Planejar e executar a manutenção de redes locais de computadores

Aula 23 - Ameaças Comuns

Exercícios

ALUNO: VICTOR BARROS ROMA

TURMA: TI 109

Questão 1

**Classifique as ameaças a seguir como internas ou externas:**

Um funcionário conectou, sem saber, um USB infectado ao laptop de trabalho.

Um funcionário inseriu informações erradas no banco de dados da empresa.

Um funcionário clicou em um link de e-mail suspeito.

Um ex-funcionário conseguiu baixar arquivos de clientes acessando remotamente a rede da empresa.

**Resposta:** Interna: 1 e 2 Externo 3 e 4

Questão 2

**Defina, com as suas palavras, o que é ataque backdoor, ataque rootkit, ataque de algoritmo e ameaças persistentes avançadas.**

**Resposta:**

**Backdoor - o hacker utiliza de ferramentas para entrar nos sistemas ignorando qualquer tipo de altenticação do alvo para ter controle administrativo e poder ter acesso a informação**

**Rootkit - é um programa que se aproveita de vunerabilidades de algum programa para dar acesso ao sistema sem necessitar de credenciais**

Questão 3

**Cenário**: Você é o administrador de uma rede local em uma pequena empresa. A rede possui vários dispositivos, incluindo computadores, impressoras e roteadores.

* Liste cinco possíveis ameaças à segurança dessa rede local. Considere ameaças internas (de dentro da organização) e externas (de fora da organização).
* Para cada ameaça, explique brevemente como ela pode afetar a rede e quais medidas de segurança podem ser implementadas para mitigá-la.

Questão 4

**Cenário**: Você está investigando um servidor web que apresentou comportamento suspeito. Você suspeita que ele possa estar comprometido por um backdoor ou rootkit.

* Descreva o que são backdoors e rootkits em termos de segurança cibernética.
* Explique como um backdoor pode ser introduzido em um sistema e como ele pode ser usado por um atacante.
* Discuta as principais diferenças entre backdoors e rootkits.
* Sugira métodos para detectar e remover backdoors e rootkits de um sistema comprometido.