Tecnologias de Segurança

Ano Letivo 2024/2025

Trabalho Prático 1

Implementar e Mitigar um tipo de Ataque | Desenvolver um Algoritmo de Encriptação e Desencriptação robusto

1. Introdução

O objetivo deste trabalho prático passa por entender de que forma um ataque informático coordenado é implementado, explorado e concluído. Pretende-se que os alunos (em grupo de 2 alunos) optem pelas duas opções disponíveis para o trabalho prático nº 1. A opção A, passa por recriar um tipo de ataque já existente e documentar o seu comportamento e a forma de mitigação. Na opção B, o grupo irá desenvolver o seu próprio mecanismo de encriptação e desencriptação com base num algoritmo proposto pelo grupo.

A. Objetivos (Ataque e Mitigação)

Depois de terminar este trabalho prático deve ser capaz de:

- Entender o conceito de ataque;
- Entender o conceito de vulnerabilidades;
- Entender o conceito de mitigação;
- Aplicar corretamente tecnologias de segurança;
- Identificar a origem de ataques;
- Instalar e configurar corretamente as ações necessárias para mitigar um ataque;

B. Objetivos (Algoritmo de Encriptação / Desencriptação)

Depois de terminar este trabalho prático deve ser capaz de:

- Entender o conceito de encriptação;
- Entender o conceito de desencriptação;
- Testar a robustez de algoritmos de encriptação;
- Analisar o fator de confiança do seu algoritmo;
- Verificar e analisar tempos de obtenção da mensagem original através de aplicativos existentes.

Tecnologias de Segurança

Ano Letivo 2024/2025

Trabalho Prático 1

Implementar e Mitigar um tipo de Ataque | Desenvolver um Algoritmo de Encriptação e Desencriptação robusto

2. Regras importantes

Devido às consequências que advém da opção A, é requerido aos alunos que efetuem a implementação do trabalho em ambiente isolado, isto é, sem que este coloque em causa qualquer funcionalidade da rede externa onde estão inseridos e que não viole qualquer lei em vigor.

3. Execução do trabalho

O trabalho deverá ser executado em grupos de 2 alunos (se o número de alunos for impar, poderá ser possível fazer um grupo de 3 alunos ou um aluno efetuar o trabalho sozinho), sendo depois apresentado na data da defesa do trabalho prático 1. Para a defesa devem demonstrar todos os procedimentos que utilizaram para efetuarem o trabalho prático, sendo que:

Caso o trabalho prático seja a opção A: devem apresentar para além da documentação produzida, um vídeo onde irão demonstrar o ataque, as vulnerabilidades e a sua mitigação.

Caso o trabalho prático seja a opção B: Devem apresentar em real time, a encriptação de uma mensagem, o envio da mesma pela rede, a captura da mensagem encriptada, a tentativa de obtenção de forma ilícita da mensagem original e, por fim o desencriptar da mensagem.

A data de defesa do trabalho prático 1 será na aula de dia 8 de Novembro de 2024.

Exemplos de Ataques a explorar:

Tecnologias de Segurança

Ano Letivo 2024/2025

Trabalho Prático 1

Implementar e Mitigar um tipo de Ataque | Desenvolver um Algoritmo de Encriptação e Desencriptação robusto

- ARP Cache Poisoning
- SYN Flooding Attack
- TCP RST Telnet & SSH
- Rip Spoofing
- DNS SPOOFING
- TCP Session Hijacking
- ICMP Redirect Attack
- SQL Injection

Bom trabalho!