

Ataque a La Carte

Essa atividade tem por objetivo desenvolver os conhecimentos sobre ferramentas de teste de intrusão em sistemas computacionais.

Nesta atividade você deverá aplicar um ataque a um sistema operacional (explorando vulnerabilidades de serviços presentes na distribuição ou aplicações instaladas) de sua escolha com o objetivo de ganhar acesso não autorizado ao sistema, por meio de técnicas de acesso remoto, exploração de aplicações web ou escalada de privilégios.

Viste o site <https://www.exploit-db.com/> e faça uma pesquisa sobre exploits disponíveis para o tipo de ameaça de segurança que desejar.

Perceba que na descrição os *exploits* normalmente apresentam o seu identificador CVE (*Common Vulnerabilities and Exposure*) e links para o respectivo site com detalhes sobre a vulnerabilidade bem como as versões vulneráveis do sistema alvo. Por exemplo, o link <https://www.exploit-db.com/exploits/44498/> apresenta um exploit para escalada de privilégios remota no *Apache CouchDB*. Alguns exploits são *stand-alone* enquanto que outros dependem de algumas ferramentas de apoio para sua execução.

Sua Tarefa: Preparar um sistema (máquina alvo e atacante, quando necessário) a ser explorado de acordo com as especificações do *exploit* escolhido e realizar o ataque (teste também possíveis variações do sistema alvo). Você pode montar o sistema em VMs ou através de sistemas emulados, como por exemplo, o Mininet ou Netkit. Ao final você deverá entregar um relatório de experimento contendo a descrição da vulnerabilidade explorada com referencial teórico sobre o funcionamento do mesmo explicando quais as propriedades de segurança violadas no processo de ataque. Além disso, no relatório é preciso detalhar o sistema utilizado, versões de software, pré-configurações utilizadas, descrição das ferramentas de apoio utilizadas (quando houver) e a descrição dos passos seguidos para a realização do ataque.

A estrutura básica do relatório final deve conter as seguintes seções: Capa (Título, Nome dos Alunos), Resumo, Introdução, Descrição dos Experimentos, Resultados e Conclusões.

O trabalho será realizado em **duplas**.

Data de entrega: **27/06/2019**

Formato de Entrega: **Arquivo único .ZIP (Contendo o PDF e os fontes do relatório).**