Segurança na Rede

Estácio - II Semana de Informática - Out/05

Fábio Borges - LNCC

Conhecimentos Necessários

- Rede

Conhecimentos Necessários

- Rede
- Sistemas

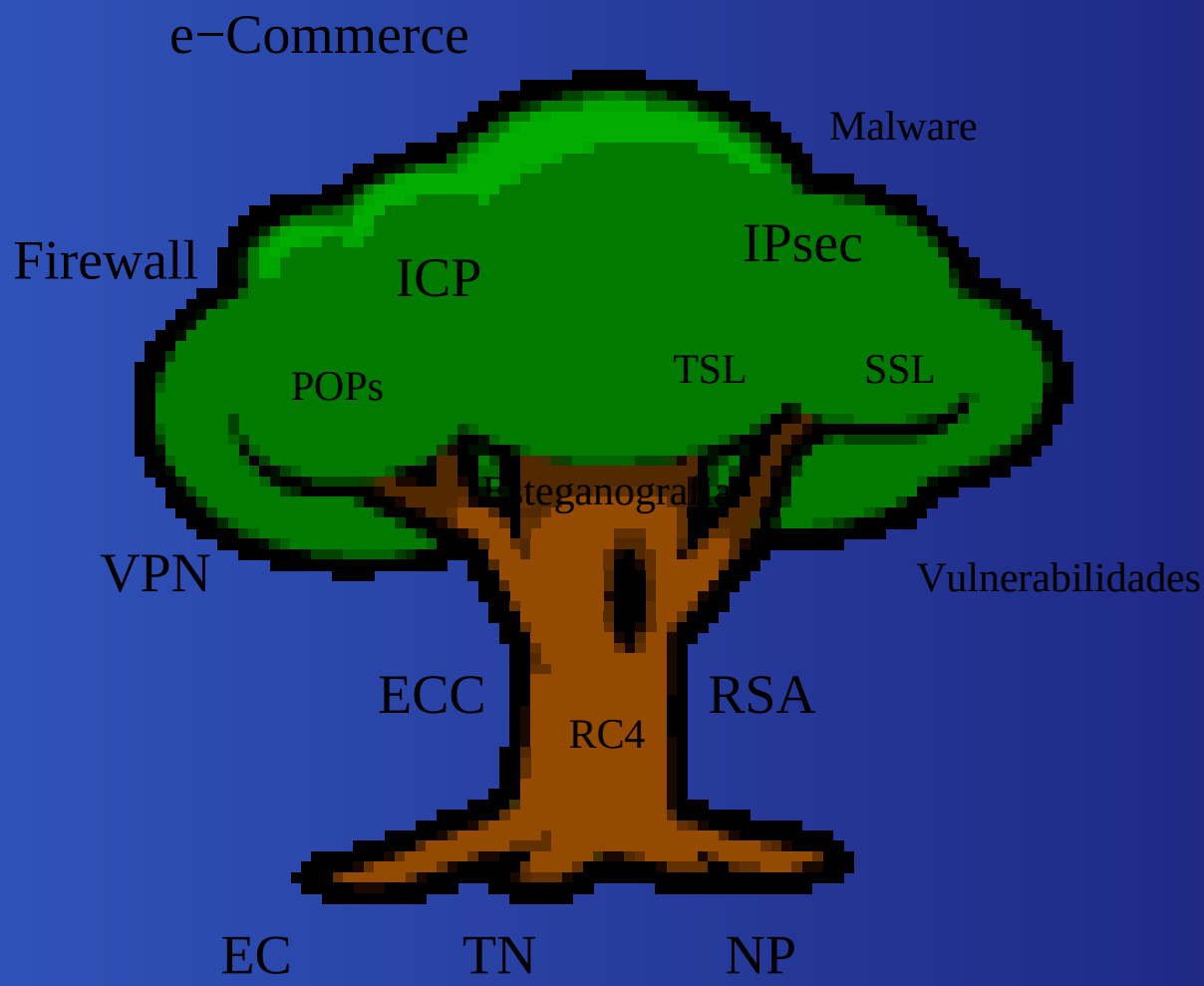
Conhecimentos Necessários

- Rede
- Sistemas
- Matemática

Conhecimentos Necessários

- Rede
- Sistemas
- Matemática
- Outros em casos específicos

Árvore da Segurança



Política de Segurança

- Política de uso aceitável

Política de Segurança

- Política de uso aceitável
- Apoio político

Política de Segurança

- Política de uso aceitável
- Apoio político
- Definição de responsabilidades

Política de Segurança

- Política de uso aceitável
- Apoio político
- Definição de responsabilidades
- Deve ser implementada em software

Ataques

- Força bruta

Ataques

- Força bruta
- Soft Attacks

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing
- Defacement

Ataques

- Força bruta
- Soft Attacks
- Criptoanálise
- DDoS (Distributed Denial of Service)
- Men-in-the-middle
- Malware
- Spoofing
- Defacement
- Phishing

Malware

- Keylogger

Malware

- Keylogger
- Root-kit

Malware

- Keylogger
- Root-kit
- Spyware

Malware

- Keylogger
- Root-kit
- Spyware
- Adware

Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus

Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms

Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)

Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)
- Backdoor (BackOrifice e NetBus)

Malware

- Keylogger
- Root-kit
- Spyware
- Adware
- Vírus
- Worms
- Bots (Botnets)
- Backdoor (BackOrifice e NetBus)
- Hoax

Eliminar Protocolos sem Criptografia

- 23 - Telnet

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec
- 6000 - X11 (com dados confidenciais)

Eliminar Protocolos sem Criptografia

- 23 - Telnet
- 20,21 - FTP
- 110 - POP3
- 143,220 IMAP
- 221,541 rlogin
- 222 - rsh
- 512 - rexec
- 6000 - X11 (com dados confidenciais)
- 80 - HTTP (com dados confidenciais)

Ferramentas

- nessus

Ferramentas

- nessus
- nmap

Ferramentas

- nessus
- nmap
- lsof

Ferramentas

- nessus
- nmap
- lsof
- ethereal

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute
- John the Ripper

Ferramentas

- nessus
- nmap
- lsof
- ethereal
- tcpdump
- top
- whois
- traceroute
- John the Ripper
- firefox

Sistema Operacional

Linux	58.6%
Windows	31.9%
FreeBSD	3.5%
desconhecido	2.7%
SolarisSunOS	1.7%
MacOSX	0.2%
AIX	0.2%
IRIX	0.2%
BSDOS	0.1%
outros	0.8%

Ataques por Domínio

.com	40.9%
.net	6.9%
.de	6.7%
.br	5.1%
.org	4.8%
.it	3.5%
.uk	3.1%
.nl	1.6%
.kr	1.6%
.ch	1.2%

Método do Ataque

Erros de administração	21.7%
Vulnerabilidades conhecidas	17.1%
Vulnerabilidades novas	14.7%
Inclusão de arquivo	9%
Força bruta	8.8%
Engenharia social	4.1%
Intrusão pelo FTP	3.8%
Senha roubada/sniffing	3.6%
Outras aplicações Web - bug	3.5%
Injeção de SQL	2.8%

Razões do Ataque

Apenas por diversão!	31.9
Eu quero ser o melhor pichador	18.4
Razões políticas	12.2
Sem razão especificada	11.2
Como um desafio	11.2
Patriotismo	10.9
Revanche contra o website	2.8
Indisponível	1.5

Segurança na Rede

- o comércio eletrônico é seguro?

Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?

Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?

Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?

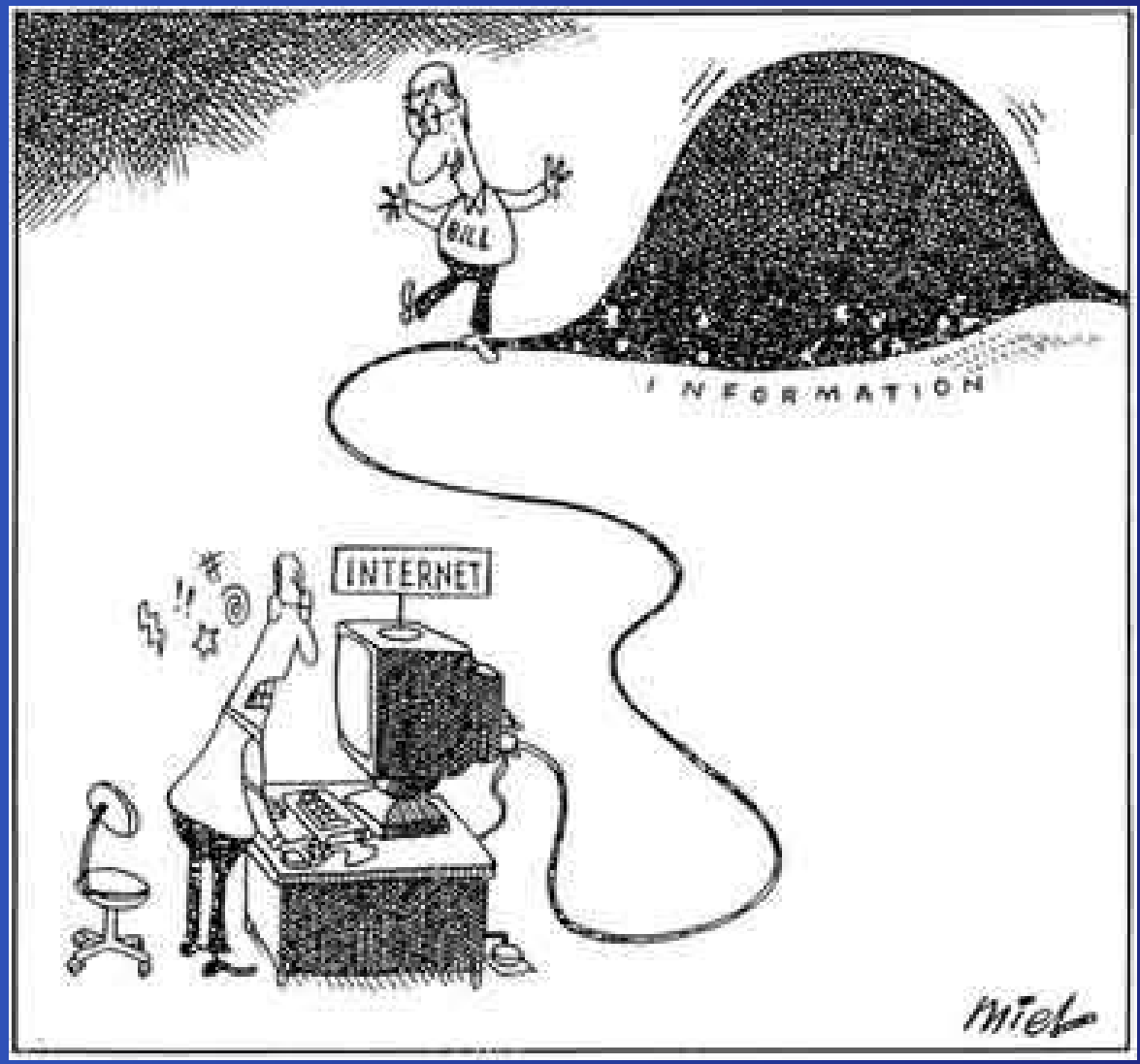
Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?
- onde está a segurança na rede?

Segurança na Rede

- o comércio eletrônico é seguro?
- você movimenta sua conta pela internet?
- os bancos não estão na internet?
- quem são os *hackers* e os *lammers* ?
- onde está a segurança na rede?
- onde está a insegurança na rede?

Ameaça



Proteção na Rede

- ACL - Roteador

Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)

Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall

Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS

Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS
- Honeypots e Honeynets

Proteção na Rede

- ACL - Roteador
- Rede Segmentada (DMZ)
- Firewall
- IDS/IPS
- Honeypots e Honeynets
- Log-analyzer

Proteção Local

- Antispam (Junk mail controls)

Proteção Local

- Antispam (Junk mail controls)
- Antivírus

Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy

Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal

Proteção Local

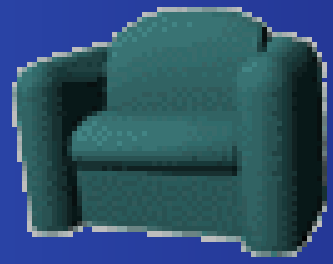
- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal
- Anti-popup

Proteção Local

- Antispam (Junk mail controls)
- Antivírus
- Antispy
- Firewall pessoal
- Anti-popup
- Block loading of remote image in mail

Check-in

Descansar?



Atualização

"Segurança não é um produto, mas um processo."

Último Slide

- Obrigado.
- Quaisquer sugestões serão bem-vindas.