Proteção de dados em segurança de redes de computadores

Conceitos e Aplicações

Prof. Ronierison Maciel (Roni)

22/11/2023

O que veremos hoje?

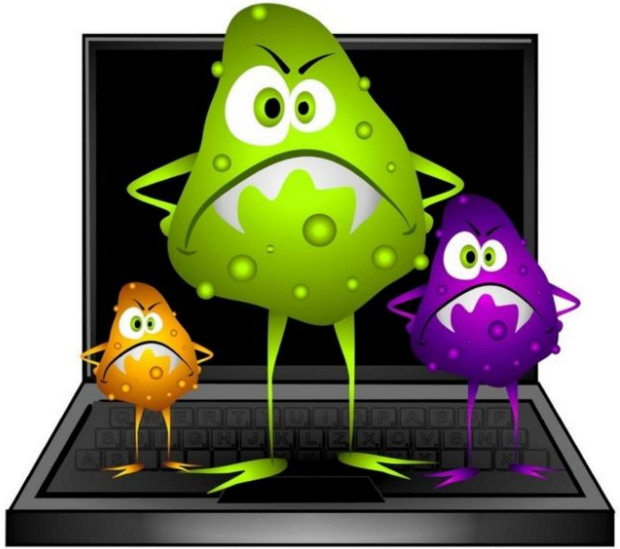
1. Conceitos introdutórios sobre segurança de redes
2. Discussão em grupo sobre notícias recentes de violações de segurança
3. Quizz

Introdução

- Dúvidas 🤔
  - Qual a quantidade de informações produzida a cada dia - 2,5 quintilhões
  - O sistema da minha empresa é seguro?
  - Será que isso acontecerá na minha empresa?
  - Como minimizar os riscos?

Introdução

➔ E quanto às suas informações, você se preocupa com a sua segurança?

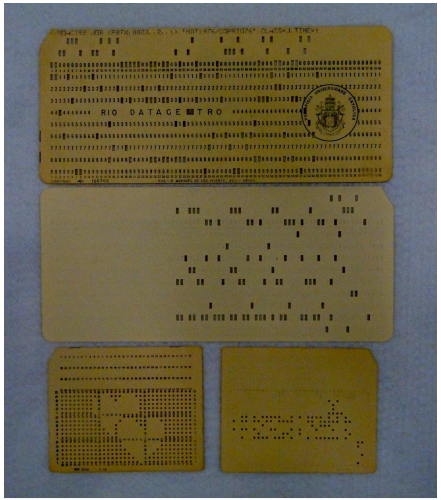


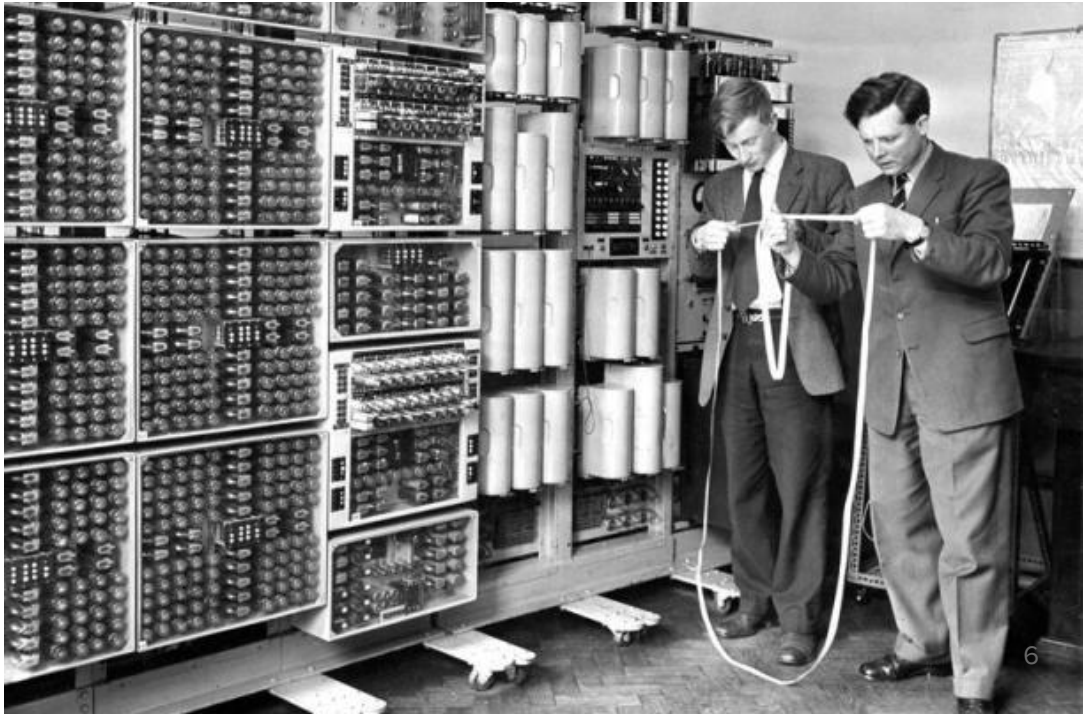
Introdução

➔ O que torna um sistema seguro? 🧐

Introdução

➔ Antigamente





Introdução

➔ Atualmente

Introdução

➔ Ameaças

Introdução

- Informação
  - “O bem mais valioso”

Objetivos do Curso e Metodologia

➔ **Ponto 1:**

- Compreender os conceitos fundamentais da segurança de redes.

Ponto 1

➔ **Fatores secundários:**

- Intempéries da natureza;
- Greves;
- Manifestações.

Objetivos do Curso e Metodologia

➔ **Ponto 2:**

- Reconhecer a importância da segurança física e lógica.

Ponto 2

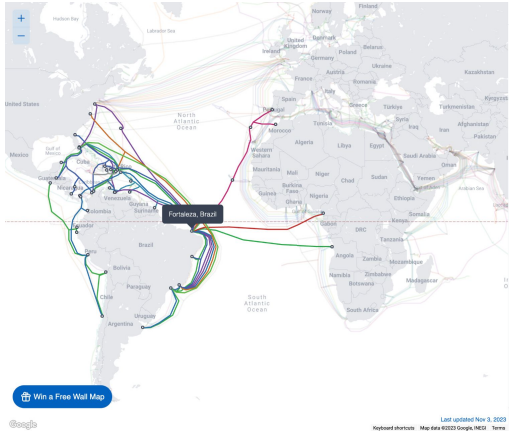
➔ Ameaças

- Um agente externo que oferece perigo.

Objetivos do Curso e Metodologia

➔ **Ponto 3:**

- Casos reais e recentes de violações de segurança 🔥
- Cable Map
- 3D Map



Ponto 3

➔ Vulnerabilidades

- É uma fraqueza que permite que um atacante reduza a garantia da informação de um sistema.

Ponto 3+

- **Vulnerabilidades**
  - Físicas;
  - Naturais;
  - Hardware;
  - Software;
  - Mídias;
  - Comunicação;
  - Humanas.

Fluxograma da vulnerabilidade

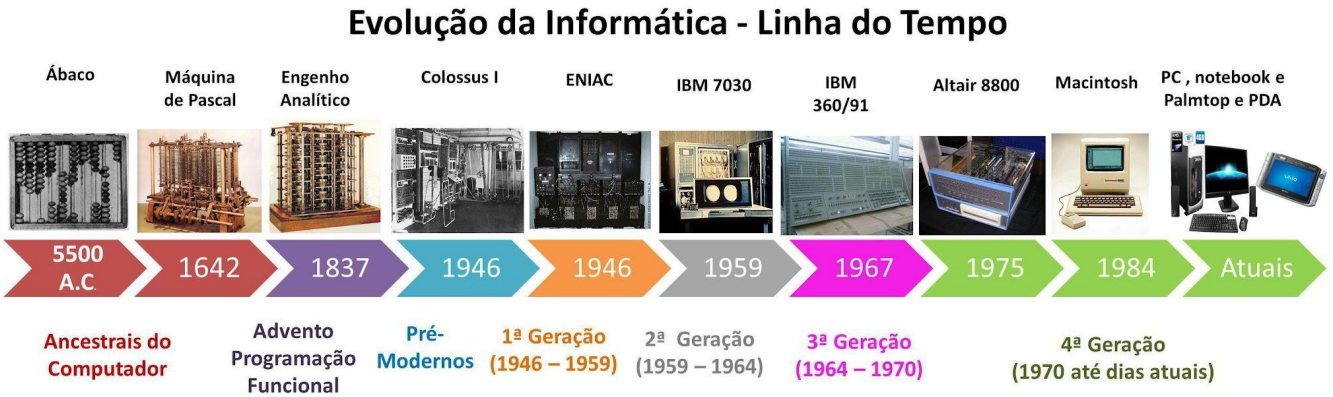
Objetivos do Curso e Metodologia

- Quizz
  - Quizizz.com

Uma Viagem no Tempo

➔ A evolução da segurança Digital

- Início dos anos **1970**: Primeiros vírus em mainframes.
- Anos **1980**: Surgimento dos primeiros antivírus.
- Anos **1990**: A era da Internet e novos desafios de segurança.
- Anos **2000**: Ataques cibernéticos de larga escala e o início da guerra cibernética.
- Anos **2010**: Aumento de ataques sofisticados e o papel da IA na segurança.



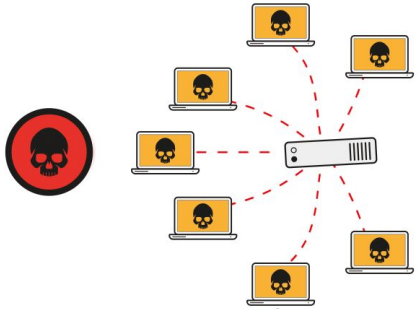
O Mundo Digital Hoje: Números que Falam

- Custo das Violências:
  - Custo médio de uma violação de dados: US$ 4,35 milhões (2022).
  - Custo médio de um ataque de ransomware: US$ 4,54 milhões.
  - Custo médio de recuperação de ransomware: quase US$ 2 milhões.
  - Nos **EUA**, o custo médio de violação de dados é de US$ 9,44 milhões.
  - O custo médio de uma violação de dados no **Brasil** foi de R$ 7,71 milhões [1].
- Frequência e Duração:
  - Empresas levaram em média 277 dias para identificar e conter uma violação (2022).
  - A cada minuto, US$ 17.700 são perdidos devido a ataques de phishing.
  - Em média, um ataque cibernético ocorre a cada três segundos.
  - No Brasil, as empresas levaram em média 347 dias para identificar e conter uma violação de dados em 2022, o que representa uma redução de 49 dias em relação ao ano anterior.[2]

Introdução aos Tipos de Ataques

- **Ataques de negação de serviço (DoS/DDoS):**
  - Esses ataques visam impedir que um sistema ou rede funcione. Eles são geralmente realizados enviando um grande número de solicitações a um servidor, o que pode sobrecarregá-lo e torná-lo inacessível.
- **Phishing:**
  - Esses ataques visam enganar as pessoas para que divulguem informações confidenciais, como senhas ou números de cartão de crédito. Eles geralmente são realizados por meio de e-mails ou mensagens de texto que parecem ser legítimos.
- **Ransomware:**
  - Esses ataques criptografam os dados da vítima e exigem um resgate para descriptografá-los. Eles geralmente são distribuídos por meio de anexos de e-mail ou downloads infectados.

Ataque DDoS/DoS

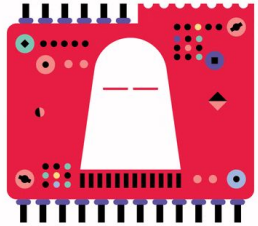


- **Inundação de Rede:**
  - Onde o atacante sobrecarrega a capacidade de rede do alvo com um alto volume de tráfego.
- **Exploitation de Vulnerabilidades de Software:**
  - Atacando as fraquezas específicas de um software para causar falhas ou sobrecarga.
- **Ataques ao Nível de Aplicação:**
  - Especificamente direcionados para aplicativos web, enviando um número excessivo de pedidos que parecem legítimos mas têm como objetivo drenar os recursos do servidor.
- **Casos reais:**
  - O ataque de 2000 contra o site da Amazon, que deixou o site inacessível por várias horas.
  - O ataque de 2016 contra o site da Sony Pictures, que deixou o site inacessível por vários dias.
  - O ataque de 2020 contra o site do governo dos Estados Unidos, que deixou o site inacessível por várias horas.

Ataque Phishing

- **E-mails de Phishing:**
  - Imagine um personagem recebendo um e-mail que parece ser de seu banco, pedindo que atualize suas informações de segurança. O e-mail contém um link que leva a um site falso, indistinguível do real, onde as informações inseridas são roubadas pelo atacante.
- **Spear Phishing:**
  - Mais direcionado, como um caçador que mira em uma presa específica. Aqui, o atacante conhece informações sobre a vítima e personaliza o ataque para torná-lo mais convincente. Por exemplo, um e-mail que parece vir de um colega de trabalho com um pedido para verificar um documento.
- **Phishing via SMS (Smishing):**
  - Mensagens de texto fraudulentas que levam as vítimas a sites maliciosos ou as induzem a divulgar informações pessoais. Pode ser representado como uma mensagem urgente pedindo ação imediata.
- **Phishing por Voz (Vishing):**
  - Envolve telefonemas, onde o atacante se faz passar por uma autoridade ou empresa confiável para extrair informações pessoais. Imagine uma cena em que um personagem recebe uma ligação de seu "banco" informando sobre uma atividade suspeita em sua conta.

Ataque Ransomware



Ransomware é um tipo de malware (software malicioso) que criptografa os arquivos do computador da vítima, tornando-os inacessíveis. O atacante então exige um pagamento (geralmente em criptomoeda, para manter o anonimato) para fornecer a chave que pode descriptografar os arquivos. É como um sequestro digital, onde os dados são os reféns.

- **Infecção:**
  - O ransomware geralmente se infiltra em um sistema através de e-mails de phishing, downloads maliciosos ou exploração de vulnerabilidades de segurança. Pode-se imaginar isso como um invasor sorrateiro que encontra uma janela destrancada para entrar em uma casa.
- **Criptografia:**
  - Uma vez dentro do sistema, o ransomware criptografa arquivos importantes. Esta etapa é como colocar cadeados em objetos de valor, onde apenas o ladrão tem a chave.
- **Exigência de Resgate:**
  - O atacante então exibe uma mensagem exigindo pagamento para desbloquear os arquivos. É como um sequestrador enviando uma nota de resgate, com instruções específicas e um prazo.

Casos Notórios

- **WannaCry (2017):**
  - Um dos ataques de ransomware mais famosos, afetou centenas de milhares de computadores em mais de 150 países. Explorou uma vulnerabilidade no Windows, afetando principalmente hospitais, empresas e instituições governamentais.
- **NotPetya (2017):**
  - Originalmente direcionado à Ucrânia, espalhou-se globalmente, causando bilhões de dólares em danos. Foi mais destrutivo que lucrativo, pois muitas vezes os dados não podiam ser recuperados mesmo após o pagamento.
- **Colonial Pipeline (2021):**
  - Um dos maiores ataques de ransomware nos EUA, afetou o fornecimento de combustível na Costa Leste. A empresa pagou um resgate significativo em Bitcoin, destacando a vulnerabilidade da infraestrutura crítica.

Data Center Locaweb

Data Center Google

Segurança Data Center da Google

Bem-vindos à Semana 2 do nosso curso!

Esta **semana**, mergulharemos profundamente no mundo dos ataques cibernéticos, explorando em **detalhes** as diversas formas que esses **ataques** podem assumir. Nossa jornada nos levará a **compreender** não apenas o que esses **ataques** são, mas também como eles **funcionam**, como **identificá-los** e, o mais importante, como nos proteger contra eles.

Objetivos da Semana

- **Entender e Diferenciar Tipos de Ataques:**
  - Vamos explorar os detalhes de ataques como Backdoor, DoS, DDoS, DMA, Eavesdropping e Spoofing. Essa compreensão é fundamental para qualquer profissional de segurança de redes.
- **Análise de Casos Reais:**
  - Através da análise de estudos de caso reais, entenderemos o impacto desses ataques no mundo real, agregando uma camada prática ao nosso conhecimento teórico.
- **Desenvolvimento de Habilidades Práticas:**
  - Com exercícios e laboratórios práticos, você terá a oportunidade de aplicar o conhecimento adquirido em situações simuladas, fortalecendo suas habilidades de identificação e mitigação de ataques.

Tópicos a serem Abordados

- **Backdoor:**
  - Exploraremos o que são Backdoors, como eles são implantados e como podem ser detectados e prevenidos.
- **DoS e DDoS:**
  - Entenderemos a diferença entre ataques DoS e DDoS, seus impactos e estratégias de defesa.
- **DMA Attack:**
  - Discutiremos ataques via Direct Memory Access e como se proteger contra eles.
- **Eavesdropping:**
  - Analisaremos técnicas de escuta indesejada e como garantir a confidencialidade dos dados.
- **Spoofing:**
  - Estudaremos diferentes tipos de Spoofing e como identificar e proteger redes contra essas ameaças.

NMAP

- Principais comandos com NMAP:
  - nmap -p- [endereço IP ou nome do host]
    - Realiza uma varredura padrão nas 1.000 portas TCP mais comuns.
  - nmap -sV [endereço IP]
    - Detecta versões de serviços em execução nas portas abertas.
  - nmap -O [endereço IP]
    - Tenta identificar o sistema operacional do alvo.
  - nmap -T4 -A [endereço IP]
    - Realiza uma varredura agressiva (mais rápida e com detecção de versões de serviços, sistema operacional, traceroute, e scripts padrão).
  - nmap -sU [endereço IP]
    - Escaneia portas UDP (útil para encontrar serviços que não estão escutando em portas TCP padrão).

Recursos

- Ferramentas:
  - Slowloris
  - LOIC
  - Wireshark
  - Collection tools
- Ambientes
  - Hack The Box
  - TryHackMe
  - VulnHub