



SEGURANÇA CIBERNÉTICA

PRINCÍPIOS DE SEGURANÇA CIBERNÉTICA II

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** Lidamos com equipamentos e infraestrutura complexa. Conhecê-la é nossa obrigação.



**Você sabe identificar
suas vulnerabilidades?**

Compreendendo o problema

- **Situação:** A informação está armazenada nos “storages”, equipamentos que buscamos proteger.



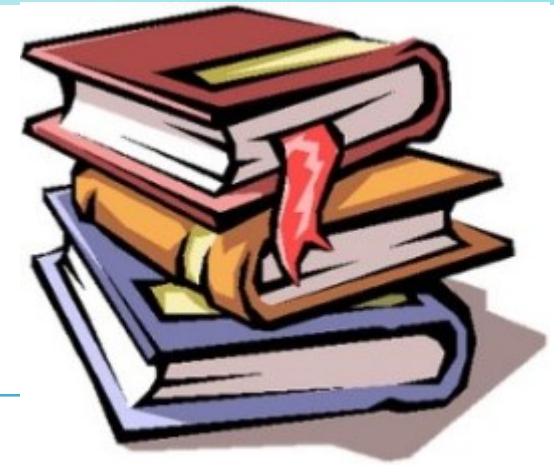
**Mas como chegam onde
são necessárias?**

Objetivos

- Compreender a importância e a manutenção de um plano de segurança
- Tomar contato com o procedimento de priorização por riscos
- Conhecer o processo de identificação de vulnerabilidades conhecidas
- Tomar contato básico com o funcionamento do tráfego de rede



Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2022a/ara0076.php (Segurança Cibernética – Aula 03)
Minha Biblioteca	<ul style="list-style-type: none">• Redes de computadores: uma abordagem top-down (978-85-8055-169-3), págs 34 a 42.• Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 10 a 19;
Material Adicional	<ol style="list-style-type: none">1) Política de Segurança da Informação em 5 passos - Disponível em: https://youtu.be/nI1ow4nKdc2) Cybersecurity Projects: Find a Project and Create a plan – Disponível em: https://youtu.be/kGt9hHoybFg3) Cyber Academy: Project Ideas. Disponível em: https://cybercademy.org/project-ideas/



AMEAÇAS À SEGURANÇA DAS INFORMAÇÕES



Ameaças à Segurança

- Potencial de violação à segurança
 - Circunstância, ação ou evento
 - quebra da segurança



Ameaças à Segurança

- Ameaça Organizacional
 - Situações externas
 - Tempo presente ou futuro
 - Podem afetar a empresa negativamente.



Eliminar, minimizar ou evitar

Ameaças x Vulnerabilidades

- Ameaças sozinhas não produzem efeito
 - Precisam explorar vulnerabilidades
- A proteção também pode vir...
 - Mitigando ou eliminando 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





PLANEJANDO A DEFESA

Instrumentos de Planejamento

- Política de Segurança da Informação (PSI)
 - Regulatória x Informativa x Consultiva
 - Procedimentos e obrigações
 - Quem pode/deve o quê



Instrumentos de Planejamento

- Fontes para uma PSI (ABNT)
 - Princípios, objetivos e necessidades da organização
 - Legislação vigente (Marco Civil e LGPD, p. exemplo)
 - Avaliação de riscos
 - Identificar ameaças e vulnerabilidades



Política x Plano de Segurança



- Política de Segurança da Informação
 - *Information Security Policy*
 - Planejamento/gerenciamento de segurança
 - Preocupação ampla com segurança
 - Física, lógica, contingência etc.
- Segurança de TI (ou *Cybersecurity Plan*)
 - Parte da PSI que trata de:
 - Monitoramento de login
 - Proteção dos servidores (uso de recursos e dados)
 - Proteção do tráfego de dados (criptografia)
 - Gerenciamento de servidores (remoto)
 - Realização de backups



PREMISSAS BÁSICAS:

DEFININDO E PRIORIZANDO AÇÕES DE SEGURANÇA

Ameaça, vulnerabilidade e desastre

- Conceitos via exemplos
 - Ameaças
 - Existência de potenciais invasores com interesse nas informações que mantemos
 - Funcionários insatisfeitos com acesso ao banco de dados
 - Vulnerabilidades
 - Uma versão antiga de *webserver* com falha conhecida
 - Código PHP mal elaborado que permita *injection*
 - Desastres
 - Furto de informações confidenciais do banco de dados
 - Deleção do banco de dados como um todo

Terminologia

- Ameaça

- Circunstância, ação ou evento que pode levar à quebra de segurança



- Vulnerabilidade

- Fragilidade nos ativos que os expõem a ameaças



- Incidente ou ataque

- Uma tentativa ou sucesso de uma ameaça em explorar uma vulnerabilidade

- Desastre

- Resultado do sucesso de um ataque



- E risco?

O que é Risco?

- Risco é uma **probabilidade**
 - Ameaças e vulnerabilidades..
 - Levarem a desastres
- Em geral, define-se risco como:
risco = ameaças . vulnerabilidades
- Em outras palavras...
 - Se não houvesse ameaças ou vulnerabilidades...
 - ... Não haveria riscos.
- Em segurança da informação...
 - O risco considera a **magnitude** do desastre



Determinação do Risco

- Avaliar:
 - A possibilidade de exploração da vulnerabilidade
 - O impacto ao negócio devido a evento adverso
 - Efetividade de controles para reduzir os riscos.
- Tabela conforme ABNT (notas 0 a 8)

	PROBABI- LIDADE DO CENÁRIO DE INCIDENTE	MUITO BAIXA (MUITO IMPROVÁVEL)	BAIXA (IMPROVÁVEL)	MÉDIA (POSSÍVEL)	ALTA (PROVÁVEL)	MUITO ALTA (FREQUENTE)
IMPACTO NO NEGÓCIO	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Inevitabilidade dos Riscos

- Riscos são inevitáveis
 - Investidores comprando ações
 - Cirurgiões realizando operações
 - Engenheiros projetando pontes
 - Empresários abrindo negócios
 - Etc...
- Mas gerenciá-los é estratégico!
 - Já que não temos como eliminá-los totalmente...
 - Precisamos lidar com eles!



Avaliação de Riscos

- Passos para a avaliação
 - Caracterização do ambiente e sistemas
 - Identificação das ameaças
 - Identificação das vulnerabilidades
 - Análise de controles d
 - Determinação da prob
 - Análise de impacto
 - Determinação do riscc
 - Recomendação dos co
 - Documentação dos re



Caracterizar o Ambiente

- Rede?
 - Interna x Externa
- Sistemas
 - Locais x Externos (“nuvem”)
- Dados
 - Locais x Externos (“nuvem”)





VISÃO GERAL: VULNERABILIDADES COMUNS



Vulnerabilidades Comuns

- Common Vulnerability & Exposure
 - CVEs
 - Mitre Corporation: <https://cve.mitre.org/>

The screenshot shows the CVE website homepage. At the top, there is a navigation bar with the CVE logo and links for CVE List, CNAs, WGs (News & Blog), Board, and About. On the right, there is a link for NVD (Go to for: CVE Scores, CVE Info). Below the navigation bar is a search bar and a menu with options: Search CVE List, Downloads, Data Feeds, Update a CVE Record, and Request CVE IDs. A prominent notice states: "TOTAL CVE Records: 171029" and "NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)". Another notice mentions "Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022". The main content area features three columns: "CVE News" (with a link to the new website), "Become a CNA" (with a world map and a link to the new website), and "Newest CVE Records" (displaying tweets from @CVEnew, including one about CVE-2022-0841 OS Command Injection).

Vulnerabilidades Comuns

- Common Vulnerability & Exposure
 - Outras interfaces de visualização
 - <https://www.cvedetails.com/>

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search [] View CVE []

Log In Register Vulnerability Feeds & Widgets New www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CVE Definitions
About & Contact
Feedback
CVE Help
FAQ

Enter a CVE id, product, vendor, vulnerability type... Search

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	758	0.40
1-2	1150	0.70
2-3	7848	4.60
3-4	8507	5.00
4-5	40585	23.70
5-6	32578	19.00
6-7	25406	14.80
7-8	34278	20.00
8-9	841	0.50
9-10	19279	11.30
Total	171230	

Weighted Average CVSS Score: 6.5

Vulnerability Distribution By CVSS Scores

CVSS Score Ranges

- 0-1
- 1-2
- 2-3
- 3-4
- 4-5
- 5-6
- 6-7
- 7-8
- 8-9
- 9-10

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <http://www.itsecdb.com> allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.
Sample CVE entry with OVAL definitions : [CVE-2007-0994](https://www.cvedetails.com/cve/2007/0994/)

Vulnerabilidades Comuns

- Desenvolvedores mantêm registro
 - RedHat:
<https://access.redhat.com/security/vulnerabilities>
 - Apache:
<https://httpd.apache.org/security/vulnerabilities24.html>
 - Microsoft: <https://msrc.microsoft.com/update-guide/vulnerability>
 - Etc...



**PARÊNTESES ESTRATÉGICO:
O TRÁFEGO NAS
REDES E INTERNET**

Contexto do tráfego de rede

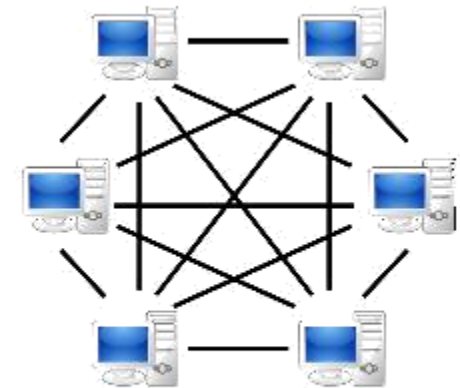
- Comunicação entre máquinas e serviços

- Paradigmas:

- Cliente-Servidor
 - Peer 2 Peer
 - Misto.



Server-based



P2P-network

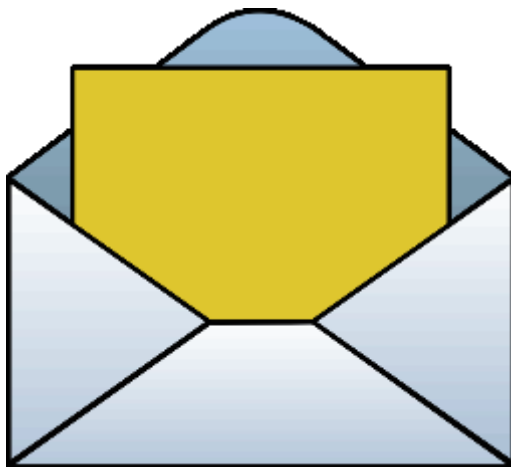
- Comunicação usual

- Sockets
 - Protocolos: UDP/TCP

- Funcionamento e origens...

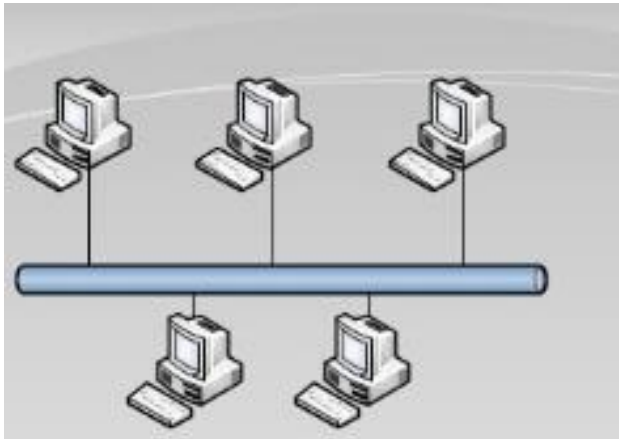
- Explicam muitas das limitações

Como funciona o correio?



Origens

- Redes locais x Inter-net



Rede Local: vila

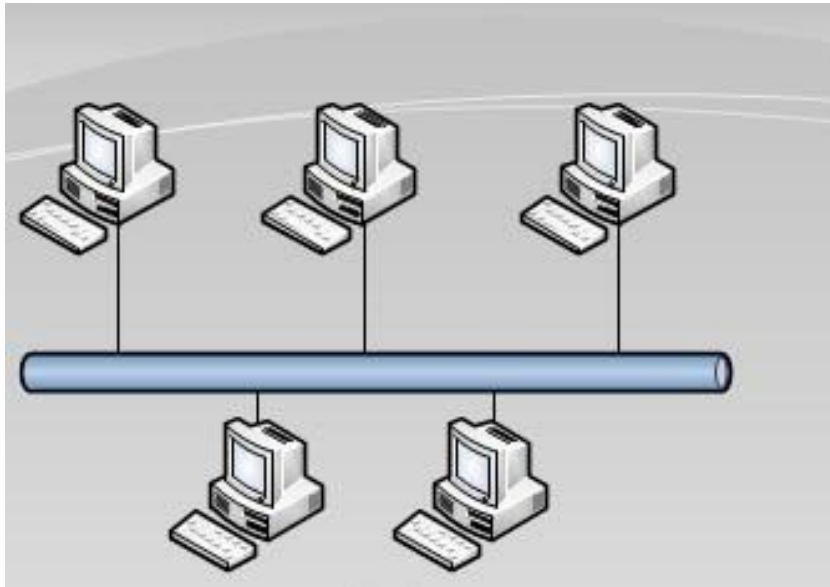


Internet: cidade

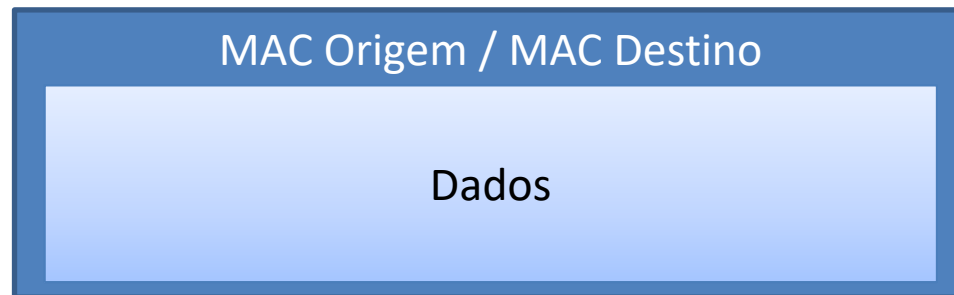
- Diferença importante:
 - Organização do tráfego de dados

Rede Local: Comunicação Direta

- Pacote com dado em contexto local

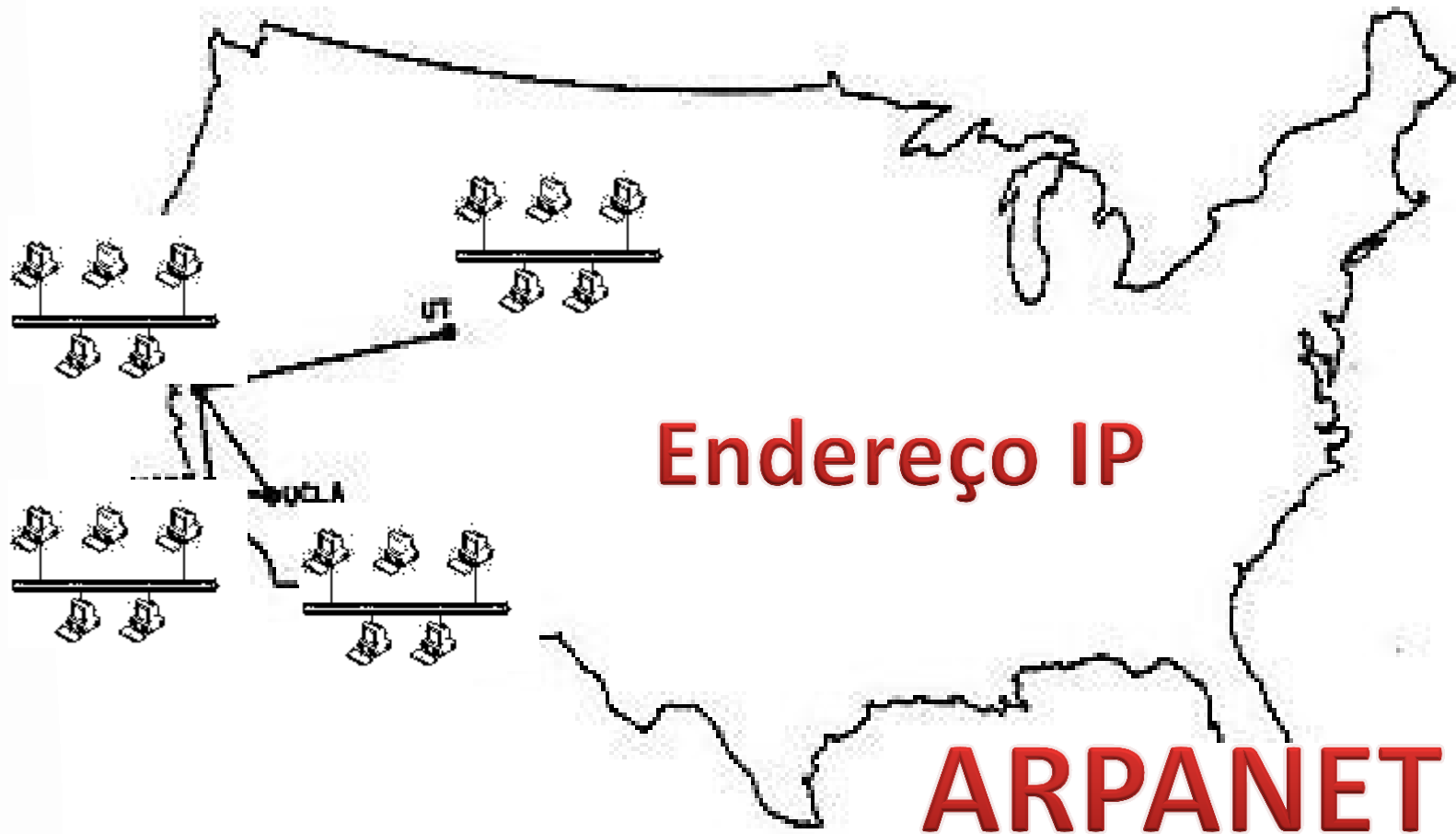


Endereço MAC



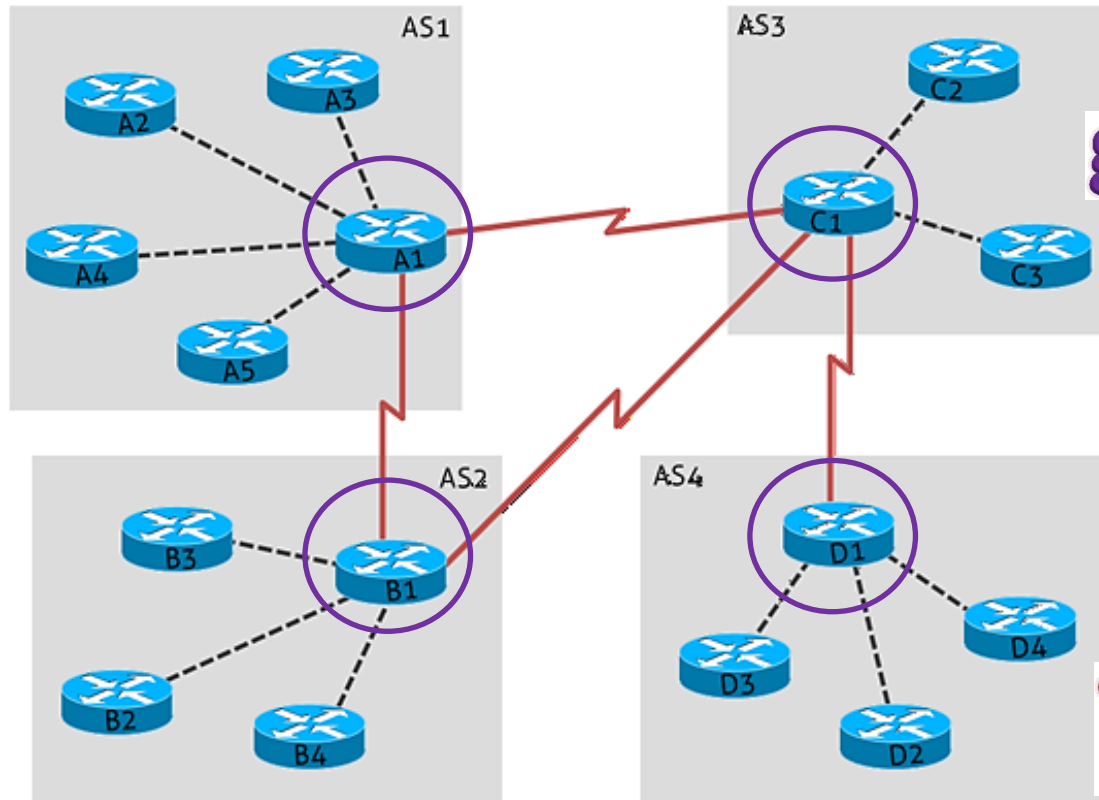
Rede: vila
MAC: nome da
pessoa

Internet: interligando redes



Internet: Comunicação Hierárquica

Rede: cidade
MAC: nome
IP: endereço

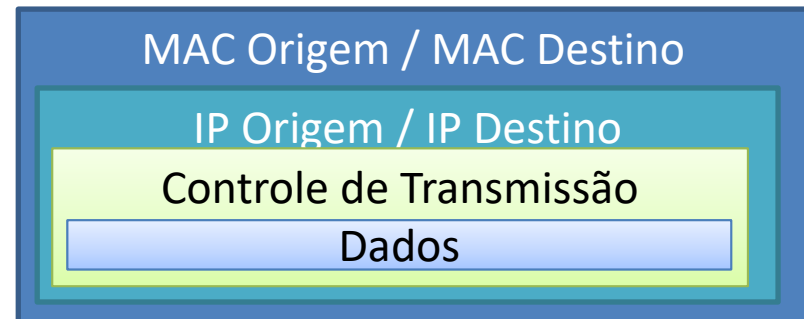
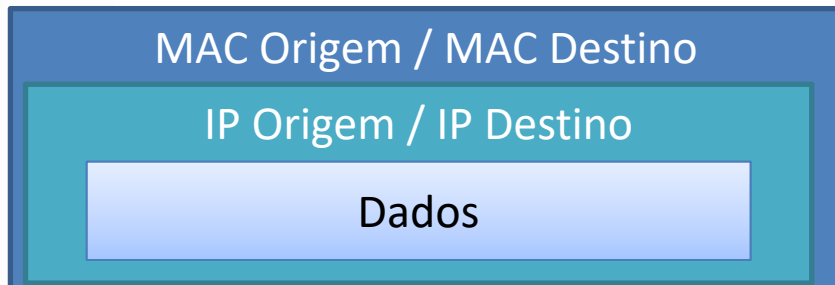


gateways

arp -a

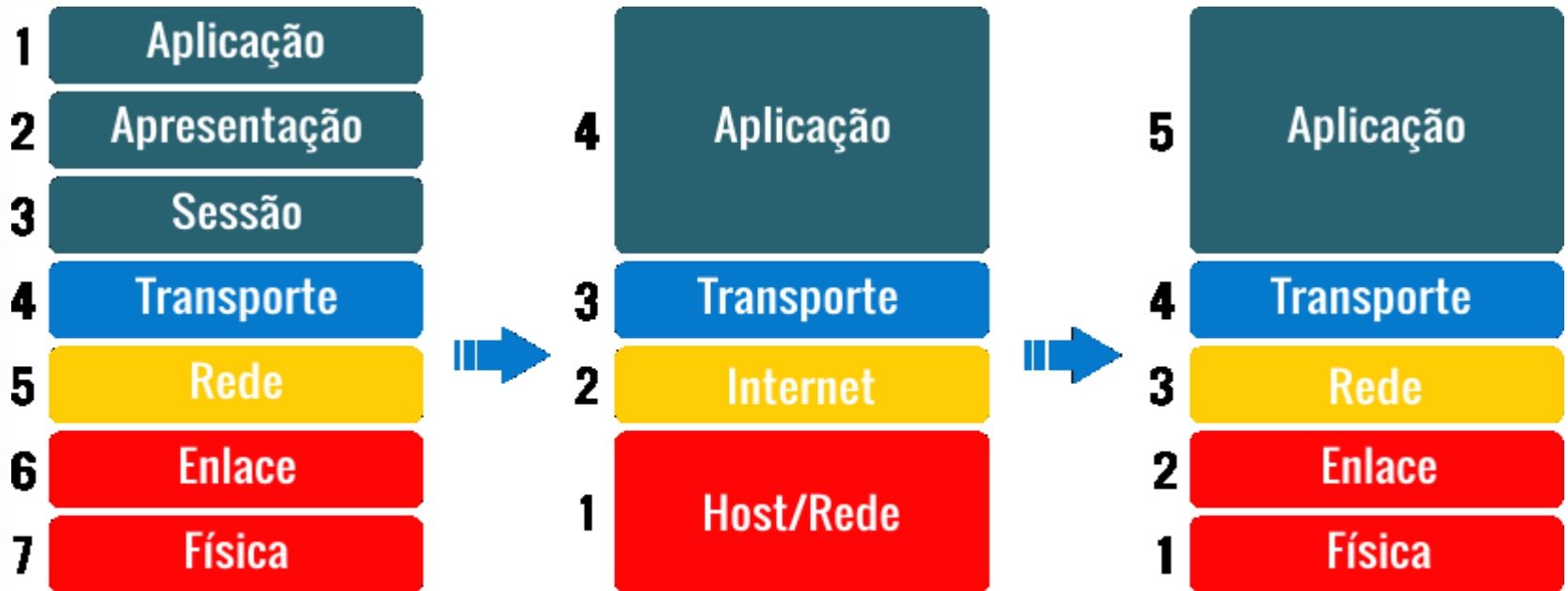
IP

TCP/IP



Protocolos

- Comunicação padronizada



Modelo de Referência OSI

Modelo de Referência TCP/IP

Pilha de Protocolos da Internet



Protocolos: Caminho dos Dados

DNS

cod.activision.com

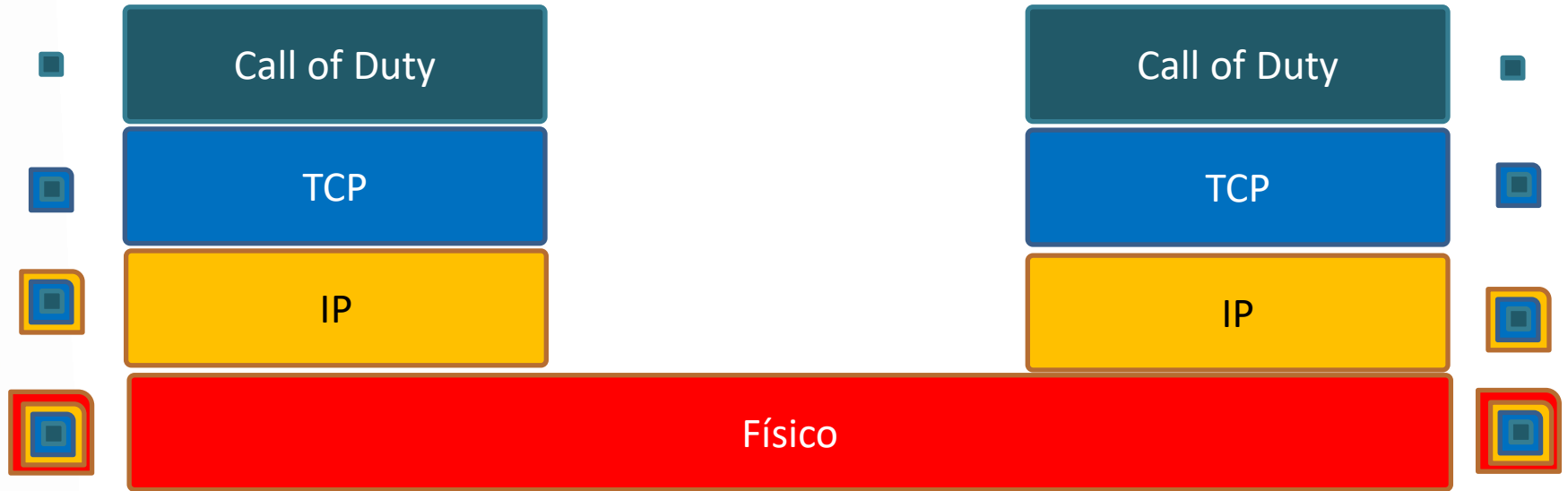
IP: 200.201.100.4

Domain Name System

IP: 64.111.160.175 ???

Cliente

Servidor



Caminhos Públicos, Dados Privados

- O mundo mudou muito nas últimas décadas
 - Documentos são digitais
 - Processos são digitais
 - Uso da “nuvem”
 - Dispositivos “sempre on
 - Todos os dispositivos sempre online...!

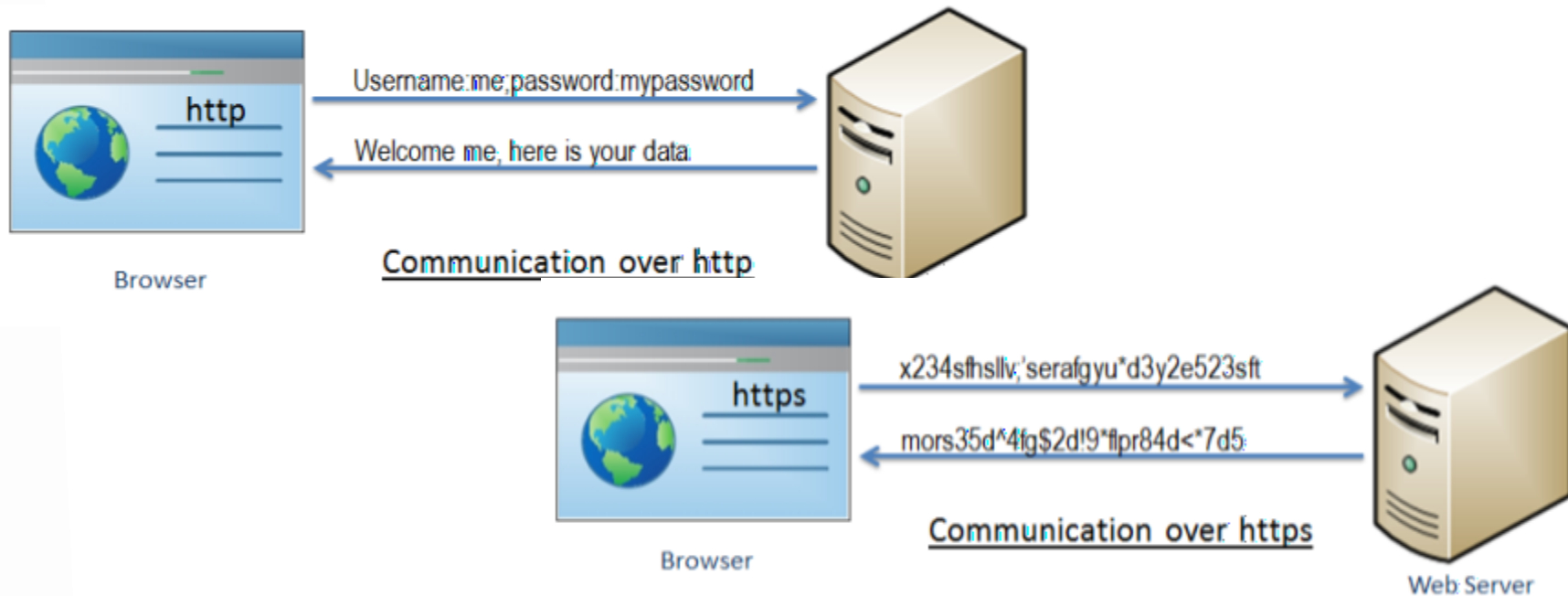


Maior Exposição!

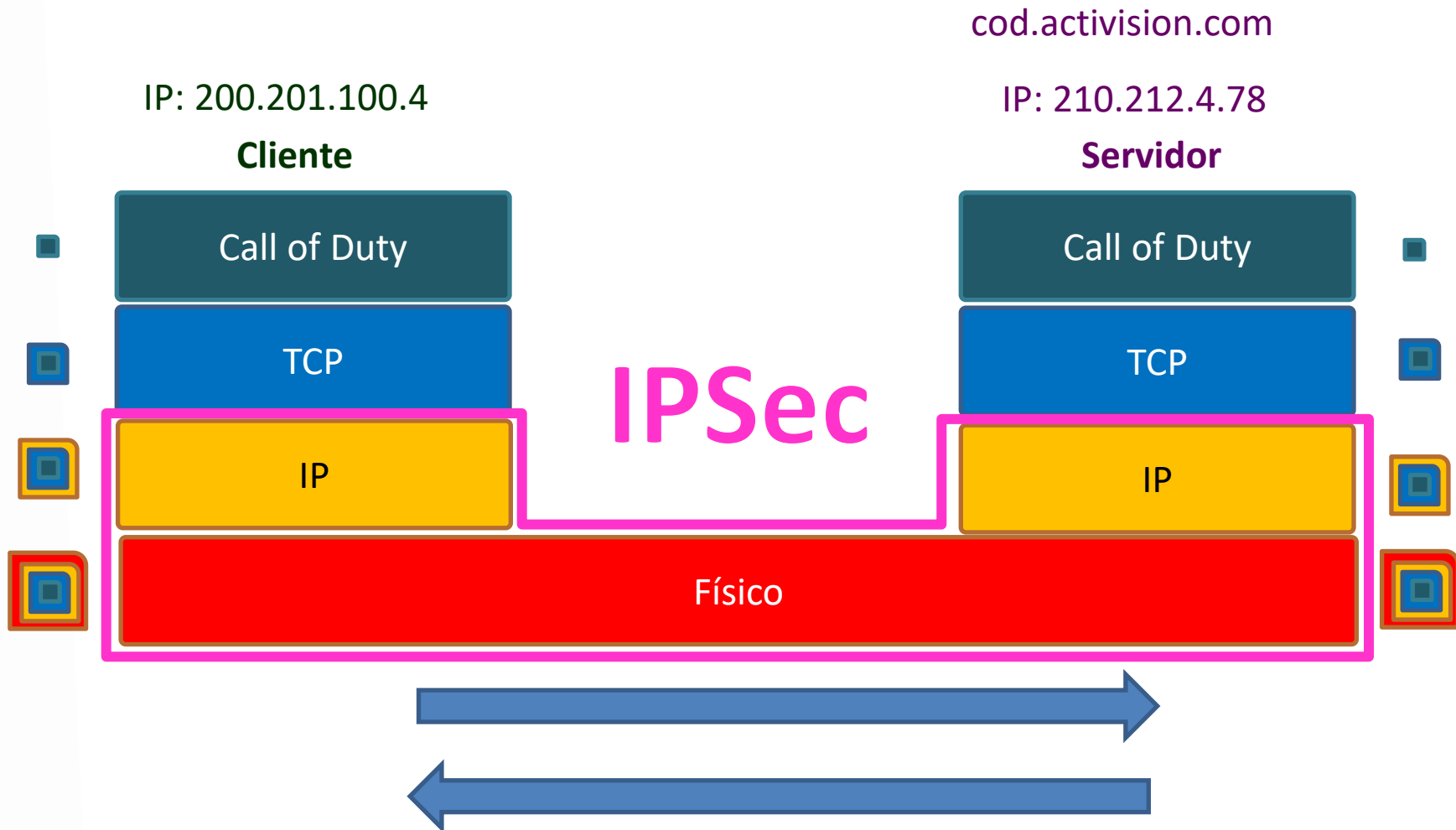
Comunicação SSL/TLS



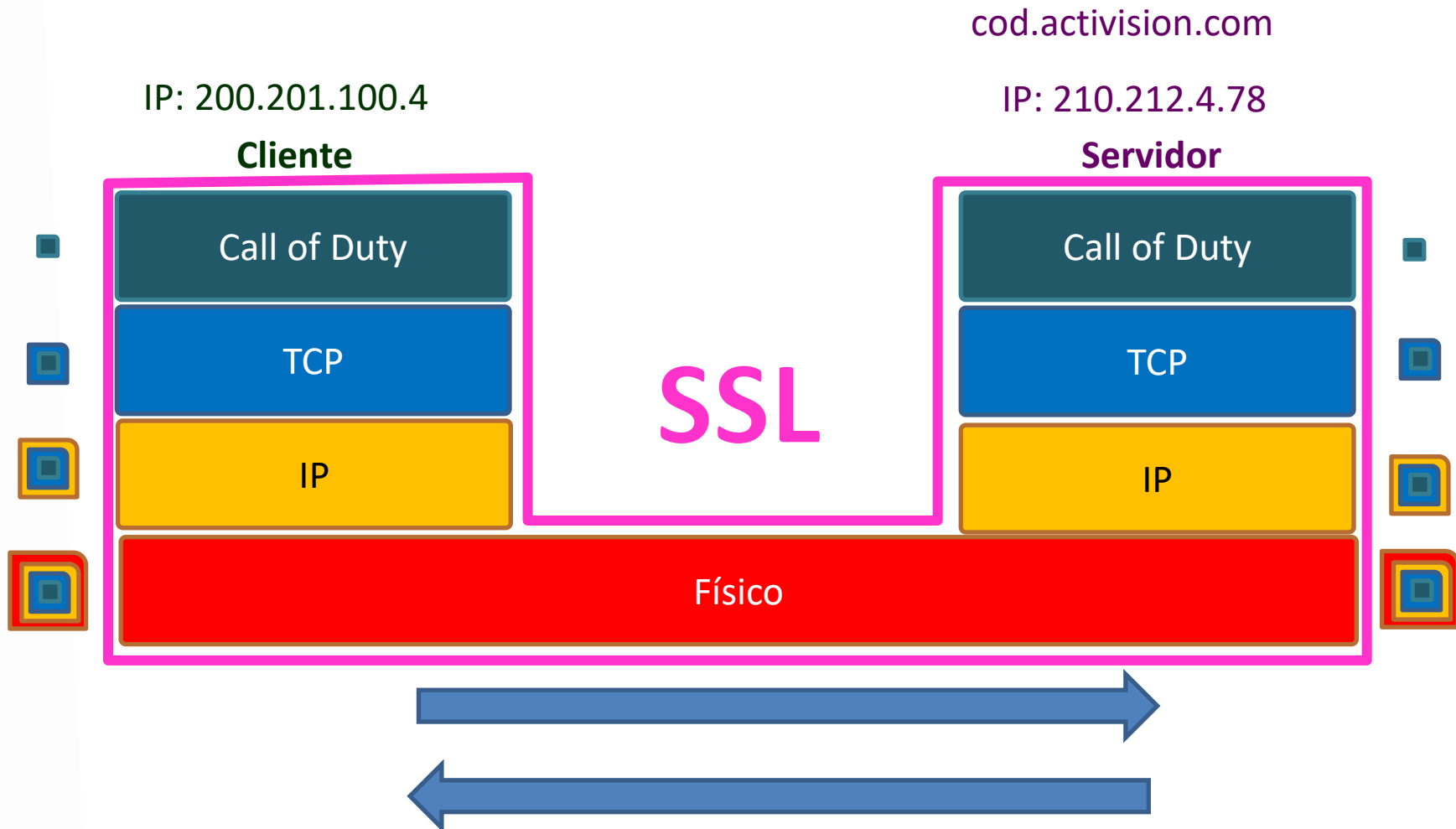
- Comunicação por meio do HTTPS
- HTTP + TLS (*Transport Layer Security*)
 - Criptografa as informações ponto-a-ponto
 - HTTPS, por si só, não significa segurança total



Atuação do IPSec e do SSL

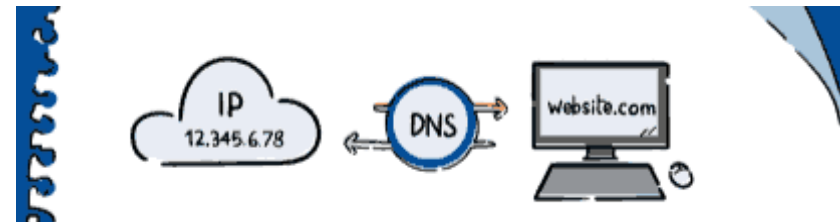


Atuação do IPSec e do SSL



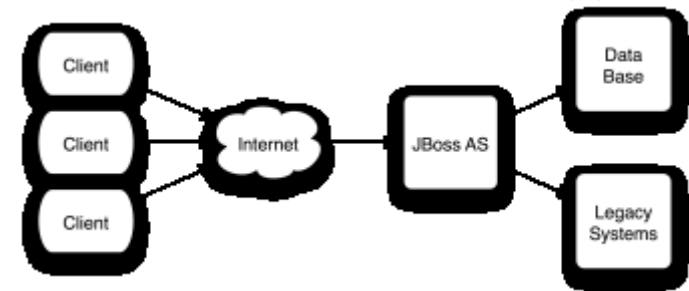
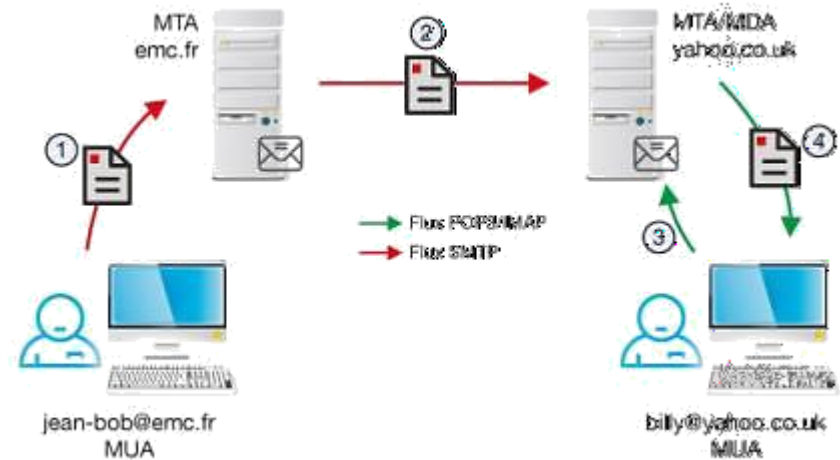
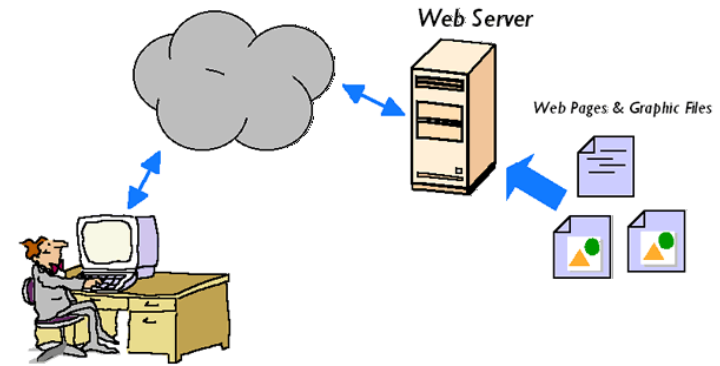
Serviços Básicos?

- Acesso remoto
 - SSH (Porta: 22)
 - Área de Trabalho Remota (Porta: 3389)
- Servidor de Nome de Domínio
 - DNS: 53
- Servidor de Arquivos
 - SMB: 445
 - Kerberos: 88
 - LDAP: 389.



Serviços Básicos?

- Servidor Web
 - Apache/Nginx/IIS: 80, 443
- Servidor de E-mail
 - PostFix/Sendmail
 - SMTP: 25, 465 e 587
 - POP3: 110, 995
 - IMAP: 143, 993
- Servidor de Aplicações
 - JBoss: 8080, 8443, etc.
 - Glassfish: 4848, 8080, 8181, etc.





ATIVIDADE

Atividade

- Discussão – Grupos – 15 minutos
- 1) Do conhecimento (trabalho ou pessoal), quais são os serviços de rede mais usados?
 - Elabore uma lista com 3 itens
- 2) Indique um software para cada um deles.
- 3) Encontre a descrição de alguma vulnerabilidade para algum deles.



ENCERRAMENTO

Resumo e Próximos Passos

- Noções básicas de plano de segurança
 - Noções de mapeamento de vulnerabilidades
 - Noções do funcionamento da rede

 - **Pós Aula:** Saiba Mais, A Seguir e Desafio!
 - No mural: <https://padlet.com/djcaetano/segciber>
-
- Noções básicas de tráfego de rede
 - Configuração básica de rede



PERGUNTAS?