**Centro Paula Souza**

**ETEC Professor Camargo Aranha**

Leonardo

**Desenvolvimento de sistemas**

**São Paulo**

**2025**

Sumário

[Trabalho Prático: Segurança de Sistemas de Informação 3](#_Toc191405290)

[Golpes na Internet 3](#_Toc191405291)

[1. Phishing 3](#_Toc191405292)

[2. Golpe de E-commerce Fraudulento 3](#_Toc191405293)

[3. Golpe de Leilão Online 3](#_Toc191405294)

[Ataques na Internet 3](#_Toc191405295)

[1. Ataque WannaCry (2017) 3](#_Toc191405296)

[2. Ataque DDoS ao GitHub (2018) 3](#_Toc191405297)

[3. Ataque de Falsificação de E-mail (Spoofing) 4](#_Toc191405298)

[Códigos Maliciosos (Malware) 4](#_Toc191405299)

[1. Vírus 4](#_Toc191405300)

[2. Worm 4](#_Toc191405301)

[3. Cavalo de Troia (Trojan) 4](#_Toc191405302)

[Ferramentas para Exploração de Vulnerabilidades 4](#_Toc191405303)

[1. Nmap 4](#_Toc191405304)

[2. Metasploit 4](#_Toc191405305)

[Conclusão 5](#_Toc191405306)

[Referências 6](#_Toc191405307)

# Trabalho Prático: Segurança de Sistemas de Informação

## Golpes na Internet

### 1. Phishing

**Exemplo**: Em 2019, um banco brasileiro sofreu um ataque de phishing, onde criminosos enviaram e-mails falsos para clientes, coletando dados bancários. O prejuízo estimado foi de R$ 10 milhões.

### 2. Golpe de E-commerce Fraudulento

**Exemplo**: Em 2021, um site de e-commerce falso foi criado para enganar consumidores. Após comprarem produtos a preços baixos, as vítimas nunca receberam o que compraram. O prejuízo foi de R$ 5 milhões.

### 3. Golpe de Leilão Online

**Exemplo**: Em 2020, um site de leilão falso enganou consumidores que acreditavam estar comprando produtos com grandes descontos. O prejuízo total foi de R$ 3 milhões.

## Ataques na Internet

### 1. Ataque WannaCry (2017)

**Descrição**: O WannaCry foi um ransomware que afetou mais de 200.000 computadores no mundo todo, incluindo hospitais e empresas. Os dados foram criptografados e os atacantes exigiram pagamento em Bitcoin. O prejuízo global foi de bilhões de dólares.

### 2. Ataque DDoS ao GitHub (2018)

**Descrição**: O GitHub sofreu um ataque DDoS (negação de serviço distribuído) que sobrecarregou seus servidores. O ataque durou apenas 10 minutos, mas causou grande impacto.

### 3. Ataque de Falsificação de E-mail (Spoofing)

**Exemplo**: Em 2019, uma empresa de telecomunicações foi vítima de spoofing, onde criminosos enviaram e-mails falsificados solicitando transferências bancárias. O prejuízo foi de R$ 2 milhões.

## Códigos Maliciosos (Malware)

### 1. Vírus

**Descrição**: O vírus "ILOVEYOU" se espalhou por e-mails em 2000, infectando milhões de computadores. Ele causou danos significativos, sendo um dos vírus mais conhecidos.

### 2. Worm

**Exemplo**: O worm "Conficker" se espalhou em 2008, explorando falhas no Windows. Ele infectou milhões de computadores ao redor do mundo.

### 3. Cavalo de Troia (Trojan)

**Exemplo**: O Trojan "Zeus" foi usado para roubar dados bancários de empresas, afetando várias organizações ao redor do mundo.

## Ferramentas para Exploração de Vulnerabilidades

### 1. Nmap

**Descrição**: O Nmap é uma ferramenta usada para fazer varredura em redes, ajudando a identificar vulnerabilidades e portas abertas em sistemas.

### 2. Metasploit

**Descrição**: O Metasploit é uma plataforma usada para testar e explorar vulnerabilidades em sistemas, ajudando a encontrar falhas de segurança.

## Conclusão

Este trabalho apresentou exemplos reais de golpes na internet, ataques cibernéticos e malwares, além de ferramentas utilizadas para explorar vulnerabilidades. A segurança de sistemas é essencial para proteger dados e evitar prejuízos, e o uso de boas práticas e tecnologias é crucial para minimizar riscos.

## Referências

* CERT.BR - Cartilha de Segurança para Internet.
* Tecnologia Info, "Golpe de E-commerce Fraudulento", 2021.
* Wired, "GitHub DDoS Attack", 2018.
* Kaspersky, "Vírus ILOVEYOU", 2000.
* Symantec, "Worm Conficker", 2008.
* McAfee, "Trojan Zeus", 2015.
* Nmap, [www.nmap.org](https://nmap.org).
* Metasploit, [www.metasploit.com](https://www.metasploit.com).