Engenharia de Segurança
Trabalho 2 – *Pentest*

Grupo: 4 *pessoas*

Objetivo: Estudar, Analisar e Implementar um ***exploit*** via **metasploit**.

Um *exploit* é uma pequeno software ou sequência de dados/instruções que tiram vantagem de um *bug*, falha ou vulnerabilidade na programação de um sistema alvo com a intenção de causar um comportamento não previsto, geralmente implicando na escalação de privilégios (usuário comum obtendo poderes administrativos), negação de serviço ou obtenção de acesso e controle.

Para a utilização do *exploit*, vocês devem utilizar a ferramenta ***metasploit*****,** um sistema que através de *plugins* e *paylods* é capaz de acionar diversos *exploits*. A ferramenta *metasploit* pode ser instalada em qualquer distribuição de Linux, mas por seu processo de instalação ser custoso, o ideal é utilizar uma distribuição especializada em teste de penetração que já tem o *metasploit framework* pré-instalado. As principais distribuições são:

- Kali Linux
- Back track 5.3
- Blackbuntu

Importante*: Preste atenção nas versões dos softwares utilizados como vítima, cujos payloads foram desenvolvidos. Softwares atualizados possivelmente corrigem as falhas exploradas.*

Apresentar:
O grupo deverá apresentar o ataque escolhido em um ambiente controlado (virtualizado)

Entrega
O grupo deverá entregar um arquivo compactado, via *moodle*, contendo:
- Relatório conforme descrito no item **relatório** a seguir
- ***Plugin*****/*****payloads*** utilizados
- Código fonte desenvolvido (se aplicável)

Relatório
O relatório, entregue em **pdf**, deve conter:
- Explicação do padrão de ataque utilizado, incluindo conforme aplicável, análise dos pacotes modificados, análise da vulnerabilidade explorada.
- Roteiro de implementação do ataque

- Estratégias complementares de defesas que poderiam interferir no sucesso do ataque.
- Descrição de ferramentas complementares, caso tenham sido utilizadas.

Critério de avaliação

1. Imaginação
2. Criatividade
3. Complexidade
4. Eficácia da defesa proposta
5. Qualidade do relatório