Aprendizado em Kali Linux e Pentest - Gabriel

Introdução

Este documento tem como objetivo registrar minha jornada de aprendizado em cibersegurança, com foco na utilização do Kali Linux, testes de penetração (pentest), e o uso de ferramentas práticas em ambientes controlados.

Ambiente de Testes

- VirtualBox configurado com Kali Linux.
- Configuração de rede NAT e modo Bridge para testes.
- Uso de máquina-alvo (ex: Metasploitable) para simular ambientes vulneráveis.
- Criação de snapshots para restaurar estados após testes.

Ferramentas Utilizadas

- Nmap: varredura e mapeamento de rede.
- Wireshark: análise de pacotes e tráfego de rede.
- Burp Suite: interceptação e análise de requisições HTTP.
- Aircrack-ng: testes em redes Wi-Fi.
- Hydra: testes de força bruta em serviços.
- Nikto e Dirb: análise de diretórios e vulnerabilidades.

Técnicas Estudadas

- Varredura de portas e identificação de serviços.
- Enumeração de diretórios e subdomínios.
- Sniffing de rede e análise de pacotes.
- Exploração de vulnerabilidades conhecidas (CVE).
- Testes de força bruta (SSH, FTP, etc).
- Escalada de privilégios local em sistemas Linux.

Cuidados com Ética e Legalidade

Aprendizado em Kali Linux e Pentest - Gabriel

Todos os testes foram conduzidos em ambientes controlados e simulados. Este aprendizado é voltado para fins educacionais, respeitando os princípios da ética hacker e o uso legal do conhecimento de segurança da informação.

Próximos Passos

- Aprimorar os conhecimentos em scripts de automação com Python para pentest.
- Estudar frameworks como Metasploit e ferramentas mais avançadas (ex: SQLMap, John The Ripper).
- Obter certificações reconhecidas como CompTIA Security+ ou eJPT.
- Participar de CTFs (Capture The Flag) e laboratórios práticos online como Hack The Box e TryHackMe.