

Adetti

Redes e Segurança
linha da Informação

Segurança de Redes e Sistemas

Seminário MGS/

Paulo Trezentos

(Paulo.Trezentos@adetti.iscte.pt)

ADETTI/ISCTE

ISCTE / 2 de Junho 2002



Adetti, Edifício ISCTE, Av. das Forças Armadas, 1600 Lisboa,

Tel.: 351 21 790 30 64 Fax: 351 21 793 53 00 Email: rsi@adetti.iscte.pt

Sumário

- **Arquitectura de rede**
- **Ameaças (internas e externas)**
- **Ferramentas e processos para enfrentar as ameaças**

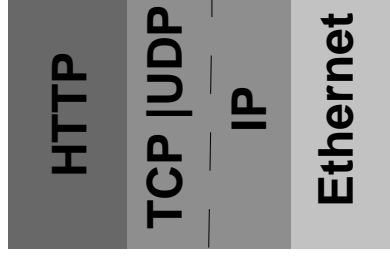
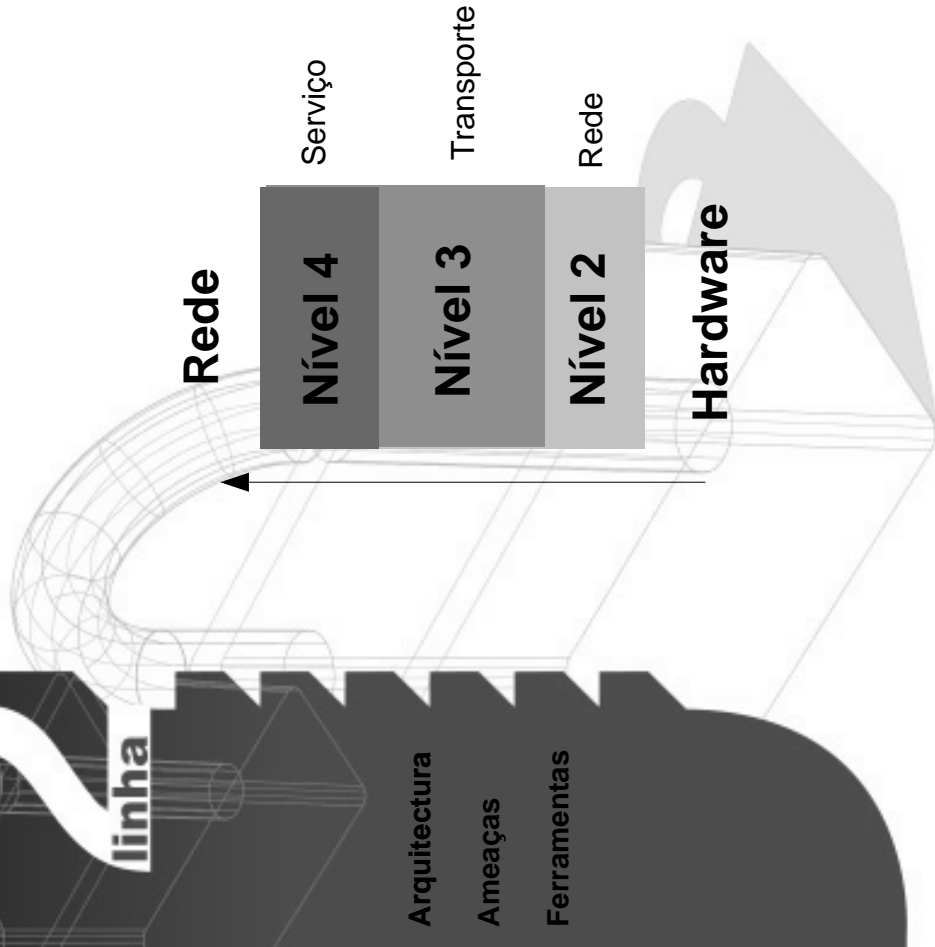
Arquitectura

Ameaças

Ferramentas



Recapitulação de alguns conceitos...



Elementos activos de networking

- Equipamentos electrónicos que asseguram o funcionamento da rede
 - Switch (nível 2)
 - Hub (nível 2)
 - Routers / gateway (nível 3)
 - Firewalls (nível 3 e 4)

Arquitectura

Ameaças

Ferramentas



2

linha

Elementos passivos rede

- Rede cablagem estruturada
- Racks
- Réguas
- Patch (chicote)

Arquitectura

Ameaças

Ferramentas



<http://www.adetti.pt>
+351 21 7903064 / +351 21 7935300

Segurança de redes e sistemas
(Paulo.Trezentos@adetti.iscte.pt)

2

linha

Arquitectura típica rede

- Composta por:
 - equipamento cliente
 - equipamento servidor
 - elementos activos rede
 - elementos passivos

Arquitectura

Ameaças

Ferramentas



Ameaças internas

- Objectivos:
 - acesso a informação para fins particulares
 - adulteração de informação (empresas financeiras)
 - espionagem industrial
 - sabotagem
- Meios:
 - cópias de dados (recorrendo a suportes físicos)
 - utilização indevida de login/password
 - sniffing / exploits locais / trojans

Arquitectura

Ameaças

Ferramentas



2

linha

Ameaças internas II

• Perfil

- Bom trabalhador
- Entra antes dos outros
- Sai depois dos outros
- Não goza férias

Arquitectura

Ameaças

Ferramentas

Fonte: Polícia Judiciária



2

linha

Arquitectura

Ameaças

Ferramentas

Ameaças Externas

• Objectivos:

- hacking 'académico'
- espionagem industrial
- sabotagem

• Meios/ técnicas:

- sniffing / exploits locais e remotos / trojans
- engenharia social



Ameaças Externas II

• Perfil:

- 90% estudantes ensino superior
- 40% pais separados
- introvertido; socialmente isolado
- notas escolares medianas
- tecnicamente competentes
- 15/20 anos
- 98% sem antecedentes criminais

Arquitectura

Ameaças

Ferramentas



Técnicas

• Exploits (locais e remotos)

- utilização de software que permite aceder a um sistema através da exploração de uma vulnerabilidade num serviço ou no próprio sistema (ex: FTP, IIS,...)
- má programação que potencia *buffer overflow*

• Sniffing

- rede: escuta de tráfego através da exploração dos *broadcast* de ethernet
- sistema: escuta de um sistema através da instalação de um serviço (*daemon*) local (BO, rootkit,...)

Técnicas II

• Cavalos de tróia (*trojans*)

- *programas que desempenham as mesmas funções que certos serviços de sistema (login, pop server,...)*
- *dissimuladamente tem um comportamento ilegítimo: esconder informação, gravar dados sensíveis, permitir acessos,...*

• *High-jacking*

- *simular que se é o interlocutor, através da apresentação de uma identificação(de rede) forjada*
- *a transacção passa a ser realizada com o interlocutor falso*

2

linha

Arquitectura

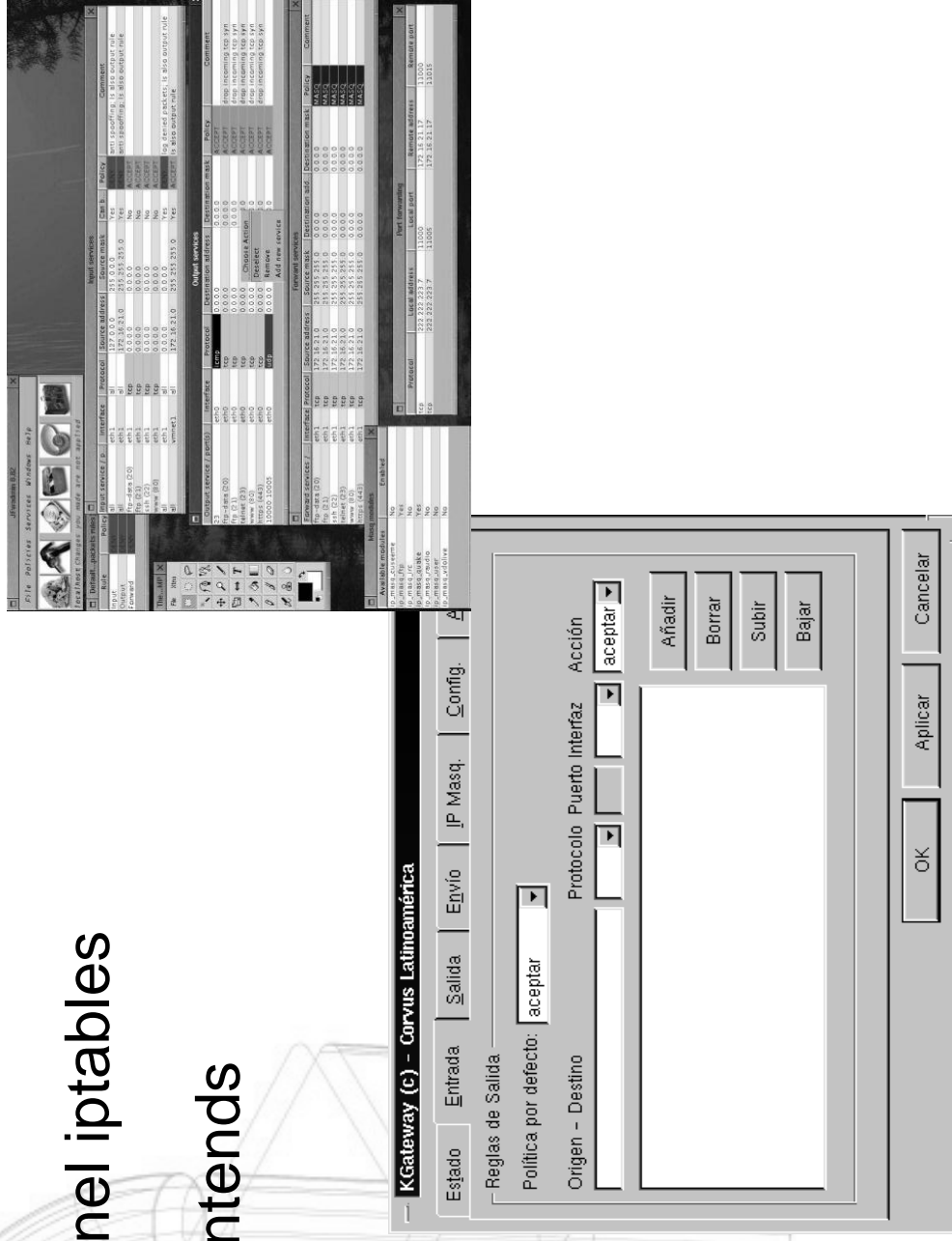
Ameaças

Ferramentas

- Definição de políticas
- Acompanhar os CERT advisories
- Firewall's, DMZ's e definição de regras (slide 14)
- Auditor de vulnerabilidades (slide 15)
- Intrusion Detection System's (snort)
- Comunicações seguras (SSH)
- Assinatura digital de ficheiros (tripwire)
- Interpretação de logs (scanlogd)

Firewall

- Comerciais (Firewall 1, Pix,...)
- Kernel iptables
- Frontends



Arquitectura

Ameaças

Ferramentas

Arquitectura

Ameaças

Ferramentas

Outro software

- **PGP** e criptografia chave pública
- **PAM** – Pluggable Authentication Modules
- Kerberos
- **CFS** - Cryptographic File System
- StackGuard
- **PGP** e criptografia chave pública
- **SSL, S-HTTP and S/MIME**
- Implementação **IPSEC**

2

linha

Conclusão

Não há sistemas seguros, mas...

- **D**eterminar o que é valioso...
- **D**escobrir as vulnerabilidades...
- **D**esencadear os mecanismos para as
minorar

Arquitectura

Ameaças

Ferramentas

Paulo Trezentos' 3 Ds policy



2

linha

Outras fontes

Linux Caixa Mágica

- <http://www.caixamagica.org>

Segurança

- <http://www.linuxsecurity.com>
- <http://www.securityfocus.com>
- Sites das distribuições

Ferramentas

- <http://www.freshmeat.net>



Paulo.Trezentos@adetti.iscte.pt

<http://paulo.trezentos.gul.pt/artigos/>

Obrigado.