento prévio do alvo rede, os processos da empresa, ou serviços que fornece.

» Iniciando um projeto de caixa preta requer uma grande quantidade de reconhecimento e, tipicamente, é um acoplamento mais com base no conceito que os atacantes do mundo real podem passar longos períodos de tempo estudando alvos antes de lançar ataques.

Metodologia Teste de Invasão

» Caixa branca é quando um verificador da penetração tem conhecimento íntimo sobre o sistema. Os objetivos do teste de penetração são claramente definidos e os resultados do relatório a partir do teste é normalmente esperado. O testador foi fornecido com detalhes sobre

o alvo, tais como informações sobre a rede, o tipo de sistemas, processos da empresa, e serviços.

Teste de caixa branca, tipicamente é focada em um objetivo de negócio específico, tais como a uma necessidade conformidade, em vez da avaliação genérico, e pode ser um engate mais curto, dependendo da forma como o espaço-alvo é limitado.

Metodologia Teste de Invasão

» Teste de caixa cinza cai entre preto e teste de caixa branca. É quando a cliente ou sistema proprietário concorda que algumas informações desconhecido acabará ser descoberto durante uma fase de reconhecimento, mas permite que o verificador da penetração para pular esta parte.

O verificador da penetração é fornecido alguns detalhes básicos do alvo; no entanto, funcionamento interno e algumas outras informações privilegiadas ainda é mantido do verificador da penetração.

Metodologia Teste de Invasão

» Um grupo de segurança interna geralmente executa teste de caixa branca.

Metodologia Teste de Invasão

Alguns fundamentos para o desenvolvimento de um espaço de trabalho para um teste de penetração são como se segue:

- Definição do sistema de destino
- Prazo do trabalho realizado
- Como as metas são Avaliado
- Ferramentas e software
- Foi comprometida e a dificuldade de explorar
- Acesso Inicial Nível
- Definição de Espaço Público-alvo
- Identificação de Áreas de operação crítica
- Resultados e Análises