Segurança Cibernética

Princípios de Segurança Cibernética I

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

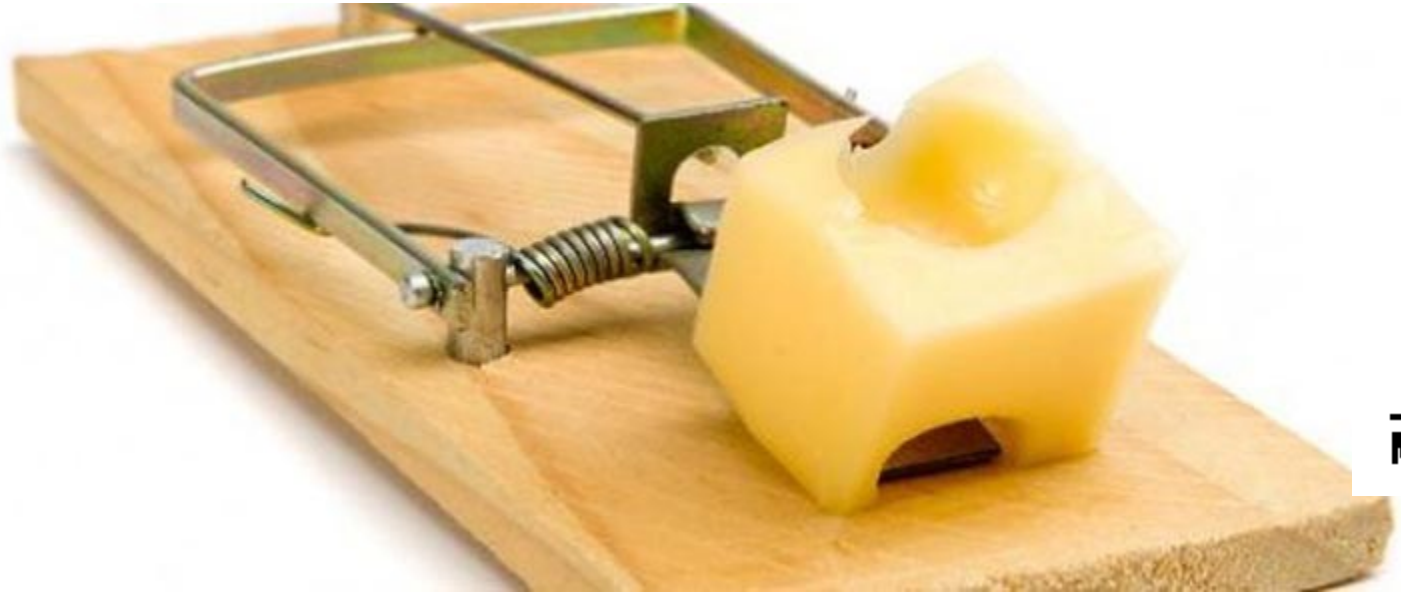
- **Situação:** Quando se pensa em segurança da informação, se pensa em vultosos investimentos em equipamentos e tecnologia.

Mentimeter

Do que estamos protegendo a informação?

Compreendendo o problema

- **Situação:** As ameaças estão por todos os lados, prontas para explorar as vulnerabilidades de nossos sistemas.



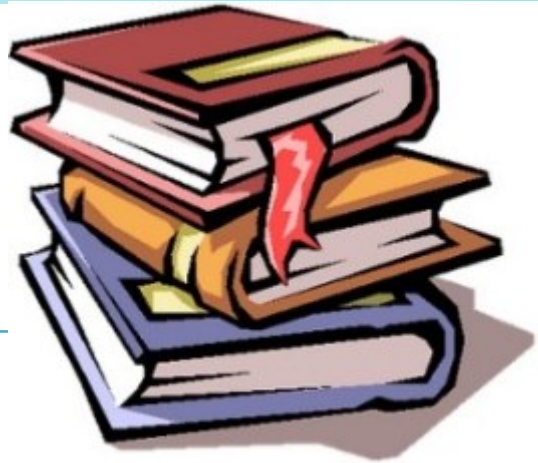
Mentimeter

Qual é o primeiro passo para evitar uma armadilha?

Objetivos

- Conhecer as informações que precisamos proteger
- Tomar contato com o nosso contexto de atuação
- Conhecer alguns dos mecanismos de proteção da informação

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2022a/ara0076.php (Segurança Cibernética – Aula 02)
Minha Biblioteca	• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 11 a 101. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 10 a 19; • Redes de computadores: uma abordagem top-down (978-85-8055-169-3), págs 34 a 42.
Material Adicional	1) 5 ferramentas de segurança para proteger sua rede! - Dispoinível em: https://youtu.be/CInn1mpc67M

Antes de Mais nada...

- **Consulte o material da 1ª Aula!**
- **Otimize seus estudos**
  - Se preparar para conteúdo da semana seguinte!
- **Atividades e Desafios Semanais**
  - No site e mural da disciplina: https://www.caetano.eng.br/aulas/2022a/ara0076.php
- **Será controlada a presença**
  - Chamada ocorrerá sempre nos 15 minutos finais
- **Contato**

Professor	E-mail
Daniel Caetano	prof@caetano.eng.br

Visão Geral:

O que, de quê e como proteger?

O que envolve a segurança?

- Elementos
  - Hardware, software, dado, instalações/rede
- Terminologia
  - Ameaça, vulnerabilidade, ataque/incidente
  - Risco, impacto/desastre
  - Contramedidas, política e plano de segurança

Ambiente a ser protegido

- Equipamentos de Operações x Datacenter
- Equipamentos Básicos
  - Infraestrutura de rede
    - Roteadores: encaminham dados entre múltiplas redes
    - Switches: distribuem dados dentro de uma rede
    - Access points: comunicação de dados sem fio
    - Cabeamento: transportam dados por meio físico.
  - Armazenamen
    - *Storages*
  - Processamento
    - Servidores.

O que precisa ser protegido?

- Dados gerais que são parte da operação
- Dados estratégicos
- Dados associados às leis gerais
  - Lei Geral de Proteção de Dados
  - Marco Civil da Internet...
  - Dados de terceiros (*copyright* etc.,

- Dados associados às leis específicas
  - Tributária, sanitária...
- Foco: evitar exposição e perda de dados
  - Adicional: evitar uso abusivo dos dados

Qual o foco dos ataques/invasões?

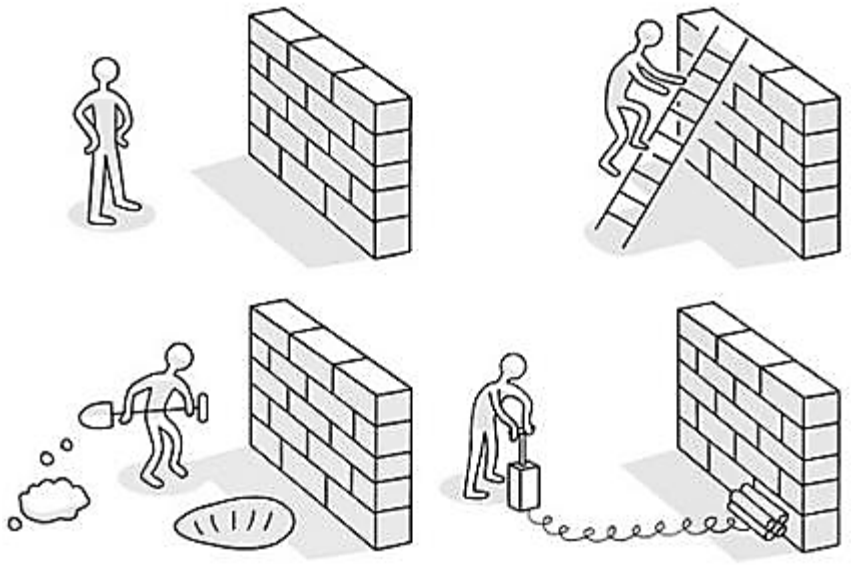
- Dados
  - Roubar, sequestrar, destruir...
- Só dados?
  - Não!
- Uso de poder computacional e banda de rede
  - Ataques a outros computadores
  - *Botnets* para usos ilegais
  - Processar criptomoedas...

Situações indesejáveis

- Revelação não autorizada
  - Quebra de confidencialidade
  - Exposição, interceptação, inferência, intrusão;
- Fraude
  - Quebra de integridade de dados ou sistema
  - Personificação, falsificação, retratação/repúdio;
- Disrupção
  - Quebra da disponibilidade ou integridade (D/S)
  - Incapacitação, corrupção, obstrução;
- Usurpação
  - Quebra da integridade do sistema
  - Apropriação indevida, utilização indevida.

Quem faz a proteção?

- Equipe de segurança
  - Interna: funcionários experientes contratados
  - Hackers éticos: identificar vulnerabilidades
    - Descobrir problemas antes que um antiético o faça!
  - Em todo o caso, devem considerar:
    - As leis
    - As regras da empresa



Como nos defender?

- Equipamentos de Proteção
  - **Antivírus**: Combate a instalação e execução de *malwares*
  - **Firewall** e **Gateway**: Combate o acesso de invasores e ataques baseados em acesso
  - **IDS/IPS**: Detecção e prevenção de ataques com base na atividade da rede
  - **Load Balancer**: Distribui a carga entre servidores espelhados
  - **Proxy Web** (WebFilter): Combate a infecção por meio de acesso a sites não confiáveis
  - **Voucher**: Combate o uso da rede wifi sem identificação
  - **VPN** (Virtual Private Network): Combate o roubo de dados que trafegam pela rede pública
    - Tunelamento usando IPSec ou SSL (TLS, na verdade)

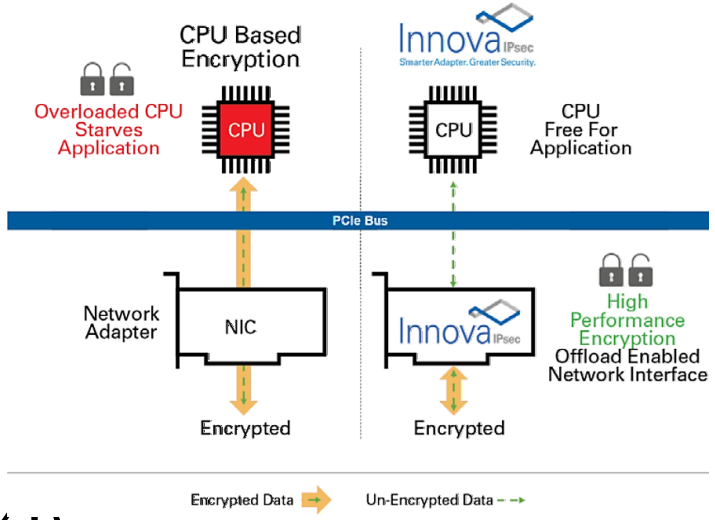
Como nos defender?

- Capacidade dos equipamentos
  - Tem a ver com segurança?
    - Evitar Indisponibilidade!

- Cuidados na aquisição!
  - Especificações de Compra
    - RFCs/Benchmarks...
      - Cuidado com os datasheets!
      - NSS Labs (faz testes mais padronizados).

Capacidade dos equipamentos

- Dados necessários
  - # de usuários simultâneos
  - # de pacotes por segundo
  - *Throughput* da rede
  - # de transações SSL (...>70%!)
  - Perfil de pacotes (IMIX) – 64 bytes a 9000...
  - Considerar o crescimento da empresa
- Conheça seus equipamentos!
- IPSec e SSL impõem peso enorme
  - Capacidade de *throughput* pode cair muito!



Visão Geral:

Noções sobre Ataque Cibernéticos

Caminhos para um ataque

- Ataques são planejados
- Inicio dos ataques planejados?
  - "Reconhecimento do terreno"
  - Coleta de dados

- Como fazer isso?
  - Técnicas de reconhecimento
    - Localização e dados, versão de software, rede...
  - Uso de software/hardware específico
    - Farejadores, por exemplo

Reconhecimento

- Pode se enquadrar em 3 tipos
  - Legal: buscar na internet, ligar para questionar...
  - Questionável: escâner passivo de portas, olhar lixo, war diving (de redes wifi abertas)...
  - Ilegal: empresas de fachada, roubar lixo, keylogger, farejadores não autorizados...
- Categorias comuns:
  - Engenharia Social
  - Mergulho no Lixo
  - Rastreio de Pegadas.

Engenharia Social

- Pessoas são predispostas a serem úteis
  - Ou são motivadas a colaborar
- Pode envolver intrusão física
  - Ou remoto: Carta, telefone, e-mail, SMS...
- Técnicas comuns:
  - Personificação (individual / funcional)
  - Suborno
  - Fraude
  - Afinidade
  - Engenharia Social Reversa.

Engenharia Social

- Como combater?
  - Orientar usuários a agirem com cautela
- Orientações?
  - Não oferecer informações a desconhecidos
    - Direta ou indiretamente
  - Não submeter informações a sites inseguros
  - Não usar sempre o mesmo usuário e senha
  - Bloquear computador quando estiver longe

Voltaremos a isso!

Mergulho no Lixo

- O que é?
  - Literalmente: vasculhar lixo (físico ou eletrônico)
- Prevenção: descarte adequado
  - Físico: picotar, reciclar
  - Digital: apagar, destruir.

Rastreio de Pegadas

- O que é?
  - Seguir os “rastros” das pe
- O que envolve?
  - Redes sociais
  - Buscas na web
    - WayBack Machine

Rastreio de Pegadas

- O que é?
  - Seguir os “rastros” das pe
- O que envolve?
  - Redes sociais
  - Buscas na web
    - WayBack Machine
    - Cache do Google

Rastreio de Pegadas

- O que é?
  - Seguir os “rastros” das pe
- O que envolve?
  - Redes sociais
  - Buscas na web
    - WayBack Machine
    - Cache do Google
  - Reconhecimento com base em DNS/rede
    - Consultas, whois etc.

Rastreio de Pegadas

- O que é?
  - Seguir os “rastros” das pe
- O que envolve?
  - Redes sociais
  - Buscas na web
    - WayBack Machine
    - Cache do Google
  - Reconhecimento com base em DNS/rede
    - Consultas, whois etc.
- Prevenção
  - Cuidado com o que postar/publicar

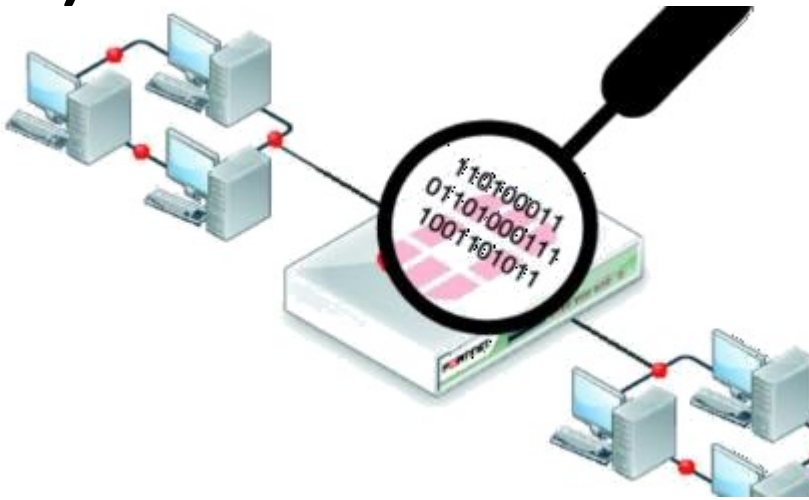
Farejadores (*Sniffers*)

- Monitoram, capturam e filtram dados na rede
  - Uso lícito: identificar anomalias no tráfego de rede
  - Uso ilícito: analisar dados sem a autorização
- Tipos:
  - Embutidos (no sistema)
    - Network Monitor, tcpdump

Farejadores (*Sniffers*)

- Monitoram, capturam e filtram dados na rede
  - Uso lícito: identificar anomalias no tráfego de rede
  - Uso ilícito: analisar dados sem a autorização
- Tipos:
  - Embutidos (no sistema)
    - Network Monitor, tcpdump
  - Comerciais
    - SolarWinds, Paessler PRTG Network Monitor
  - Livres
    - Wireshark, WinDump.

Farejadores (Sniffers)



- Por que funcionam?
  - Broadcast de pacotes
  - Placa de rede em modo prc
- Local ideal de instalação: g
- Como se proteger
  - Detectores... apenas verificam condições
    - Antisniff/Neped.c: rede em modo promísculo
    - SniffDet: # de consultas ao dns, ping com MAC falso etc.
  - Criptografia
    - SSL/TLS
    - PGP ou similares
    - SSH

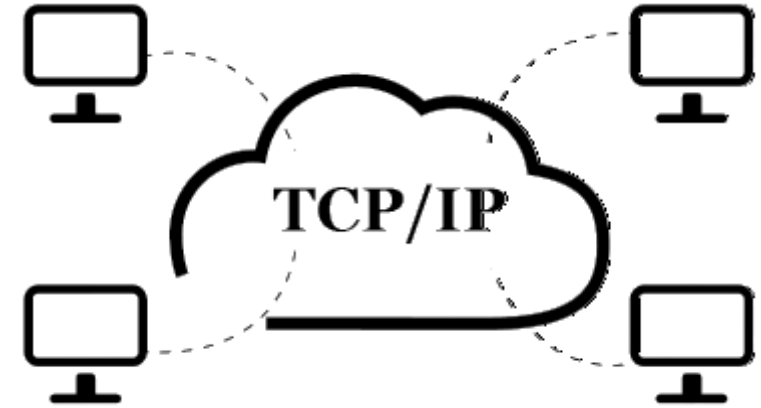
Voltaremos a isso!

Visão Geral:

Vulnerabilidades do Protocolo TCP/IP

O Protocolo TCP/IP

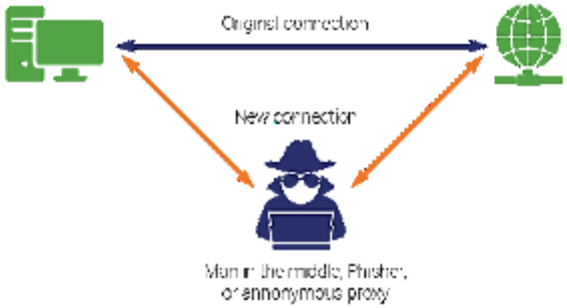
- É o protocolo de comunicação da internet
- Criado com propósitos militares
  - Impedir a interrupção da comunicação
  - Inicialmente: sem previsão de criptografia.



Voltaremos a isso!

Vulnerabilidades x Soluções

- Manter o TCP/IP atualizado
- Não há criptografia/autenticação por padrão
  - Usar criptografia (autenticação, sessões, tráfego...)
- Falsificação de IP
  - Envolve mudanças na pilha TCP/IP: pouco prático
- Sequestro de conexão
  - Uso de VPN, criptografia de ponta a ponta...



Vulnerabilidades x Soluções

- Ataque (DoS – ICMP ou SYN)
  - Usar IDS/IPS
  - Reduzir o timeout ao estabelecer conexão
  - Aumentar o máximo de conexões simultâneas
  - Limitar as conexões por um mesmo IP.
- Ataque RIP
  - Implementar firewall.

ATIVIDADE

Atividade

- Discussão – Grupos – 20 a 25 minutos

1. Escolha uma empresa de porte médio que atua online. Discuta com seu grupo quais são os principais tipos de dados que ela deve proteger e qual o impacto de perdê-los.
2. Enumere os equipamentos de tecnologia que compõem um parque tecnológico de porte intermediário, quais as potenciais vulnerabilidades.
3. Identifique alguns dos equipamentos de proteção necessários e faça uma rápida pesquisa na internet e estime o custo para esse investimento.

ENCERRAMENTO

Resumo e Próximos Passos

- Noções básicas de segurança e equipamentos
- Noções de redundância e backup
- Noções de básicas de ataque cibernético
  - Alguns exemplos de proteção
- **Pós Aula**: Saiba Mais, A Seguir e Desafio!
  - No mural: https://padlet.com/djcaetano/segciber

- Equipamentos básicos da rede
- Vulnerabilidades comuns

PERGUNTAS?