



# SEGURANÇA CIBERNÉTICA

## AMEAÇAS, VULNERABILIDADES E ATAQUES I: INTERCEPTAÇÃO DE TRÁFEGO E MAPEAMENTO DE REDES

Prof. Dr. Daniel Caetano

2021 - 2

# Compreendendo o problema

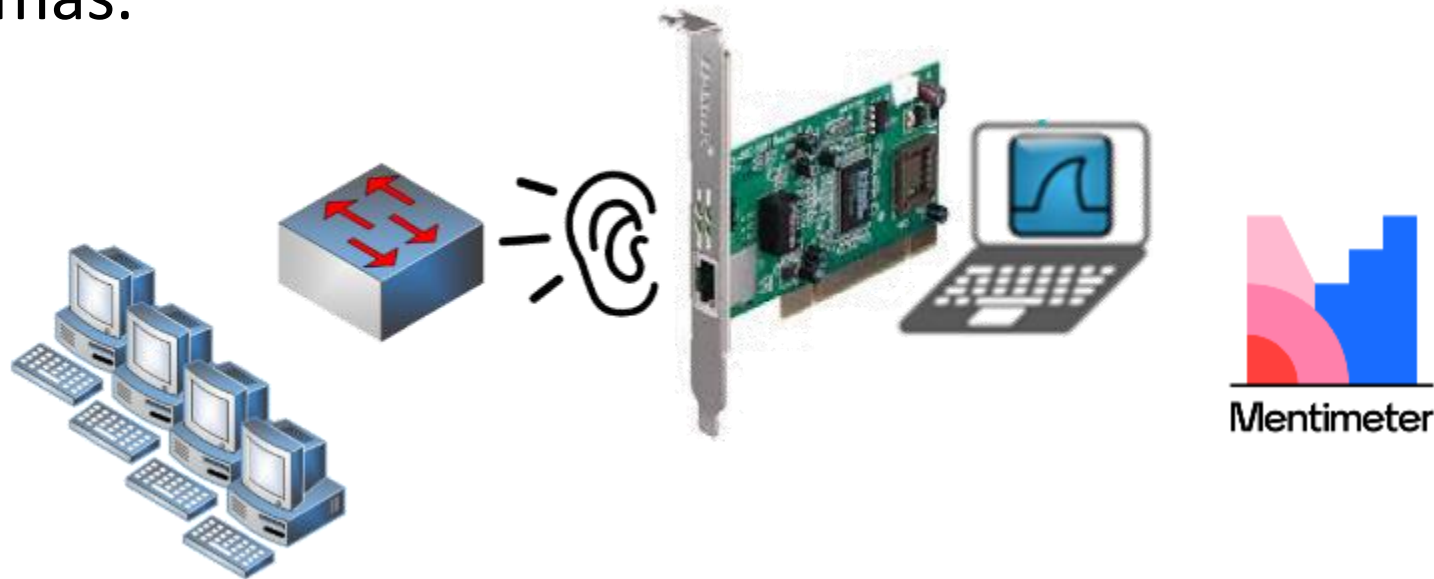
- **Situação:** Entre a origem e o destino, os dados circulam pela rede, passando por muitos equipamentos.



**A quais riscos estão  
expostos??**

# Compreendendo o problema

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



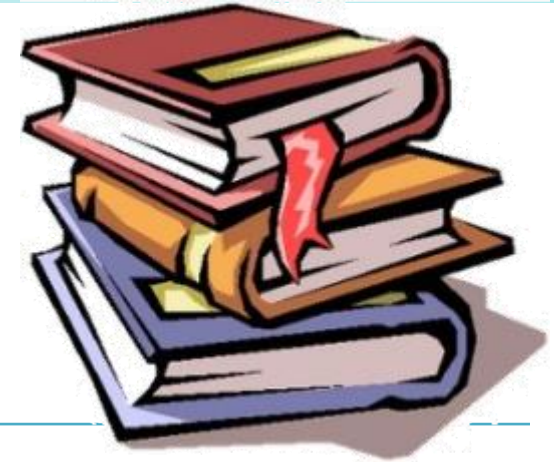
**Você saberia usar esses programas?**

# 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	<a href="https://www.caetano.eng.br/aulas/2021b/ara0076.php">https://www.caetano.eng.br/aulas/2021b/ara0076.php</a> (Segurança Cibernética – Aula 4)
Minha Biblioteca	<ul style="list-style-type: none"><li>• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 43 a 45.</li><li>• Redes de computadores: uma abordagem top-down (978-85-8055-169-3), págs 43 a 82.</li></ul>
Material Adicional	<ol style="list-style-type: none"><li>1) Como interceptar conexões IP em um laboratório de análises de malware - Disponível em: <a href="https://youtu.be/1KBv1Yp78qM">https://youtu.be/1KBv1Yp78qM</a> (em inglês)</li><li>2) Dicionário de Informática: Sniffing - Disponível em: <a href="https://youtu.be/yZdhAXMWw-c">https://youtu.be/yZdhAXMWw-c</a></li><li>3) badKarma - Kit de Ferramentas Avançadas de Reconhecimento de Rede – Disponível em <a href="https://youtu.be/oQMCwh4NMsl">https://youtu.be/oQMCwh4NMsl</a></li></ol>



**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 reforçar e aprofundar alguns detalhes!



# Ambiente







# COMUNICAÇÃO EM REDE E TCP/IP



# Objetivo da Comunicação

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



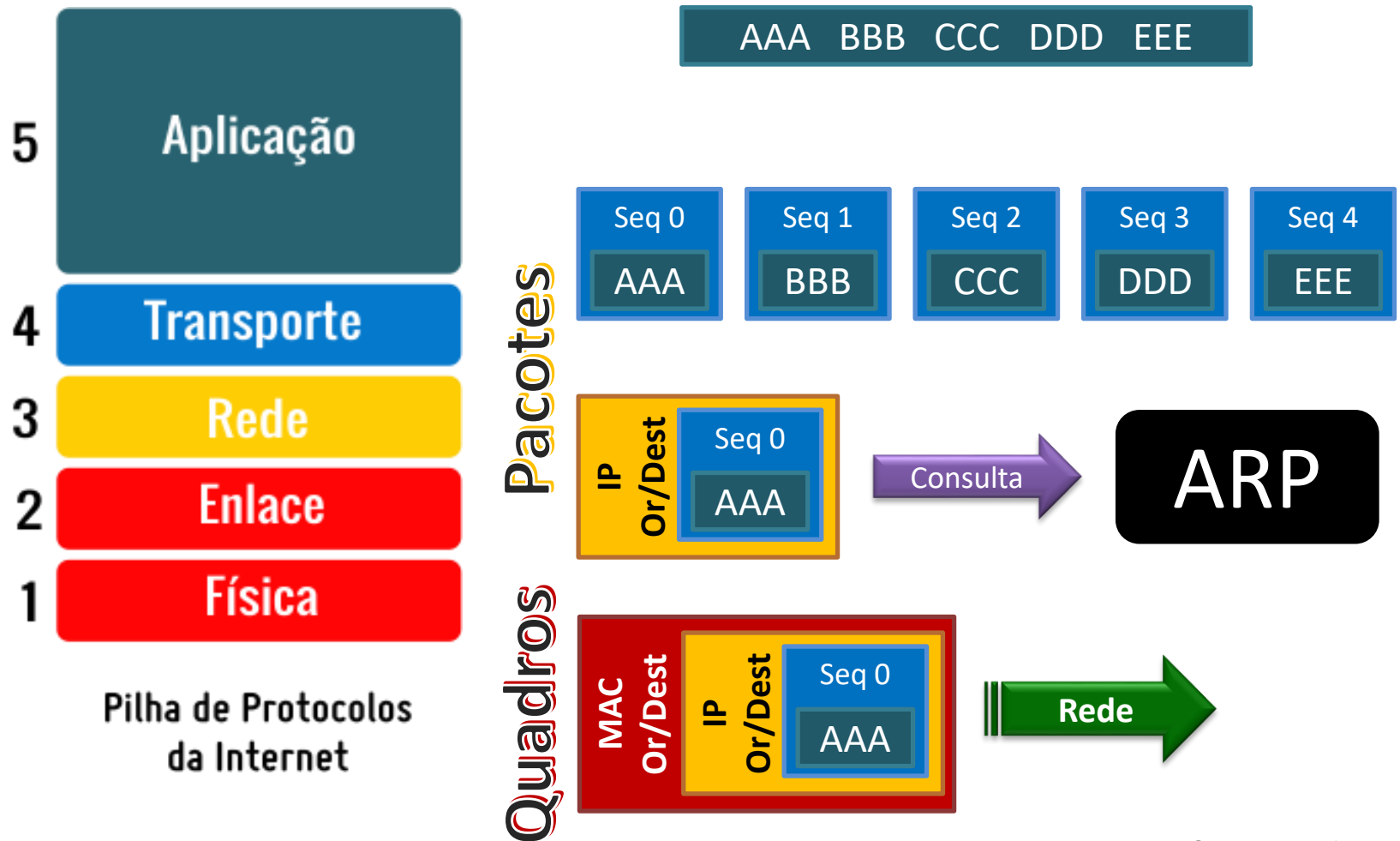
# Requisitos da Comunicação

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



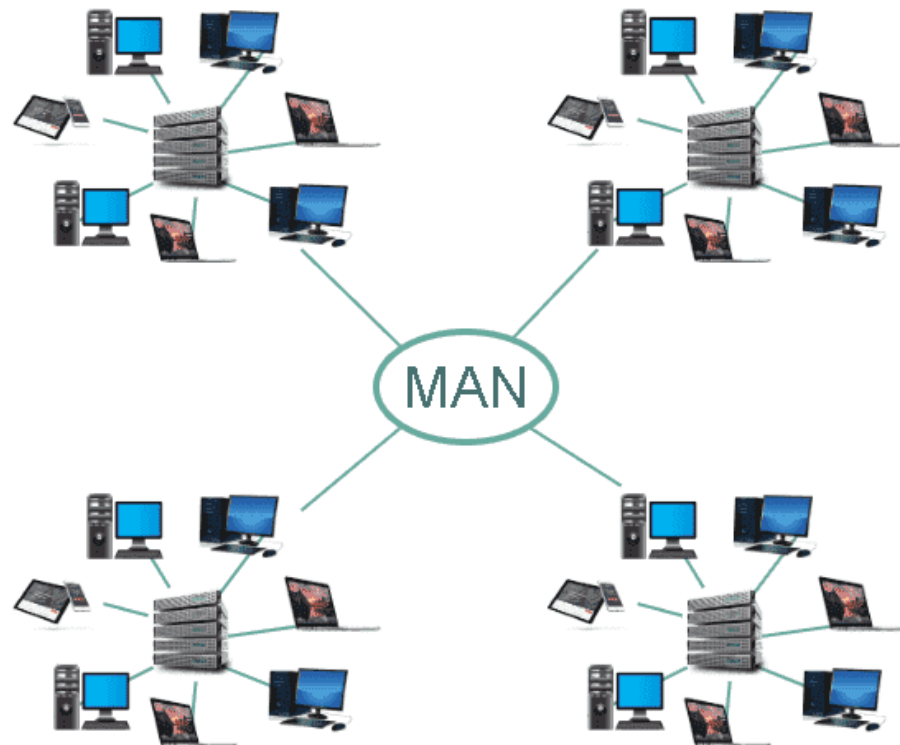
# Preparação dos Dados

- 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?
  - Switches/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
<u>192.168.0.200</u>	<u>e0-69-95-4f-5a-81</u>	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

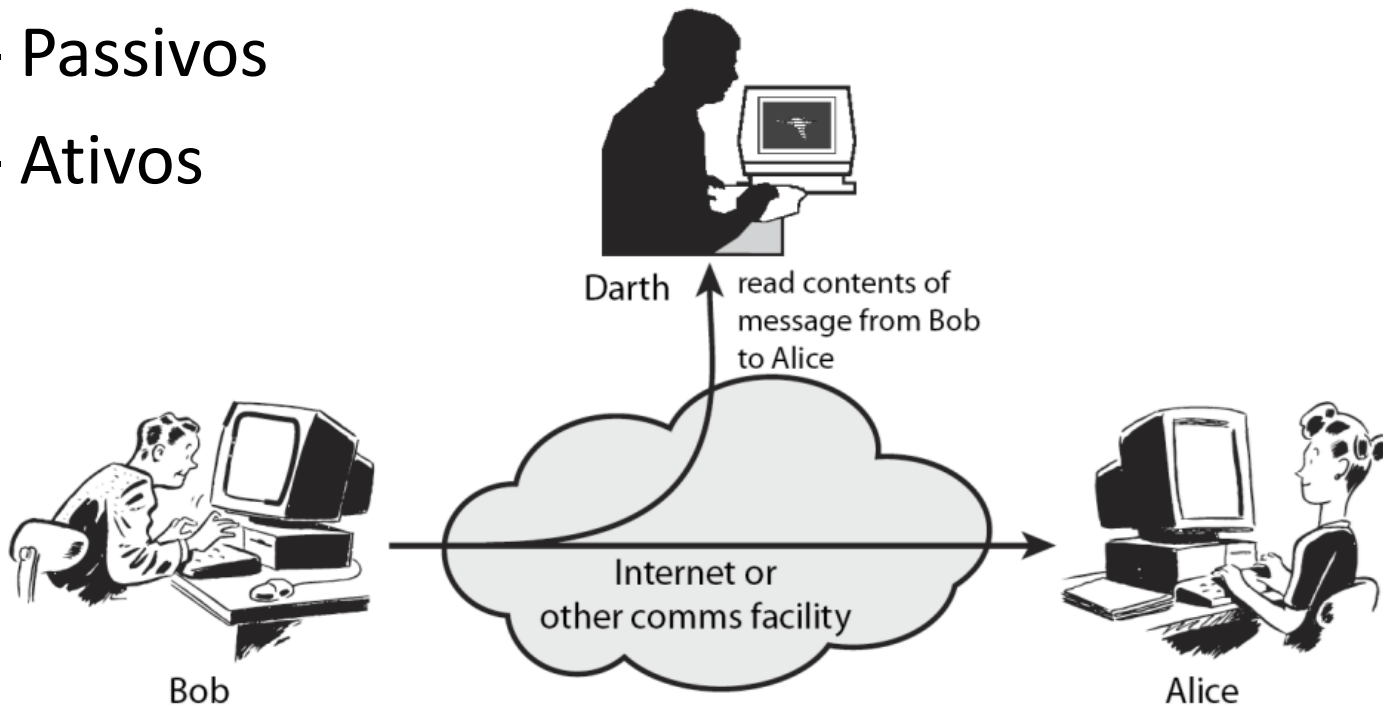
Serviço	Porta Normal	Porta Segura
FTP	21	22
SSH		22
Telnet	23	
SMTP	25	465 / 587
DNS	53	
HTTP	80	443
POP3	110	995
IMAP	143	993
IRC	6667	
MySQL	3306	
MSSQL	1039	

# ANÁLISE DE TRÁFEGO



# Sniffers

- O que são?
- Há dois tipos
  - Passivos
  - Ativos



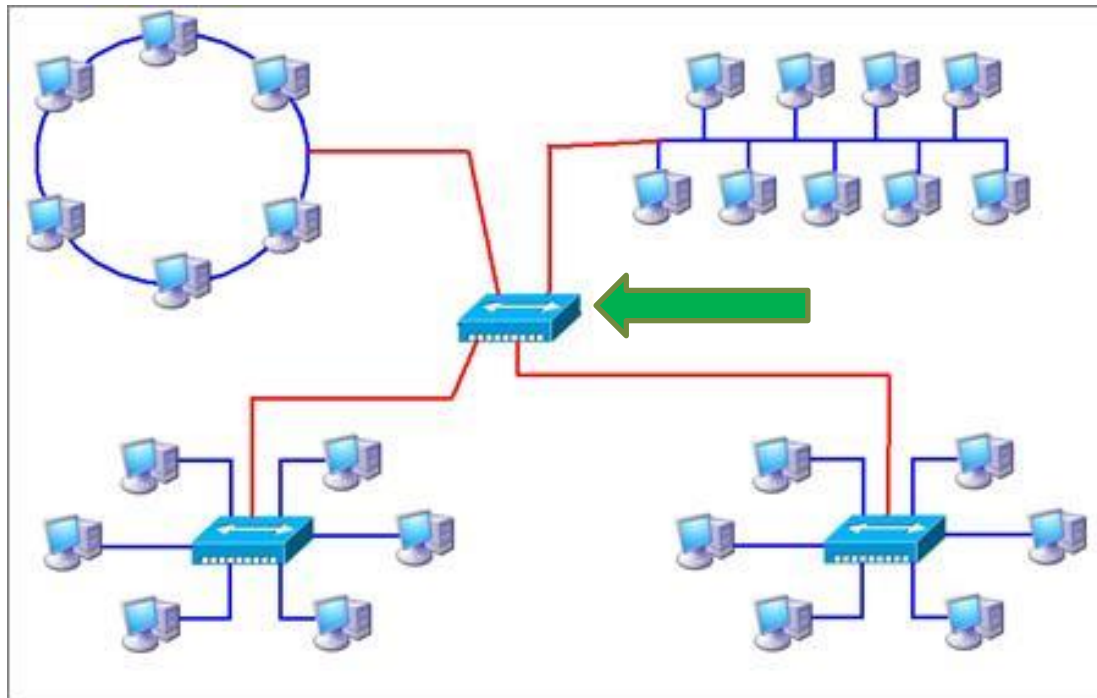
# Sniffers

- Para quê servem?
  - Uso legal: identificar problemas na rede
    - Problemas de comunicação (não conecta)
    - Problemas de sobrecarga (lentidão)
    - ...
  - Uso “discutível”: vasculhar pacotes
    - Necessário autorização
    - Sem autorização: como escuta telefônica.



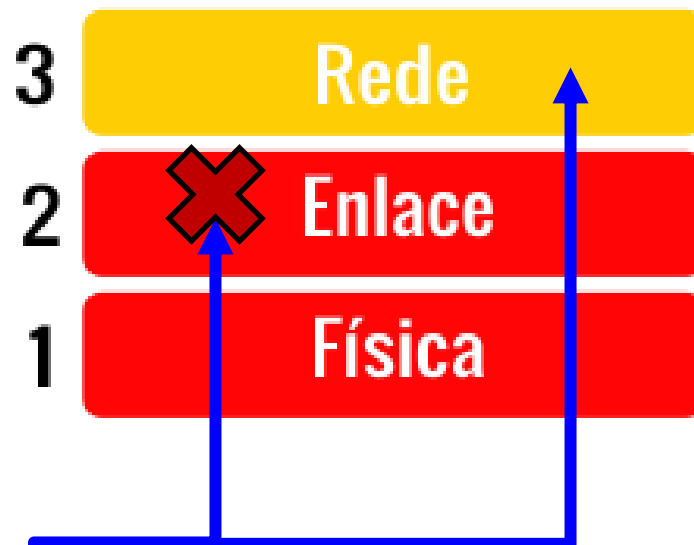
# Sniffers

- 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





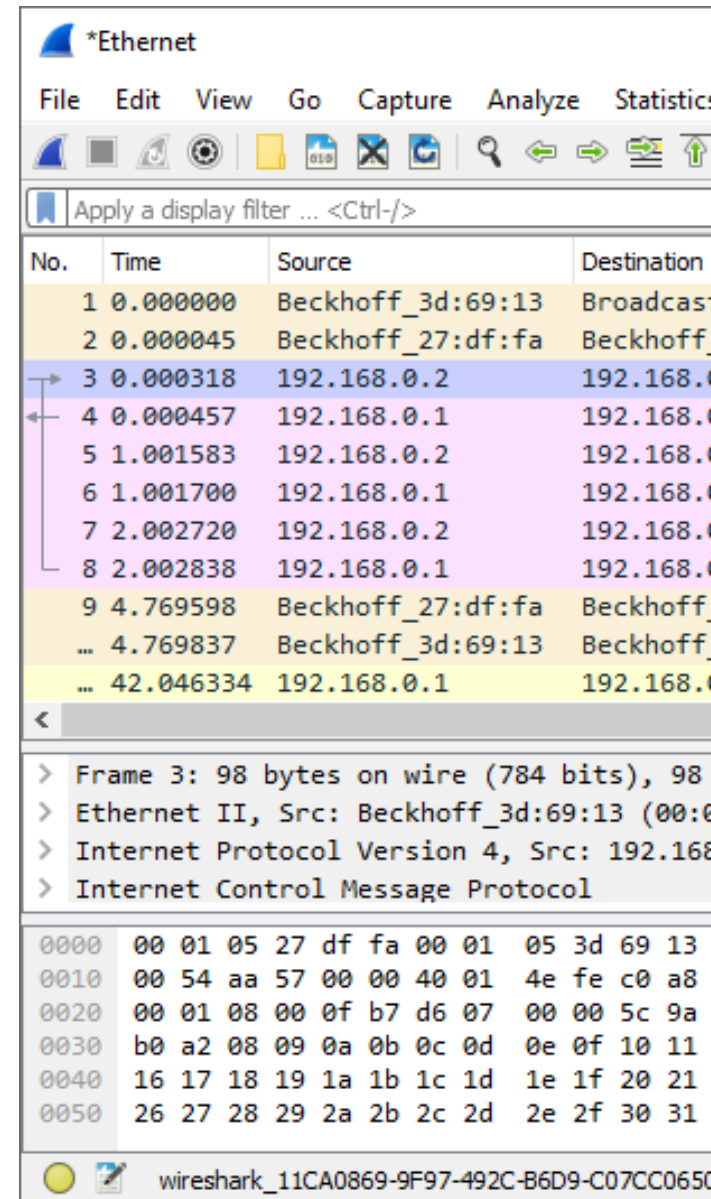
# Sniffers

- 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



\*Ethernet

File Edit View Go Capture Analyze Statistics

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination
1	0.000000	Beckhoff_3d:69:13	Broadcas
2	0.000045	Beckhoff_27:df:fa	Beckhoff
3	0.000318	192.168.0.2	192.168.0.1
4	0.000457	192.168.0.1	192.168.0.2
5	1.001583	192.168.0.2	192.168.0.1
6	1.001700	192.168.0.1	192.168.0.2
7	2.002720	192.168.0.2	192.168.0.1
8	2.002838	192.168.0.1	192.168.0.2
9	4.769598	Beckhoff_27:df:fa	Beckhoff
...	4.769837	Beckhoff_3d:69:13	Beckhoff
...	42.046334	192.168.0.1	192.168.0.2

<

> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
> Ethernet II, Src: Beckhoff\_3d:69:13 (00:0c:27:df:fa), Dst: 192.168.0.1 (08:00:27:00:00:01)  
> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1  
> Internet Control Message Protocol

```
0000  00 01 05 27 df fa 00 01 05 3d 69 13
0010  00 54 aa 57 00 00 40 01 4e fe c0 a8
0020  00 01 08 00 0f b7 d6 07 00 00 5c 9a
0030  b0 a2 08 09 0a 0b 0c 0d 0e 0f 10 11
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
```

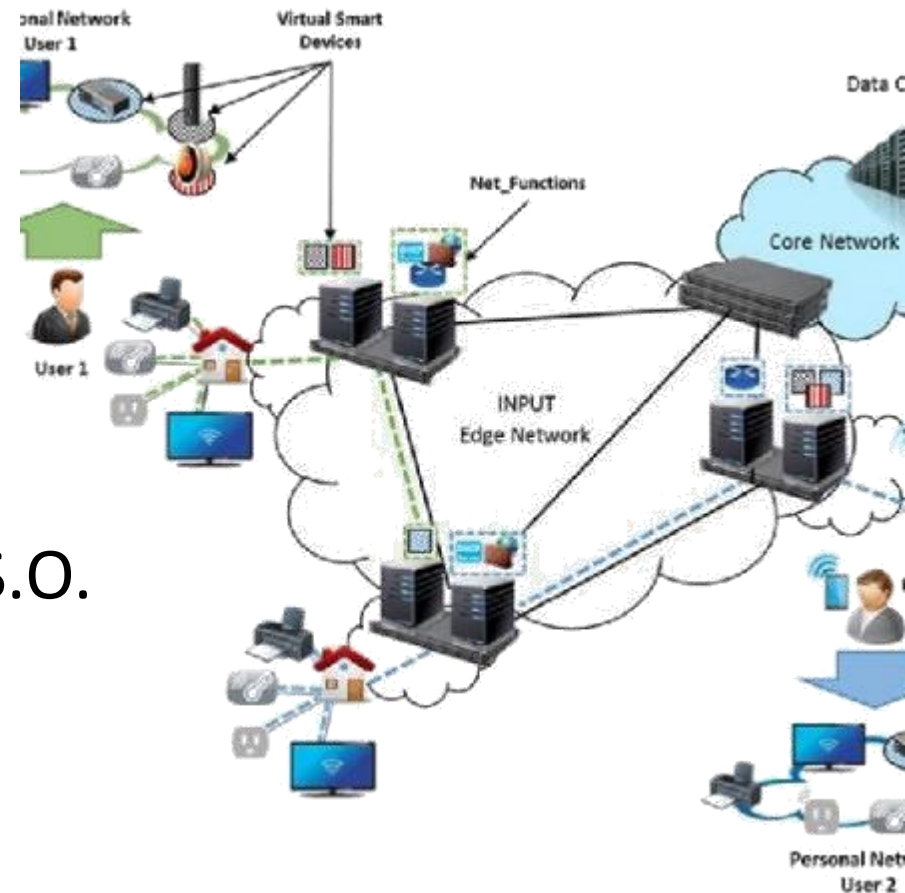
wireshark\_11CA0869-9F97-492C-B6D9-C07CC0650

# 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.O.
  - ...



# 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.



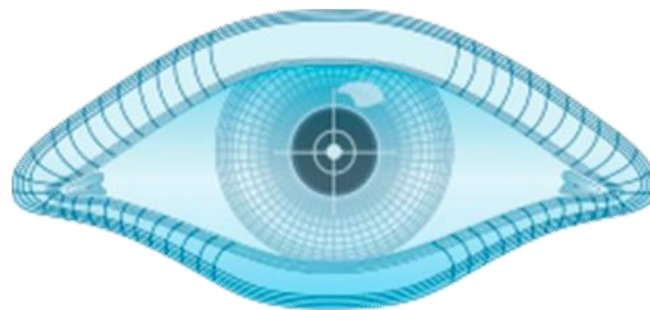
# Mapeamento de Rede

- 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](http://scanme.nmap.org)



# Mapeamento de Rede

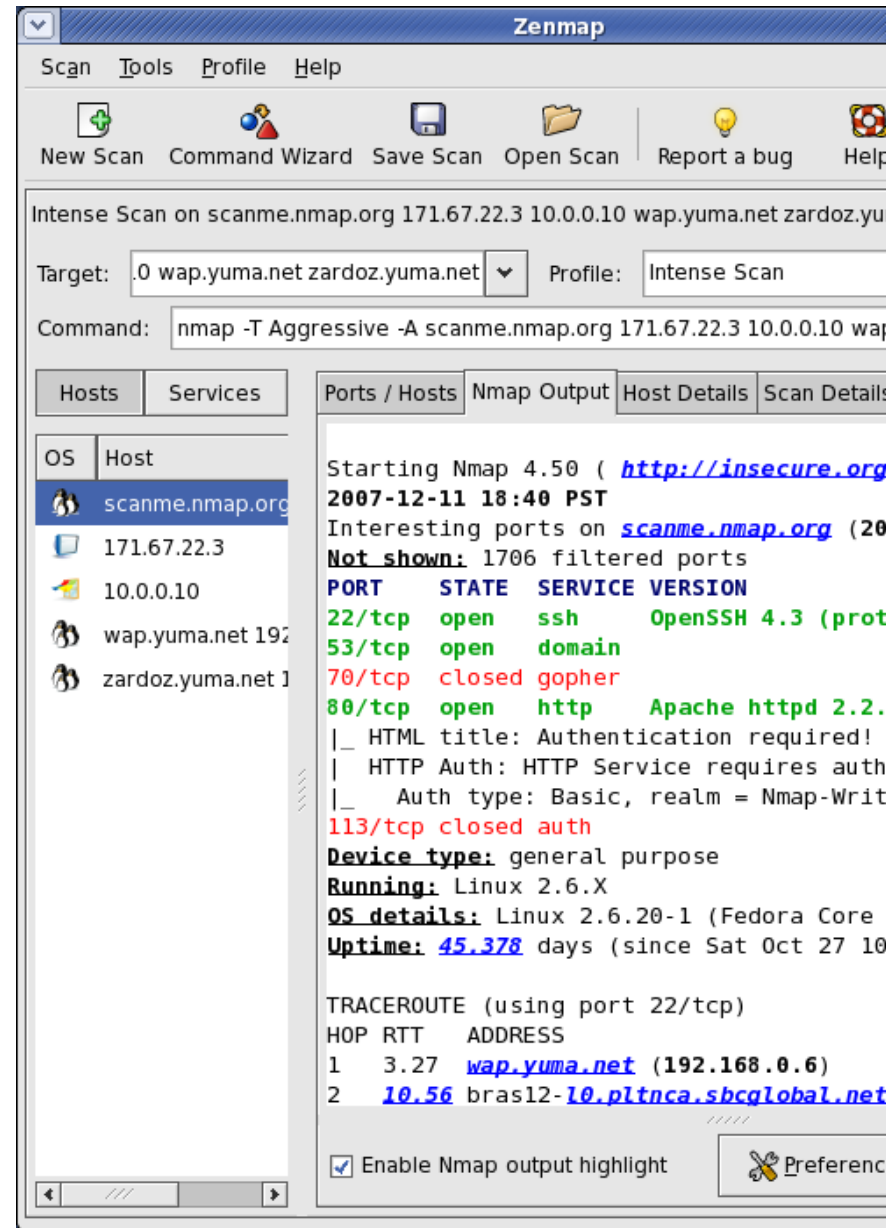
- Aplicação mais comum: NMap
  - Usa primariamente as camadas de rede e transp.
    - IP e TCP
  - Também usa dados da camada enlace
  - Parte-se de...
    - Um IP acessível ou uma faixa de IPs acessíveis



**NMAP**

# Mapeamento de Rede

- Conhecendo o NMap
  - Scan simples
  - Scan de range
  - Scan intenso
  - 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: Aprenda Mais, Pós Aula e Desafio!**
    - No padlet: <https://padlet.com/djcaetano/segciber>
- 
- Códigos maliciosos e a internet
    - A Engenharia Social na rede



# PERGUNTAS?