Segurança Cibernética

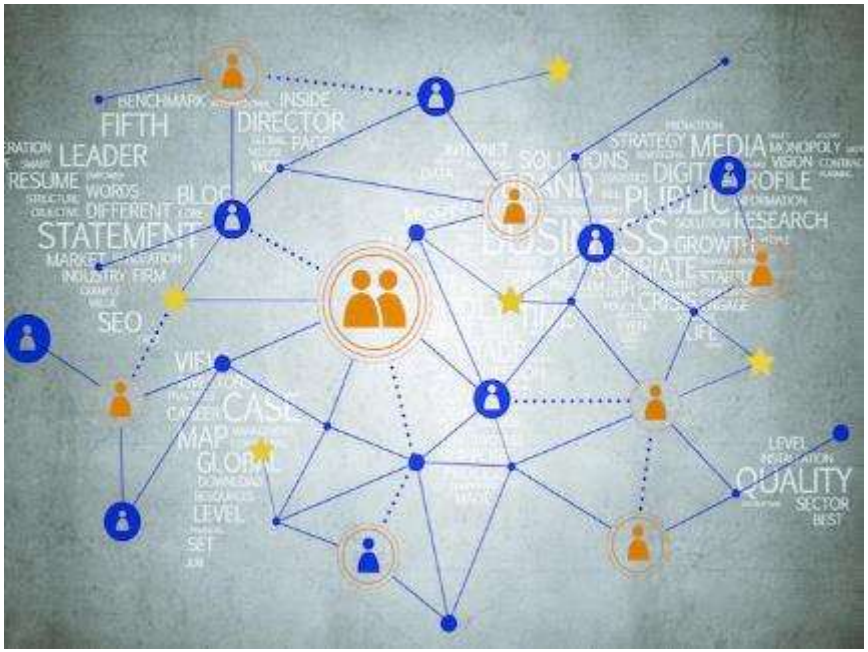
Ameaças, Vulnerabilidades e Ataques I:
Interceptação de Tráfego e Mapeamento de Redes

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** Entre a origem e o destino, os dados circulam pela rede, passando por muitos equipamentos.

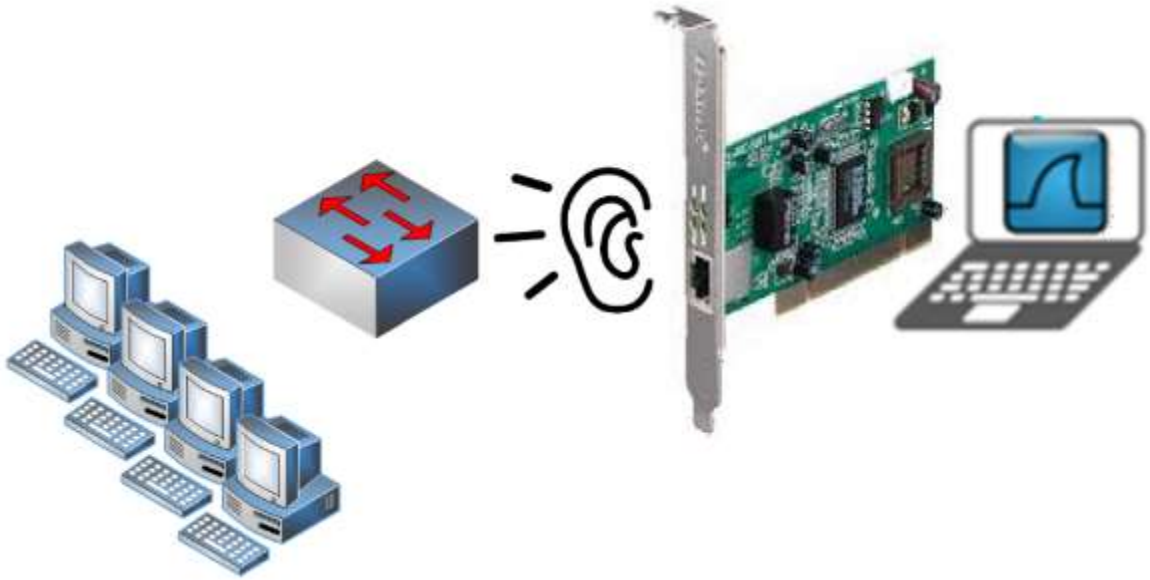


A quais riscos estão expostos??

Mentimeter

Compreendendo o problema

- **Situação:** O correto uso e a prevenção de interceptações exigem conhecimento técnico e bons progr

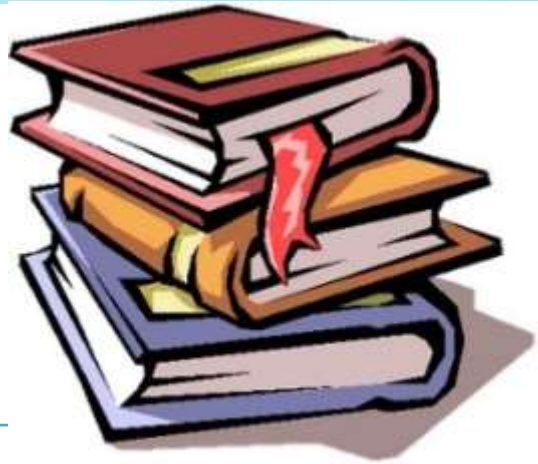


Você saberia usar esses programas?

Objetivos

- Compreender os fundamentos necessários para o uso dos programas
- Compreender o que é e como se utiliza um *sniffer* de rede
- Compreender o que é e como se utiliza um mapeador de rede

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 4)
Minha Biblioteca	• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 43 a 45. • Redes de computadores: uma abordagem top-down (978-85-8055-169-3), págs 43 a 82.
Material Adicional	1) Como interceptar conexões IP em um laboratório de análises de malware - Dispoinível em: https://youtu.be/1KBv1Yp78qM (em inglês) 2) Dicionário de Informática: Sniffing - Dispoinível em: https://youtu.be/yZdhAXMWw-c 3) badKarma - Kit de Ferramentas Avançadas de Reconhecimento de Rede – Disponível em https://youtu.be/oQMCwh4NMsI

Visão Geral:

Recordando o Ambiente

Ferramentas de Análise

- Analisar o quê?
  - Tráfego de rede
  - Mapa de “destinos” dos dados

- Compreender o uso das ferramentas
  - Exige entender a rede... como já recordamos
  - Vamos ! detalhes!

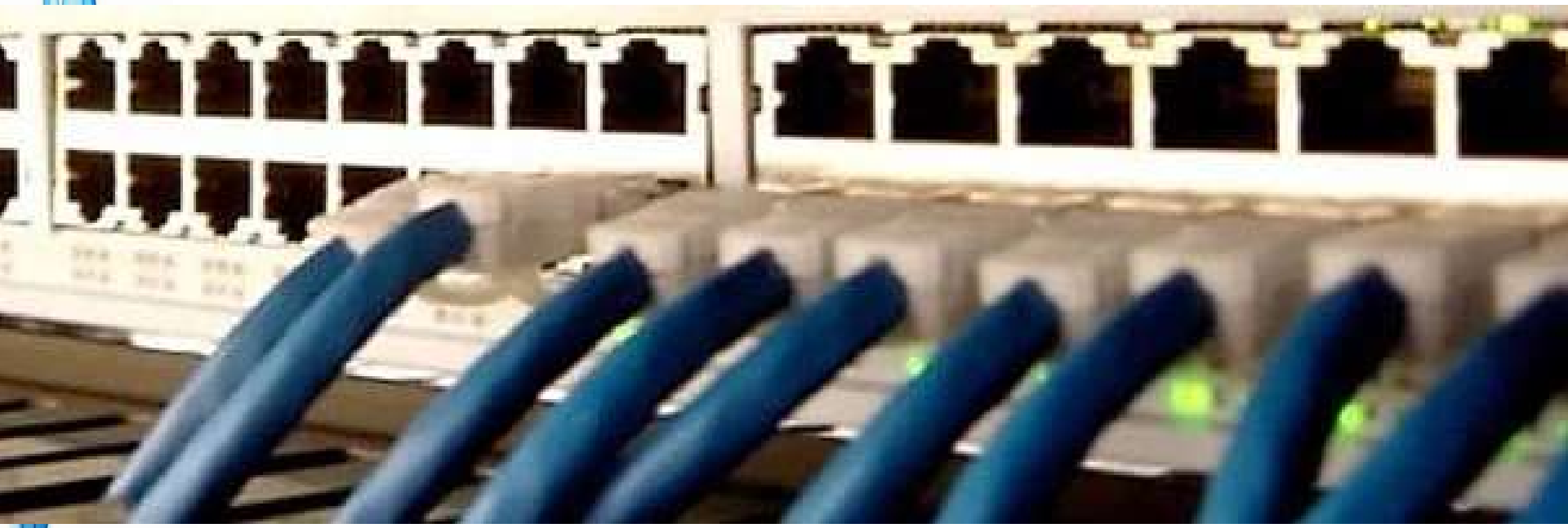
Ambiente

Mentimeter

Comunicação em Rede e TCP/IP

Objetivo da Comunicação

- Transmitir dados da origem ao destino
  - Conjunto de dados coerente
  - Ex.: Arquivo, vídeo, áudio...

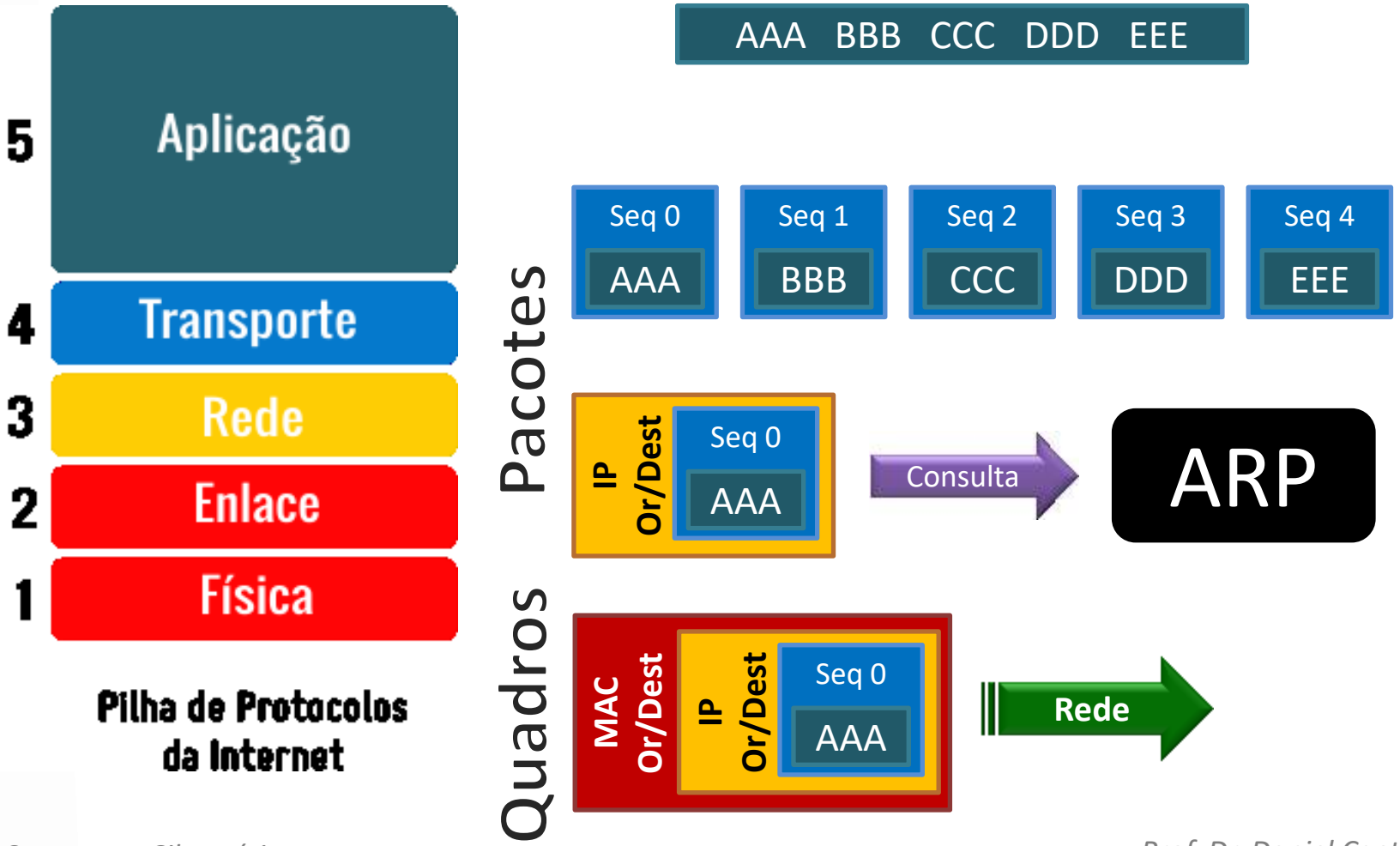


Requisitos da Comunicação

- Requisito fundamental da entrega
  - Completude: TCP
  - Fluência: UDP
- Eficiência / Latência:
  - Qualidade do meio
    - Ar x Cobre x Fibra
  - Tamanho dos pacotes
    - Proporção *payload* x cabeç

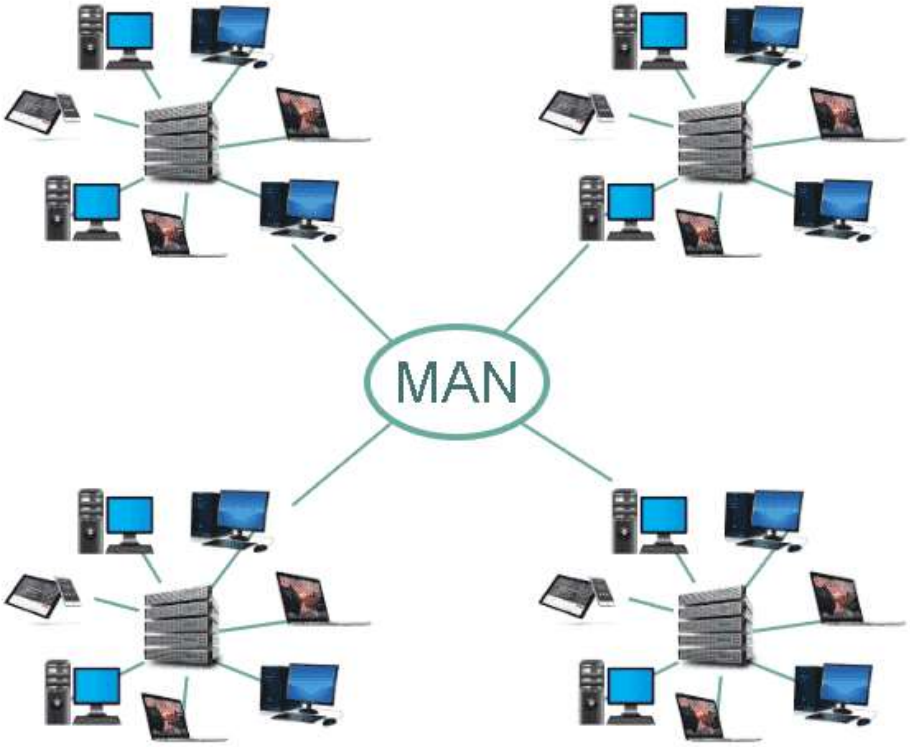
Preparação dos Dados

- Dados → Pacotes → Quadros



Encaminhamento dos Dados

- Destino na Rede Local x Internet
  - Verifica pela máscara de rede



Encaminhamento Local `arp -a`

1. Ajusta os frames com o MAC do destino

```
Interface: 192.168.0.201 --- 0x7
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           d8-c6-78-36-84-48     dinâmico
  192.168.0.3           74-da-88-37-b6-98     dinâmico
  192.168.0.4           30-b5-c2-fb-bb-7a     dinâmico
  192.168.0.10          00-1a-3f-8a-db-d9     dinâmico
  192.168.0.105         58-fd-b1-eb-8c-74     dinâmico
  192.168.0.125         74-a7-ea-20-e8-98     dinâmico
```

- Se não estiver: broadcast ARP
  - MAC: FF:FF:FF:FF:FF:FF
  - Quem tem o IP tal?
  - Switchs/bridges replicam o broadcast
  - Roteadores/gateways não replicam

Encaminhamento Local

1. Ajusta os frames com o MAC do destino

```
Interface: 192.168.0.201 --- 0x7
  Endereço IP           Endereço físico      Tipo
  192.168.0.1           d8-c6-78-36-84-48    dinâmico
  192.168.0.3           74-da-88-37-b6-98    dinâmico
  192.168.0.4           30-b5-c2-fb-bb-7a    dinâmico
  192.168.0.10          00-1a-3f-8a-db-d9    dinâmico
  192.168.0.105         58-fd-b1-eb-8c-74    dinâmico
  192.168.0.125         74-a7-ea-20-e8-98    dinâmico
  192.168.0.192         f4-ce-46-21-e7-55    dinâmico
  192.168.0.193         74-29-af-39-bc-29    dinâmico
  192.168.0.200         e0-69-95-4f-5a-81    dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff    estático
```

2. Ajusta frame com MAC destino
3. Encaminha pacote pela rede

Encaminhamento Internet

1. Consulta a tabela de roteamento (gateway)

```
Tabela de rotas IPv4
===========================================================================
Rotas ativas:
Endereço de rede            Máscara   Ender. gateway       Interface   Custo
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.201     281
        127.0.0.0        255.0.0.0      No vínculo         127.0.0.1     331
        127.0.0.1  255.255.255.255      No vínculo         127.0.0.1     331
  127.255.255.255  255.255.255.255      No vínculo         127.0.0.1     331
      192.168.0.0    255.255.255.0      No vínculo     192.168.0.201     281
    192.168.0.201  255.255.255.255      No vínculo     192.168.0.201     281
    192.168.0.255  255.255.255.255      No vínculo     192.168.0.201     281
        224.0.0.0        240.0.0.0      No vínculo         127.0.0.1     331
        224.0.0.0        240.0.0.0      No vínculo     192.168.0.201     281
  255.255.255.255  255.255.255.255      No vínculo         127.0.0.1     331
  255.255.255.255  255.255.255.255      No vínculo     192.168.0.201     281
===========================================================================
Rotas persistentes:
  Endereço de rede            Máscara  Ender. gateway    Custo
          0.0.0.0          0.0.0.0      192.168.0.1  Padrão
===========================================================================
```

route print

Encaminhamento Internet

2. Ajusta os frames com o MAC do gateway

```
Interface: 192.168.0.201 --- 0x7
  Endereço IP           Endereço físico      Tipo
  192.168.0.1           d8-c6-78-36-84-48    dinâmico
  192.168.0.3           74-da-88-37-b6-98    dinâmico
  192.168.0.4           30-b5-c2-fb-bb-7a    dinâmico
  192.168.0.10          00-1a-3f-8a-db-d9    dinâmico
  192.168.0.105         58-fd-b1-eb-8c-74    dinâmico
  192.168.0.125         74-a7-ea-20-e8-98    dinâmico
  192.168.0.192         f4-ce-46-21-e7-55    dinâmico
  192.168.0.193         74-29-af-39-bc-29    dinâmico
  192.168.0.200         e0-69-95-4f-5a-81    dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff    estático
```

3. Encaminha frame pela rede

4. Roteador vai repetir todo o processo

Serviços e Portas TCP

- Podemos ter um único serviço no servidor?
  - Ou é servidor web ou servidor de e-mail?
- Não! Podemos ter vários!
  - Mas o endereço é um só!

- Imagine um edifício comercial
  - Endereço do prédio: endereço IP
  - Número da Sala/Conjunto: Serviço

Serviços e Portas TCP

- Alguns serviços e portas comuns

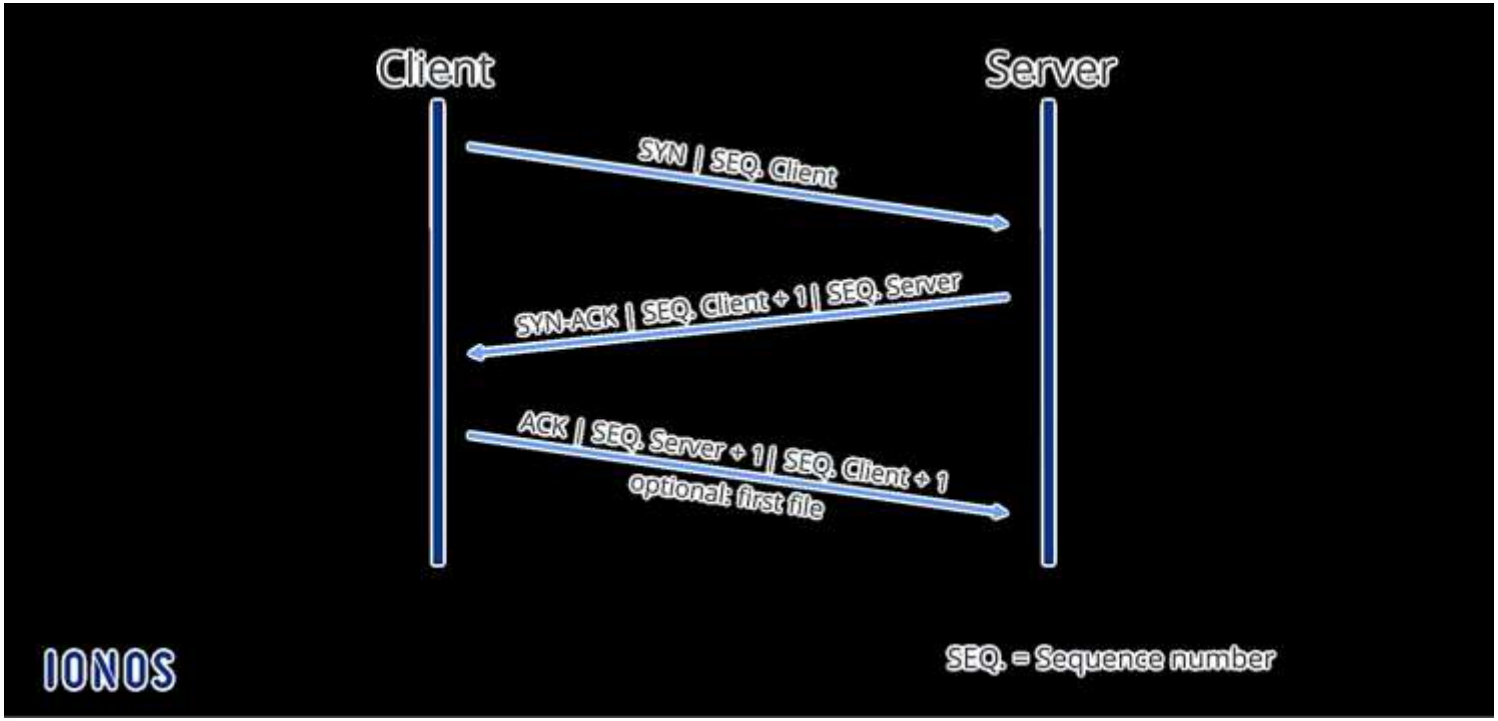
Serviço	Porta Normal	Porta Segura
FTP	21	22
SSH		22
Telnet	23	
SMTP	25	465 / 587
DNS	53	
HTTP	80	443
POP3	110	995
IMAP	143	993
IRC	6667	
MySQL	3306	
MSSQL	1039	

Transmissão de Dados em TCP/IP

- Como ocorre a transmissão?
  - Dados são empacotados e transmitidos em aberto
- Tipos de Pacotes
  - 6 Flags:
    - URG: Urgent (muda prioridade)
    - ACK: Acknowledge (confirma recebimento)
    - PSH: Push (muda prioridade)
    - RST: Reset (finaliza conexão)
    - SYN: Sync (sincroniza – “aperto de mão”)
    - FIN: Finalize (solicita fim de conexão)
    - Normalmente 1 ou 2 ativas por pacote

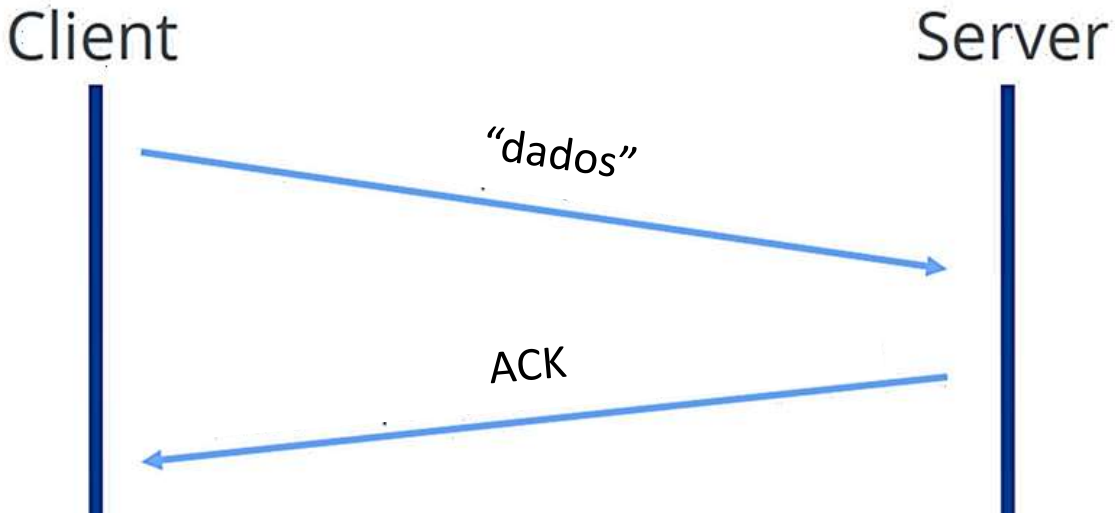
Transmissão de Dados em TCP/IP

- Estabelecer conexão
  - Início de comunicação:
    - SYN origem >> ACK destino (SEQ)
    - SYN destino >> ACK origem



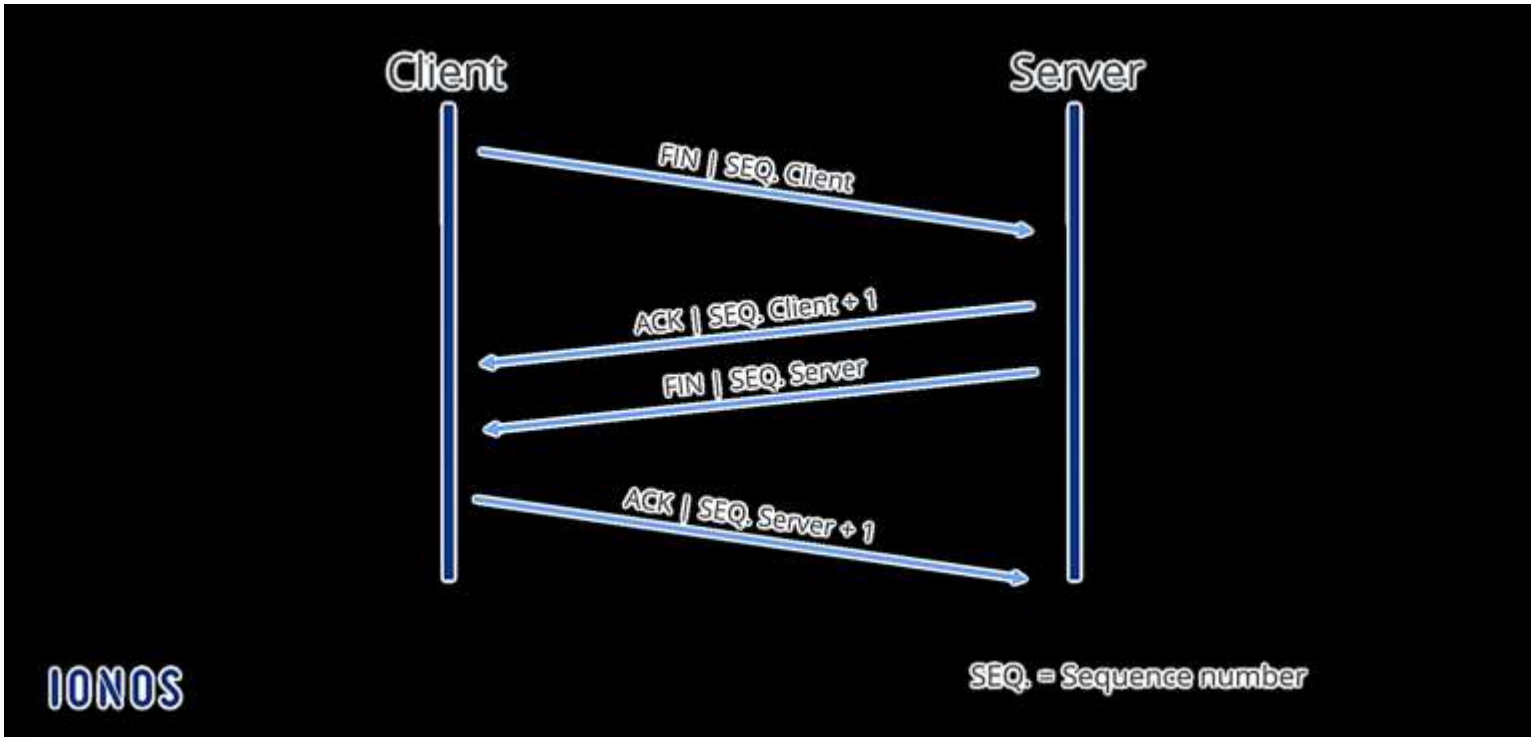
Transmissão de Dados em TCP/IP

- Transmissão de dados
  - Repetido várias vezes durante a transmissão
    - Dados origem >> ACK destino



Transmissão de Dados em TCP/IP

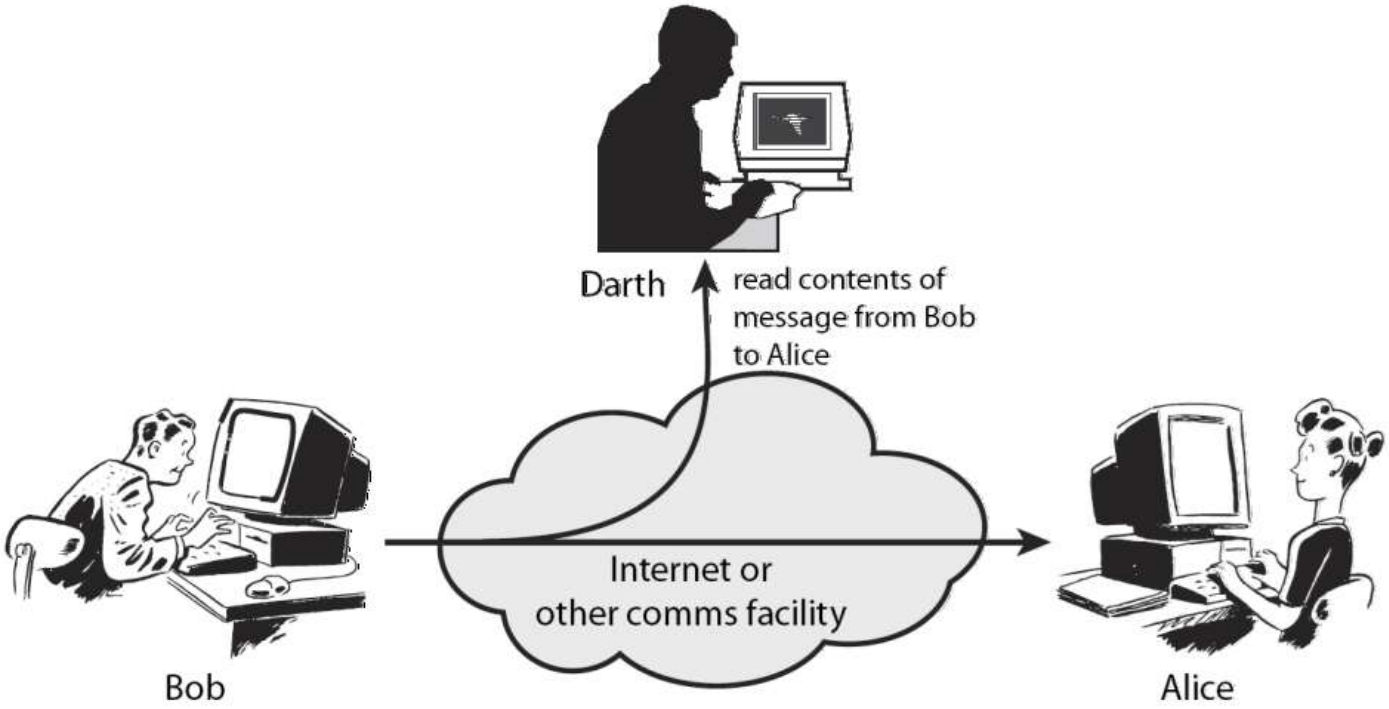
- Finalizar conexão
  - Fim de comunicação:
    - FIN origem >> ACK destino (SEQ)
    - FIN destino >> ACK origem



Análise de Tráfego

Sniffers

- O que são?
- Há dois tipos
  -
  -



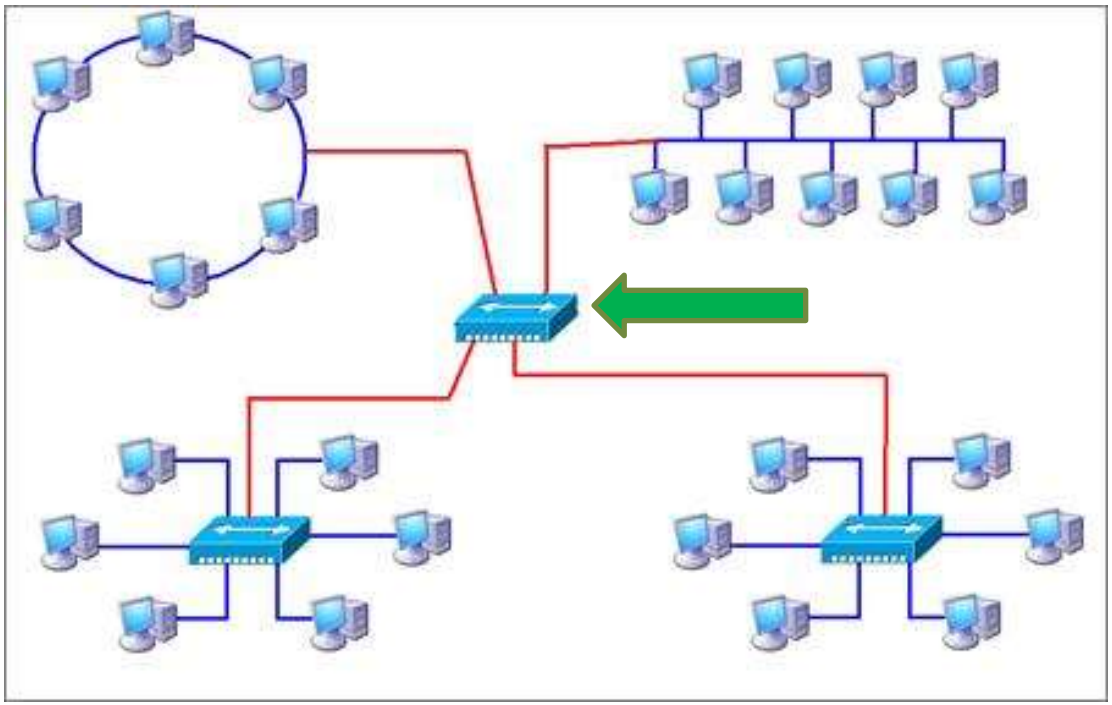
Sniffers

- Para quê servem?
  - Uso legal: identificar problemas na rede
    - Problemas de comunicação (não co
    - Problemas de sobrecarga (lentidão)
    - ...

  - Uso “discutível”: vasculhar pacotes
    - Necessário autorização
    - Sem autorização: como escuta telefônica.

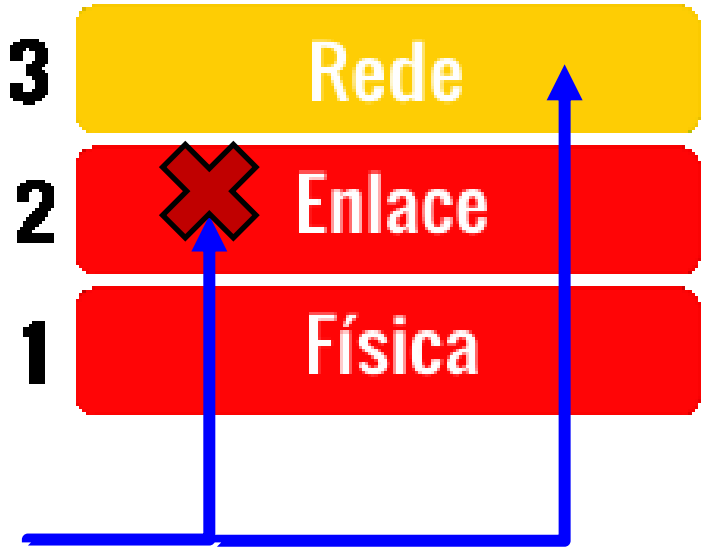
Sniffers

- Eficácia
  - Limitado ao segmento de rede
    - Ideal instalar no **gateway**



Sniffers

- Eficácia
  - Limitado ao segmento de rede
    - Ideal instalar no gateway
  - Placas de rede em modo promíscuo
    - Todos os dados da rede ficam disponíveis

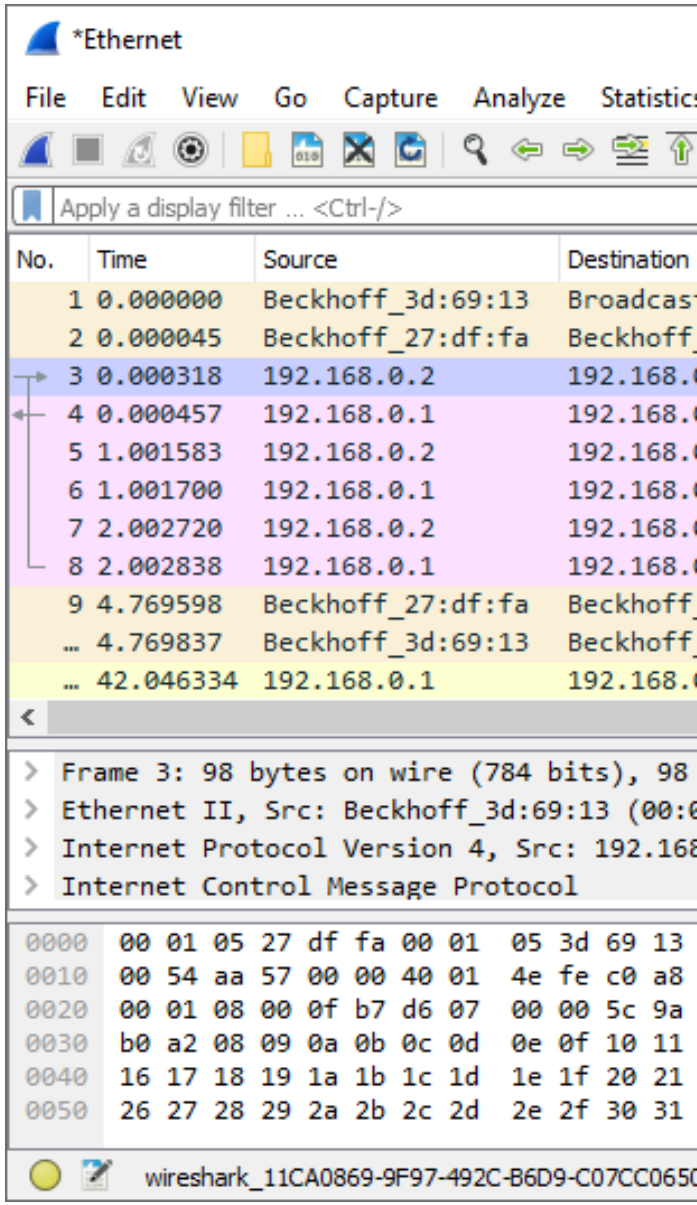


Sniffers

- Eficácia
  - Limitado ao segmento de rede
    - Ideal instalar no gateway
  - Placas de rede em modo promíscuo
    - Todos os dados da rede ficam disponíveis
  - Analisar “offline”
    - Analisar em tempo real pode ser muito confuso!

Sniffers

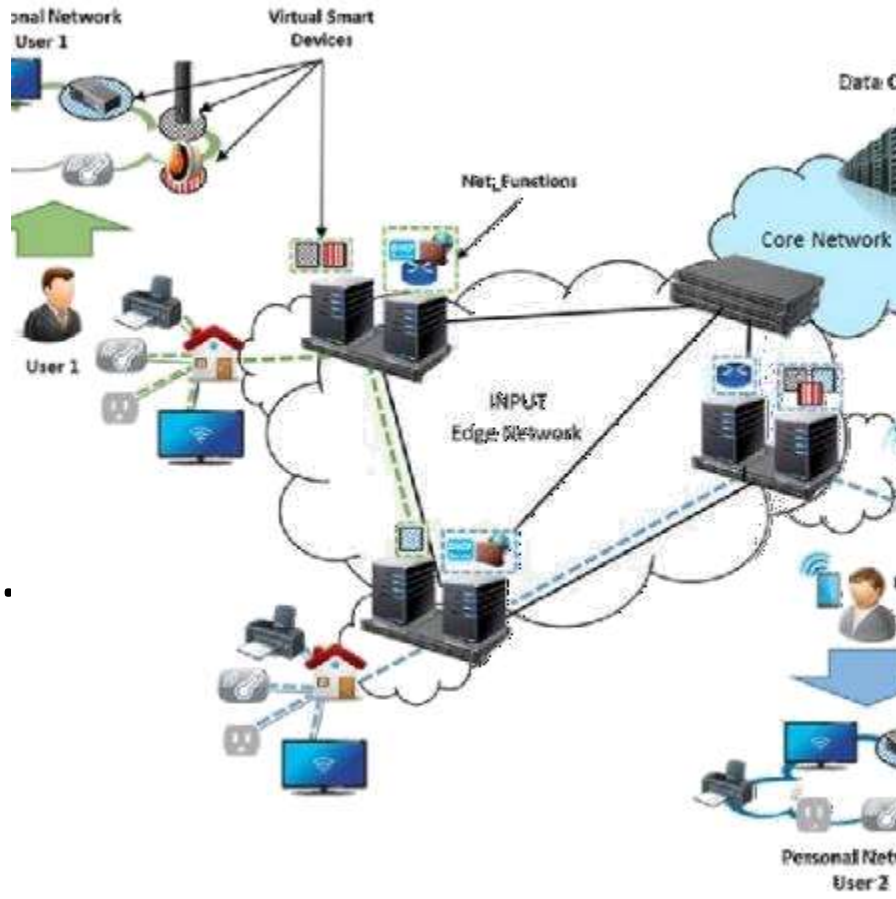
- Conhecendo o Wireshark
  - Organização
  - Estrutura dos dados
  - Filtros
  - Entendendo os pacotes
  - Seguindo os pacotes
  - Analisando os pacotes



Mapeamento de Redes

Mapeamento de Rede

- O que é isso?
- Identificar
  - Caminhos dos dados
  - Portas em uso
  - Serviços em execução
  - Versão de software e S.
  - ...



Mapeamento de Rede

- Por que funciona?
  - Princípio da comunicação
    - Para ser acessível, precisa estar aberto
  - Variações na forma de comunicação
    - Protocolos mudam com o tempo
    - Implementações mudam com o tempo
    - Permitem identificar tipos e versões de software.

Mapeamento de Rede

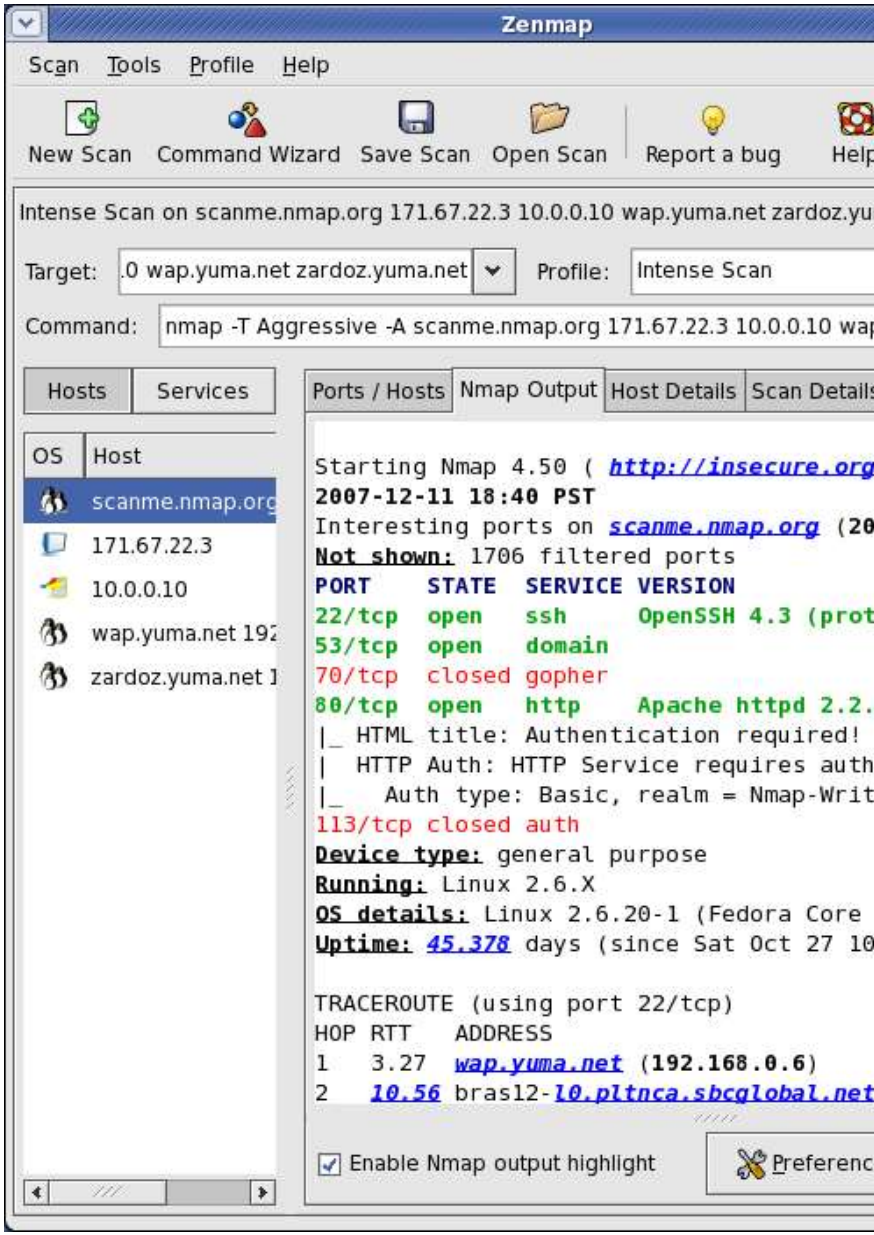
- Efetividade
  - Depende das configurações do firewall
    - Pode bloquear muitas consultas
  - Fica na zona cinza da lei
    - Similar a observar dentro da casa de outra pessoa
  - Para testar...
    - Site: scanme.nmap.org

Mapeamento de Rede

- Aplicação mais comum: NMap
  - Usa primariamente as camadas de rede e transp.
    - IP e TCP
  - Também usa dados da camada enlace
  - Part
    - L eis

Mapeamento de Rede

- Conhecendo o NMap
  - Scan simples
  - Scan de range
  - Scan intense
  - Scan longo



ATIVIDADE

Atividade

- Individual!
- Escolha um site e use o wireshark para monitorar os pacotes trocados com esse site. O que você conseguiu identificar nesse tráfego?
- Descubra o IP público de sua máquina ou rede com o https://www.whatismyip.com/. Execute o Nmap online https://nmap.online/ para ver se consegue encontrar algum serviço aberto. Que serviço é esse?
- Experimente depois instalar o Zenmap em sua máquina, e rodá-lo no IP interno, que você descobre com o ipconfig /all

ENCERRAMENTO

Resumo e Próximos Passos

- Noções do roteamento de pacotes
- Wireshark
  - Compreendendo o uso básico
- Nmap
  - Mapeando uma rede
- **Pós Aula**: Saiba Mais, A Seguir... e Desafio!
  - No mural: https://padlet.com/djcaetano/segciber

- Códigos maliciosos e a internet
  - A Engenharia Social na rede

PERGUNTAS?