**Criando-um-Ataque-Brute-Force-de-senhas-com-Medusa-e-Kali-Linux**

**Descrição do Projeto**

Este projeto implementa e documenta cenários simulados de ataques de força bruta usando Kali Linux como plataforma ofensiva e Metasploitable 2/DVWA como alvos vulneráveis. Utilizei a ferramenta Medusa para testar serviços como FTP, formulários web e SMB, em um ambiente isolado (VMs no VirtualBox com rede host-only).

Este conteúdo é apenas para fins educacionais e de conscientização sobre segurança cibernética. O uso de ferramentas como Medusa para realizar ataques de força bruta contra sistemas sem autorização é ilegal e antiético. Sempre obtenha permissão explícita antes de realizar testes de segurança.

**Reflexões e Aprendizado**

Durante este projeto sobre ataques de força bruta com Medusa no Kali Linux, mergulhei de cabeça no mundo da segurança ofensiva. Aprendi a configurar o ambiente Kali, instalar ferramentas como o Medusa e entender como funcionam os ataques de força bruta e de dicionário. Foi fascinante ver como listas de usuários e senhas podem ser usadas para testar a robustez de sistemas sempre em ambientes controlados e com autorização, é claro.

Usei o Nmap para identificar serviços ativos em máquinas-alvo e depois executei ataques simulados em protocolos como FTP. A cada teste, eu analisava os resultados e compreendia melhor como vulnerabilidades podem ser exploradas e, mais importante, como evitá-las.

Além da parte técnica, o curso reforçou a importância da ética no hacking e entendi que todo teste de invasão precisa de permissão formal. Também aprendi boas práticas de defesa, como autenticação multifator e políticas de senha seguras.

Essa experiência me mostrou que, para proteger sistemas, é essencial pensar como um invasor — mas agir sempre como um profissional ético e responsável.