



SEGURANÇA CIBERNÉTICA

PRINCÍPIOS DE SEGURANÇA CIBERNÉTICA II

Prof. Dr. Daniel Caetano

2021 - 2

Compreendendo o problema

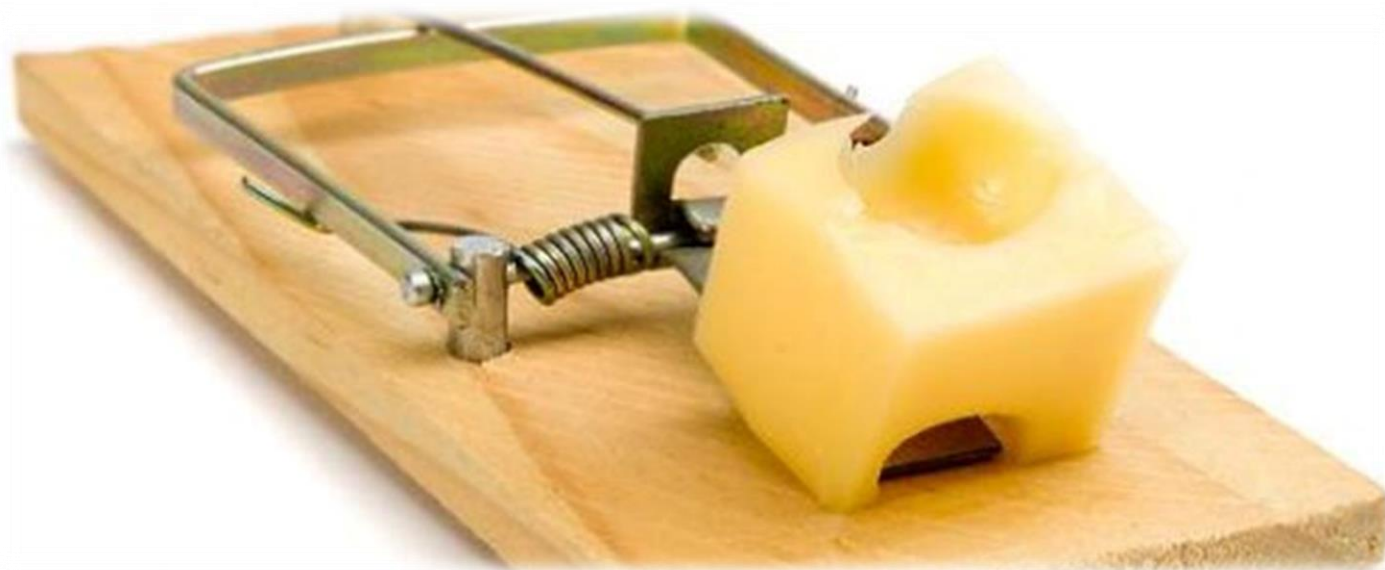
- **Situação:** Se há vários tipos de investimentos a serem feitos, como dimensioná-los?



O que precisamos medir?

Compreendendo o problema

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



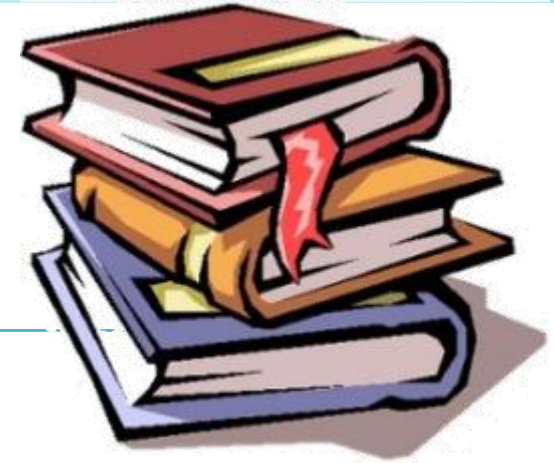
Qual é o primeiro passo para evitar uma armadilha?

Objetivos

- Compreender onde se localizam as principais vulnerabilidades
- Entender como um ataque se inicia
- Tomar contato com alguns tipos comuns de ataques e algumas estratégias de prevenção



Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 3)
Minha Biblioteca	<ul style="list-style-type: none">• 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	<ol style="list-style-type: none">1) 5 ferramentas de segurança para proteger sua rede! - Disponível em: https://youtu.be/ClInn1mpc67M2) Como dimensionar os equipamentos de segurança em sua rede - Disponível em: https://youtu.be/fw1tVXBURDk



VISÃO GERAL:

ONDE PODEMOS ENCONTRAR VULNERABILIDADES?



Onde estão as vulnerabilidades?

- Onde estão?
- Múltiplas fontes
 - Pessoas
 - Engenharia Social
 - Softwares
 - Falhas de design
 - Falhas de implementação
 - Problemas de configuração
 - Equipamentos e Infraestrutura
 - Falhas de hardware/software/configuração
 - Problemas de capacidade



Quais são os equipamentos?

- Operações x Datacenter
 - No datacenter: equipamentos básicos x proteção
- 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.
 - Armazenamento
 - *Storages*
 - Processamento
 - Servidores.



Equipamentos/Sistemas 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)

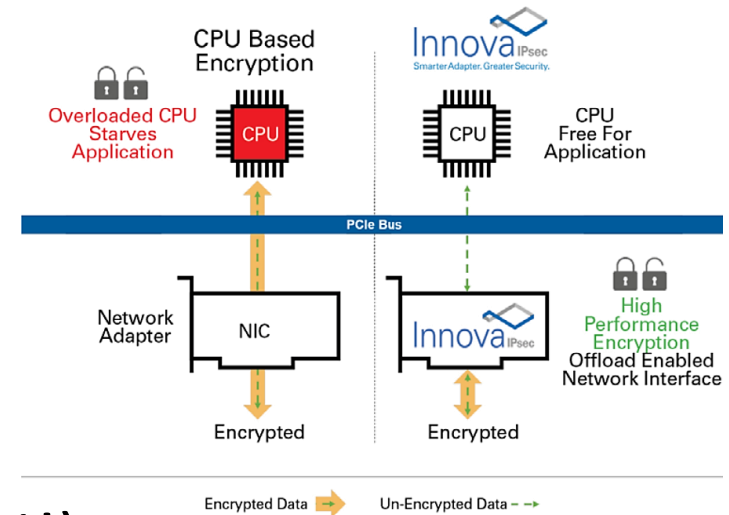
Capacidade dos equipamentos

- Indisponibilidade por incapacidade
 - Tem a ver com segurança?
- Cuidados na aquisição!
 - Especificações de Compra
 - RFCs/Benchmarks...
 - Cuidado com os datasheets!
 - NSS Labs (faz testes mais padronizados).

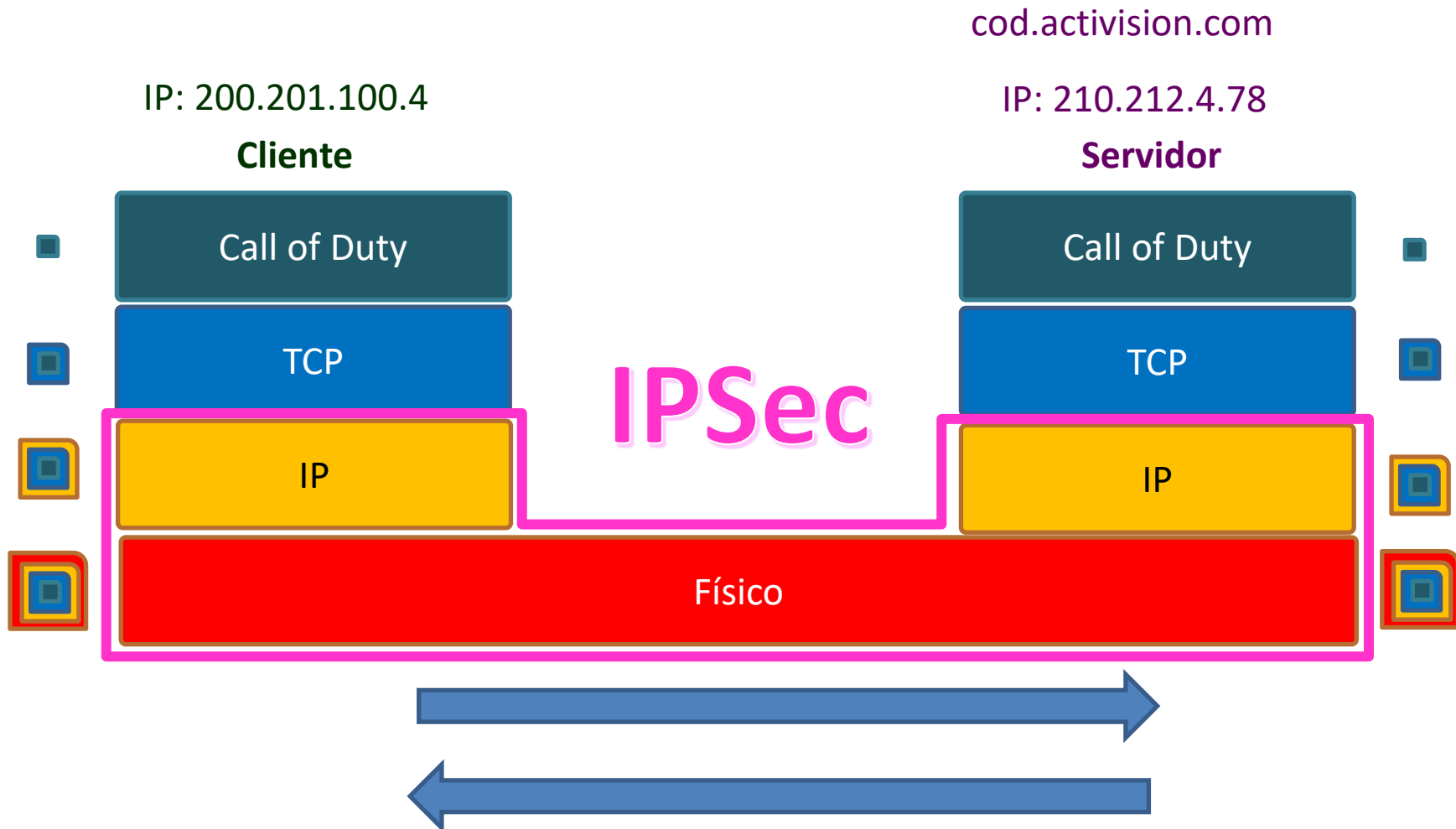


Capacidade dos equipamentos

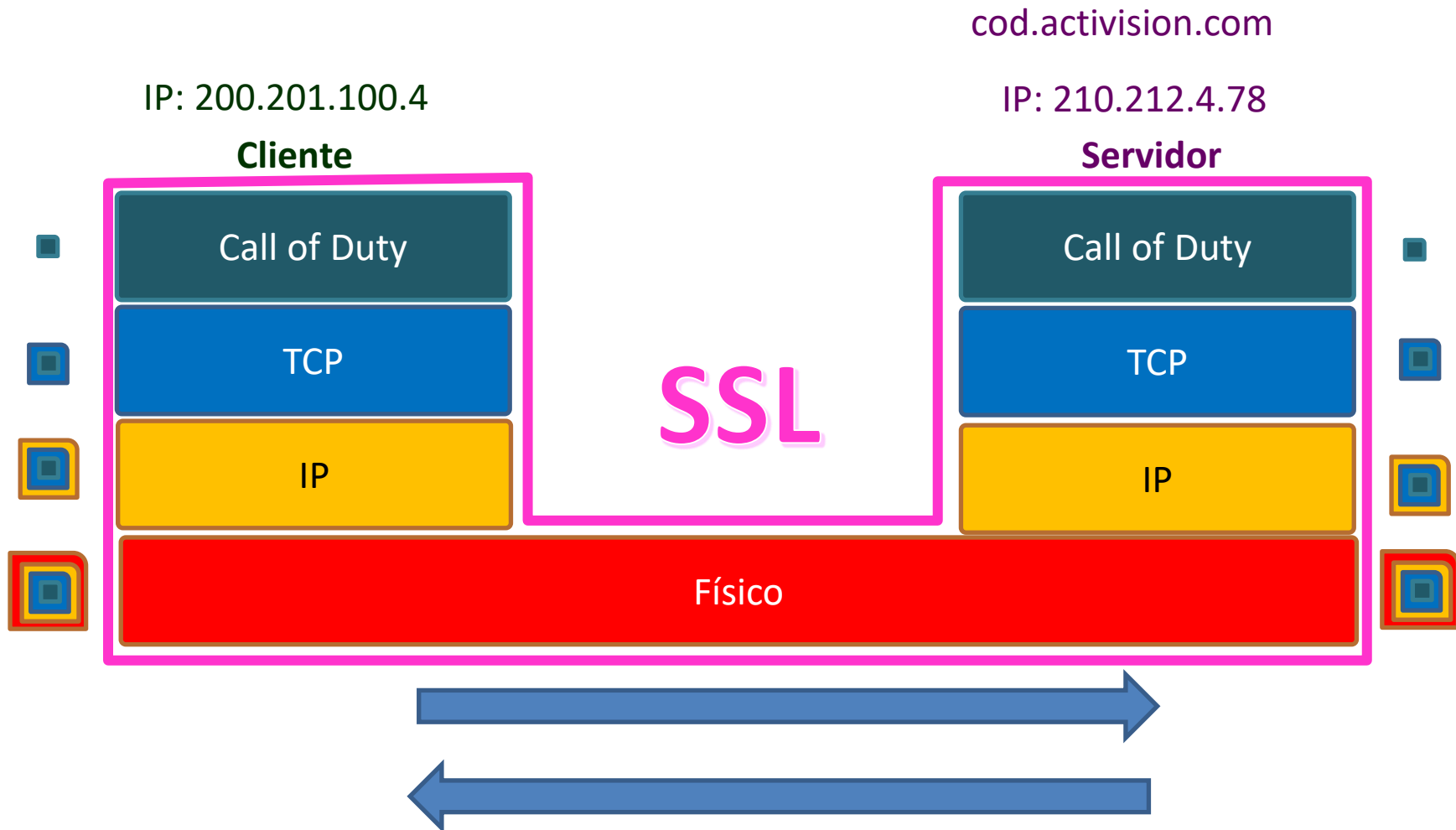
- Dados necessários
 - # de usuários simultâneos
 - # de pacotes por segundo
 - *Throughput* da rede
 - # de transações SSL (...>70%!)
 - Perfil de pacotes (IMIX) – 64 bytes a 9000...
 - Considerar o crescimento da empresa
- Conheça seus equipamentos!
- IPSec e SSL impõem peso enorme
 - Capacidade de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



Atuação do IPSec e do SSL



Atuação do IPsec e do SSL



QUAIS OS PRIMEIROS PASSOS DE UM ATAQUE?



Caminhos para um ataque

- Ataques são planejados
- Início dos ataques planejados?
 - 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)...
 - Illegal: empresas de fachada, roubar lixo, keylogger, farejadores não autorizados...
- Categorias comuns:
 - Engenharia Social
 - Mergulho no Lixo
 - Rastreamento 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.



Rastreamento de Pegadas

- O que é?
 - Seguir os “rastros” das pessoas
- O que envolve?
 - Redes sociais
 - Buscas na web
 - [WayBack Machine](#)



Rastreamento de Pegadas

- O que é?
 - Seguir os “rastros” das pessoas
- O que envolve?
 - Redes sociais
 - Buscas na web
 - [WayBack Machine](#)
 - [Cache do Google](#)



Rastreamento de Pegadas

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



Rastreamento de Pegadas

- O que é?
 - Seguir os “rastros” das pessoas
- 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



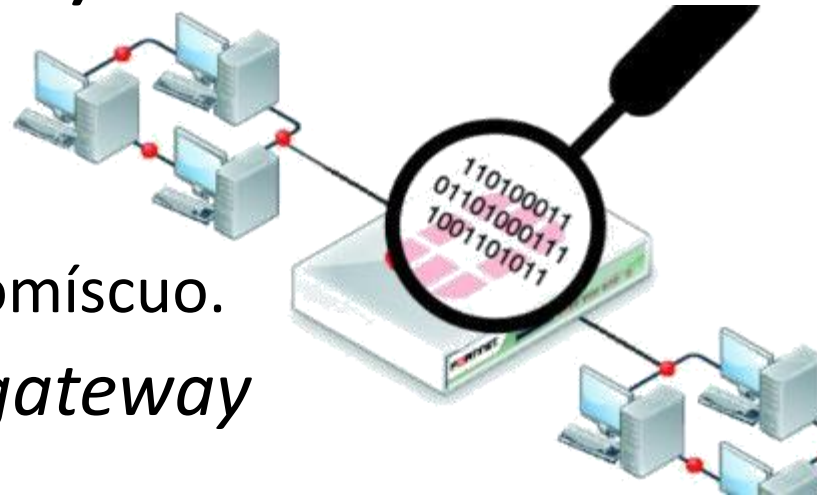
Farejadores (*Sniffers*)

- 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 promísquo.
- Local ideal de instalação: *gateway*
- Como se proteger
 - Detectores... apenas verificam condições
 - Antisniff/Neped.c: rede em modo promísquo
 - SniffDet: # de consultas ao dns, ping com MAC falso etc.
 - Criptografia
 - SSL/TLS
 - PGP ou similares
 - SSH



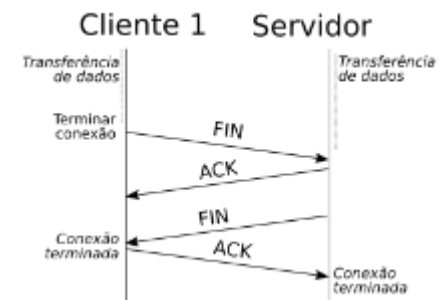
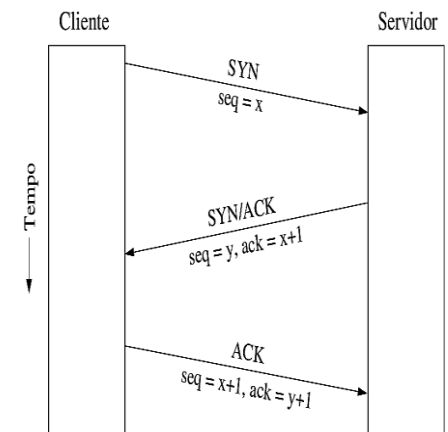
Voltaremos a isso!



ENTENDENDO A BASE DAS VULNERABILIDADES DO TCP/IP

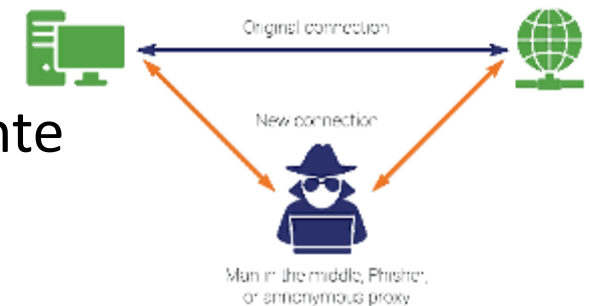
Aspectos do TCP/IP

- Protocolo simples e rápido: não segurança
- Como ocorre a transmissão?
 - Dados são empacotados e transmitidos em aberto
- Tipos de Pacotes
 - 6 Flags: URG, ACK, PSH, RST, SYN e FIN
 - Normalmente 1 ou 2 ativas por pacote
 - Início de comunicação:
 - SYN origem >> ACK destino (SEQ)
 - SYN destino >> ACK origem
 - FIN/RST: finalizar conexão
 - PSH/URG: mudar a prioridade nas filas
- Temporizadores de espera.



Vulnerabilidades do TCP/IP

- Não há criptografia ou autenticação por padrão
- Falsificação de IP
 - Precisa adivinhar o sequenciamento pro ACK
- Roteamento de remetente
 - Fornecia caminho de retorno
- Sequestro de conexão
 - Envia pacotes para o destino como se origem fosse
- Ataque ICMP (DoS)
 - Ajustes no cabeçalho para forçar um RST na conexão
- Ataque TCP SYN (DoS)
 - Iniciar múltiplas conexões rapidamente
- Ataque RIP
 - Redefinir o roteamento da rede



Desviando das vulnerabilidades

- Falhas inerentes, difícil eliminação
 - Usar criptografia ajuda (autenticação, sessões, tráfego...)
- Falsificação de IP
 - Mudar o método de gerar esse número (pouco prático)
- Ataque TCP SYN (DoS)
 - Reduzir o timeout entre SYN e ACK
 - Limitar as conexões por um mesmo IP
 - Aumentar o número de conexões simultâneas total.
- Sequestro de conexão
 - Envia pacotes para o destino como se origem fosse
- Ataque ICMP (DoS)
 - IDS/IPS
- Ataque RIP
 - Implementar firewall





ATIVIDADE

Atividade

- Discussão – Grupos – 15 minutos
- Considerando esses serviços e o que estudamos na aula, quais são as principais vulnerabilidades?
 - Elabore uma lista com 3 itens
- Escolha um colega de seu grupo e busque na internet informações sobre ele.
 - Vocês conseguiram encontrar alguma coisa que pudesse ser usada num ataque?



ENCERRAMENTO

Resumo e Próximos Passos

- Equipamentos básicos
 - Noções de dimensionamento
 - Vulnerabilidades comuns
 - Compreendendo x Evitando
 - **Pós Aula:** Aprenda Mais, Pós Aula e Desafio!
 - No padlet: <https://padlet.com/djcaetano/segciber>
-
- Interceptação de tráfego e mapeamento
 - Como funciona e o que dá pra descobrir?



PERGUNTAS?