Segurança da Informação

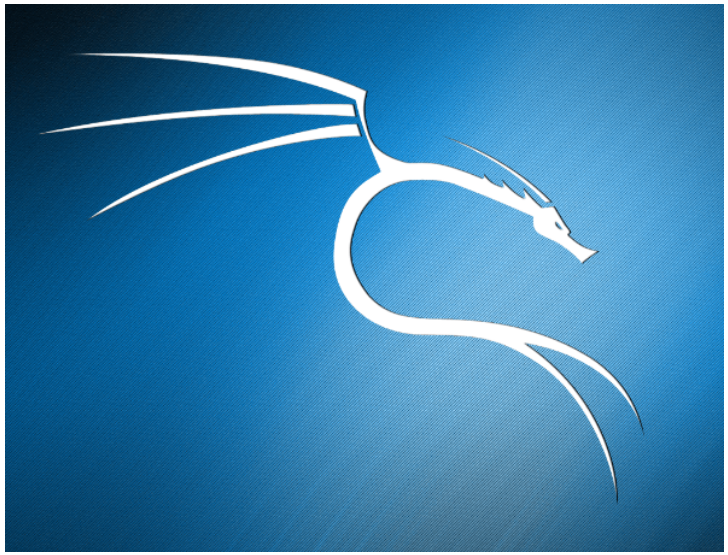
Prevenção de Ataques e Defesas
Utilização do Kali Linux

Prof. Fábio Henrique Ribeiro Machado
fabiohenriquerm@gmail.com

Distribuição Kali Linux

» Possui ferramentas para Pentest (Penetration Test), indicado para profissionais Ethical Hacker também chamado de Pentester.

KALI
BY OFFENSIVE SECURITY



Visão geral ferramentas Kali

» Kali Linux oferece uma série de ferramentas personalizadas concebidas para testes de penetração.

Ferramentas são classificadas por grupos no menu drop-down “Aplicativos” na barra de tarefas do Kali;

Visão geral ferramentas Kali

» **Coleta de Informações:** são ferramentas de reconhecimento utilizados para coletar dados

em sua rede alvo e dispositivos. Ferramentas variam de identificar os dispositivos a protocolos utilizados;

» **Análise de Vulnerabilidade:** concentra em sistemas de avaliação de vulnerabilidades. Normalmente, estes são executados em sistemas encontrados usando a

coleta de informações ferramentas de reconhecimento;

Visão geral ferramentas Kali

» **Aplicações Web:** Estas são ferramentas utilizadas para auditar e explorar vulnerabilidades em servidores web. Muitas das ferramentas de auditoria utiliza a partir desta categoria. No entanto aplicações web nem sempre se referem de ataques contra servidores web, eles podem simplesmente ser ferramentas baseadas na Web para serviços de rede. Por exemplo, a web proxies será encontrado em nesta seção.

Visão geral ferramentas Kali

» **Senha Ataques:** Esta seção de ferramentas lida principalmente com a força bruta ou a computação desligada de senhas ou códigos compartilhados usados para autenticação;

» **Ataques sem fio:** Estas são ferramentas utilizadas para explorar as vulnerabilidades encontradas em protocolos sem fio. 802.11, por exemplo, aircrack, airmon e ferramentas de quebra de senhas wireless. Além disso, esta seção tem ferramentas de vulnerabilidades de RFID e Bluetooth também. Em muitos casos, será necessário uma rede sem fio;

Visão geral ferramentas Kali

» **Ferramentas de Exploração:** são utilizadas para explorar vulnerabilidades encontradas em sistemas. Normalmente, a vulnerabilidade é identificada durante uma vulnerabilidade Avaliação de um alvo;

» **Cheirando e falsificação:** Estas são as ferramentas utilizadas para a captura de pacotes de rede,

manipuladores de pacotes de rede, aplicações de artesanato pacotes e web spoofing. Há também algumas aplicações de reconstrução VoIP;

Visão geral ferramentas Kali

» **Mantendo o acesso:** são usados uma vez um ponto de apoio é estabelecida em uma rede ou sistema alvo. É comum encontrar sistemas comprometidos com vários ganchos de volta para o atacante fornecer rotas alternativas em caso de uma vulnerabilidade que é usado por o atacante é encontrado e corrigido;

Visão geral ferramentas Kali

» **Engenharia reversa:** são usadas para desativar um executável e programas de depuração.

O objetivo da engenharia reversa está analisando como foi desenvolvido um programa para que possa ser copiado, modificado, ou levar a desenvolvimento de outros programas. Engenharia reversa também é usado para análise de malware para determinar o que faz um executável ou por pesquisadores para tentar encontrar vulnerabilidades em aplicações de software;

Visão geral ferramentas Kali

» **Teste de Stress:** utilizados para avaliar a quantidade de dados a sistema pode manipular. Resultados indesejados podem ser obtidos a partir de sobrecarga sistemas como causando um dispositivo de controle de comunicação de rede para abrir todos os canais de comunicação ou de um sistema de desligar (também conhecido como

um ataque de negação de serviço);

» **Hardware Hacking:** Esta seção contém ferramentas de Android, que poderiam ser classificada como ferramentas móveis, e Arduino que são utilizados para a programação e

controlar outros pequenos dispositivos eletrônicos;

Visão geral ferramentas Kali

» **Forense:** Ferramentas forenses são usados para monitorar e analisar o computador tráfego de rede e aplicações;

» **Ferramentas de Relatórios:** são métodos para entregar informações encontradas durante um exercício de Pentest;

» **Serviços do Sistema:** Isto é onde você pode ativar e desativar serviços de Kali.

Os serviços são agrupados por área, Dradis, HTTP, Metasploit, MySQL, e SSH.

O que é ser um Pentester?

» **P**rofissional de segurança responsável por encontrar vulnerabilidades em sistemas, redes e empresas.

Que pode ser categorizado como:

- Júnior (que domina as ferramentas e gera relatórios)
- intermediário (consegue otimizar ferramentas e tem noções de lógica de programação, além do domínio das ferramentas existentes
- Avançado (desenvolve suas próprias ferramentas e amplo domínio das existentes.

Certificação

» Neste área existem órgãos internacionais que garantem a certificação do profissional, basta pagar a prova e atingir a nota mínima exigida.

Um exemplo é a Exin.

https://www.exin.com/BR/pt/exames/

Cursos

» Existem diversos cursos de ethical hacking disponíveis na internet, inclusive em português, mas a maioria é voltado para a categoria júnior.

A Udemy é um site por exemplo que oferece bons cursos na área.

Legislação

» A Lei Carolina Dieckman é como ficou conhecida, a Lei Brasileira 12.737/2012, tipificando os chamados delitos ou crimes informáticos. Os delitos previstos na Lei Carolina Dieckmann são:

1) Art. 154-A - Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Legislação

2) Art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa.

3) Art. 298 - Falsificação de documento particular/cartão - Pena - reclusão, de um a cinco anos, e multa.

4) Art.154-B

Cuidados

Estes Pentest precisão ser documentados e autorizados pelos clientes para evitar penas previstas na lei.