Relatório Técnico - Simulação Red Team

Autor: Felipe Fragoso | Data: 05/05/2025

Objetivo

Este projeto simula uma cadeia de ataque Red Team completa, com o objetivo de testar a segurança de um ambiente em camadas. Todas as fases são executadas em laboratório controlado e documentadas.

1. Reconhecimento

Coleta de informações com ferramentas como theHarvester, dnsrecon, Nmap, Gobuster e WhatWeb para identificar superfícies de ataque e tecnologias do alvo.

2. Acesso Inicial

Utilização de exploits públicos identificados com o Nmap + Searchsploit. Execução de ataque via Metasploit contra o serviço vsftpd 2.3.4.

3. Execução

Geração de payload com msfvenom e captura de sessão com meterpreter usando o Metasploit multi/handler.

4. Pós-exploração

Extração de credenciais com mimikatz, mapeamento de domínio com BloodHound, e escalonamento de privilégios com winPEAS e técnicas manuais.

5. Persistência

Criação de usuários administrativos, serviços automatizados no Windows e backdoors em scripts de inicialização.

6. Exfiltração

Extração de arquivos sensíveis com curl, netcat e scripts Python via HTTP POST, além de compressão com tar/gzip.

Conclusão

Este projeto demonstrou na prática como funciona uma cadeia ofensiva completa de Red Teaming, desde a

enumeração até a extração de dados, com documentação técnica e organização adequada para portfólio profissional.