


Segurança em Ambientes Corporativos utilizando a



Plataforma Operacional Linux

Rosane Caldeira

e-mail: rosane.caldeira@ifms.edu.br

Breve Histórico e Motivação



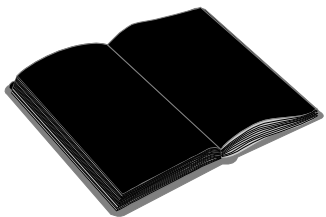
Diz o ditado: “ Boas cercas fazem bons vizinhos.”

Breve Histórico e Motivação

- ❑ O vírus “Internet Worm” de 1988 ganhou atenção nacional nos EUA depois de pegar grande número de *sites* desprevenidos.
- ❑ Robert Morris, o autor do verme, tinha soltado uma praga imperdoável na comunidade da Internet.
- ❑ O verme causou pouco dano mas aumentou a **coinsciência de segurança na Internet** mais que qualquer outro evento.
- ❑ Como resultado surgiram ferramentas para utilização em administração de sistemas.

Paradigmas

- ❑ Os paradigmas para escolha de ferramentas de segurança deixam empresas a mercê de um produto com soluções tipo “**Caixa Preta**”, no qual a tecnologia empregada é de conhecimento do fabricante e a segurança é obscura.
- ❑ Em contrapartida, podemos pensar em soluções baseadas em **software livre e código aberto**.



O que é Software Livre ?

- ❑ Programas de computadores construídos de forma colaborativa via Internet por uma comunidade de desenvolvedores independentes.
- ❑ São milhares de “hackers” no verdadeiro sentido da palavra, ou seja, programadores especialistas que renegam sua associação com os “ violadores de segurança “.

O que é Software Livre ?

- ❑ Nos programas convencionais, o código de programação é de propriedade da empresa que o desenvolveu, sendo impossível decifrar a programação.
- ❑ Muitas soluções de segurança “Open Source” nasceram em ambientes acadêmicos e são base para soluções proprietárias.
- ❑ O fato de não existir custo na aquisição da ferramenta não significa que sua tecnologia seja inferior.

O que é Software Livre ?

- Um software só pode ser considerado “Livre” se proporcionar quatro **liberdades fundamentais**:
 - Utilização com qualquer propósito;
 - Modificação e adaptação do programa tendo acesso ao código fonte com liberdade;
 - Redistribuição de Cópias;
 - Distribuição de versões modificadas do programa

O que é Software Livre ?

- ❑ o sistema operacional Linux é o exemplo mais conhecido que segue o conceito de software livre, é alternativo ao Windows e usado por quase metade dos provedores de internet do mundo.
- ❑ O sistema de defesa norte-americano e a NASA utilizam o sistema operacional Linux.
- ❑ Além disso, o Linux é baseado numa licença livre.

Segurança do Servidor

- ❑ O Servidor é o alvo primordial dos hackers.
- ❑ Se os hackers conseguem acesso a este computador, que em geral é o mais bem protegido da rede, é fácil conseguir acesso ao restante da rede

“Software Livre”

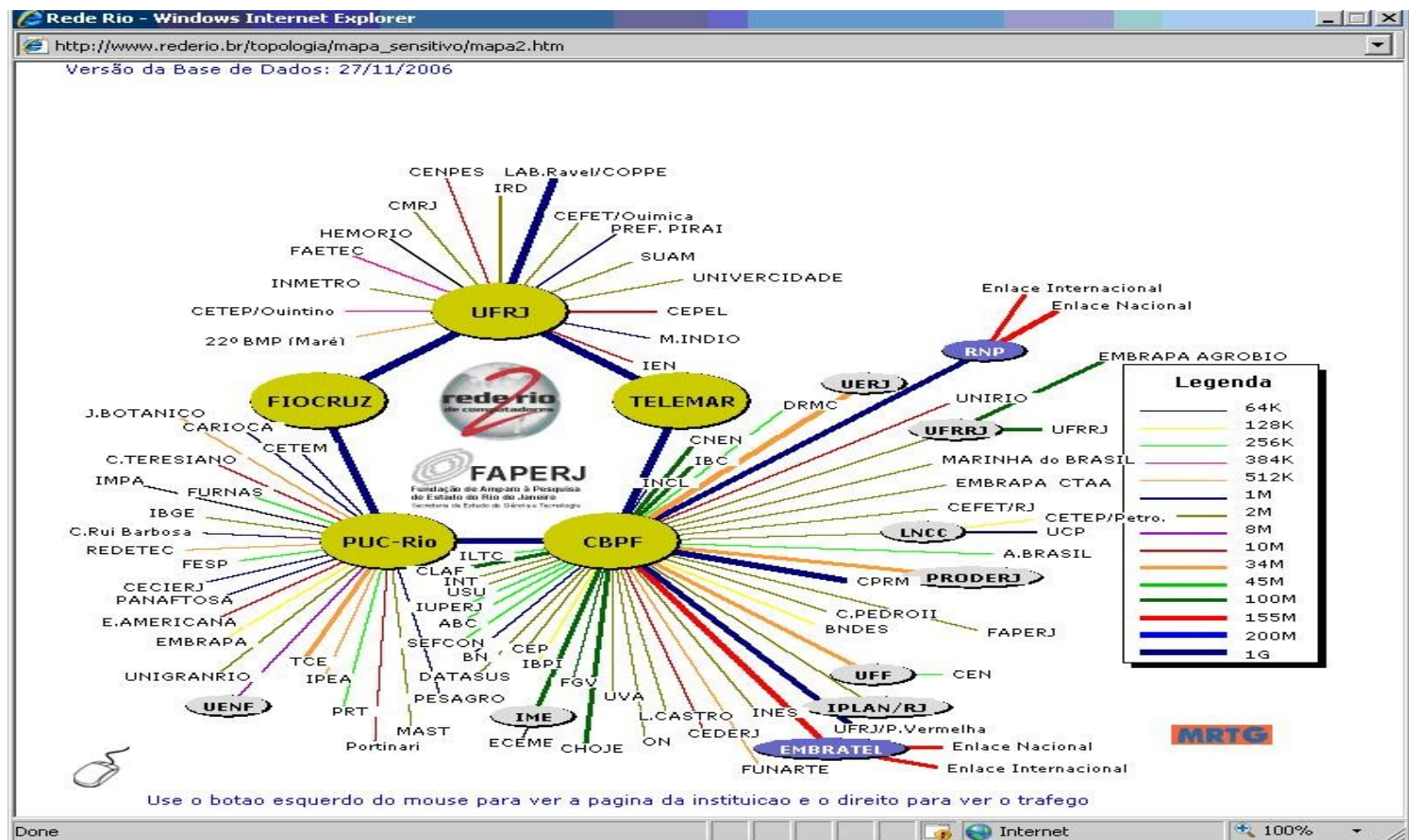
- Sabe-se que não existe segurança 100%.

EXISTE SIM



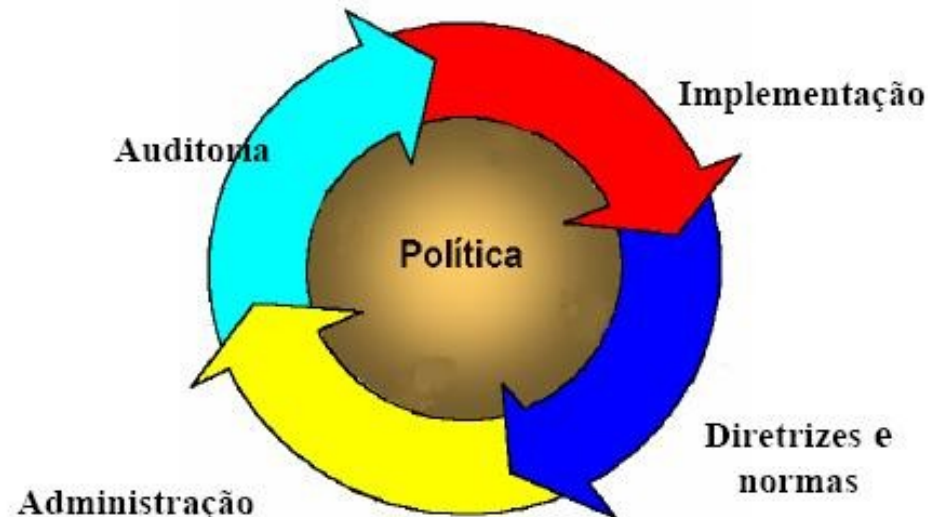
Necessidade de equilibrar fatores, o que se pensa como implementação de segurança do sistema tendo, a capacitação como base e, políticas, normas e softwares específicos, como meio.

Mapa da Rede Rio - Magnitude



Política de Segurança

- ❑ Deve prover direção e apoio a segurança da informação.
- ❑ Especificar metas de segurança da organização.
- ❑ Possui ciclo de vida indefinido.





Análise de Riscos

É a análise das ameaças, impactos e vulnerabilidades.

- ❑ Externos → Vírus, Worms e Trojans
- ❑ Internos → Desastres naturais e pessoas

Onde mora o perigo...

- ... Ele pode muito bem morar ao lado !



Vulnerabilidade é ...

- ❑ Falha no projeto, implementação ou configuração de um sistema que, quando sofre ataque, resulta na violação da segurança de um computador.

?

Quem é vulnerável ?

?

?

Como Identificar componentes

?

?

?

de rede vulneráveis ?

?

Quem é Vulnerável ?

- ❑ Instituições financeiras e Bancos

Atacados para cometer fraudes em C/C

- ❑ Provedores de Internet

Por usar grande quantidade de dados

- ❑ Companhias Farmacêuticas

Em Espionagem Industrial

- ❑ Governo e Agências de Defesa

Devido a falta de investimento

- ❑ Empresas Multinacionais

Tentativas de Espionagem

Identificando Componentes Vulneráveis

- ✓ O nmap varre portas de rede
- ✓ É executado por usuário root
- ✓ Se o cracker usar máquina Linux com conexão rápida, ele pode instalar um scanner de portas de rede como o nmap e sua presença não será notada.

Ferramentas de Segurança

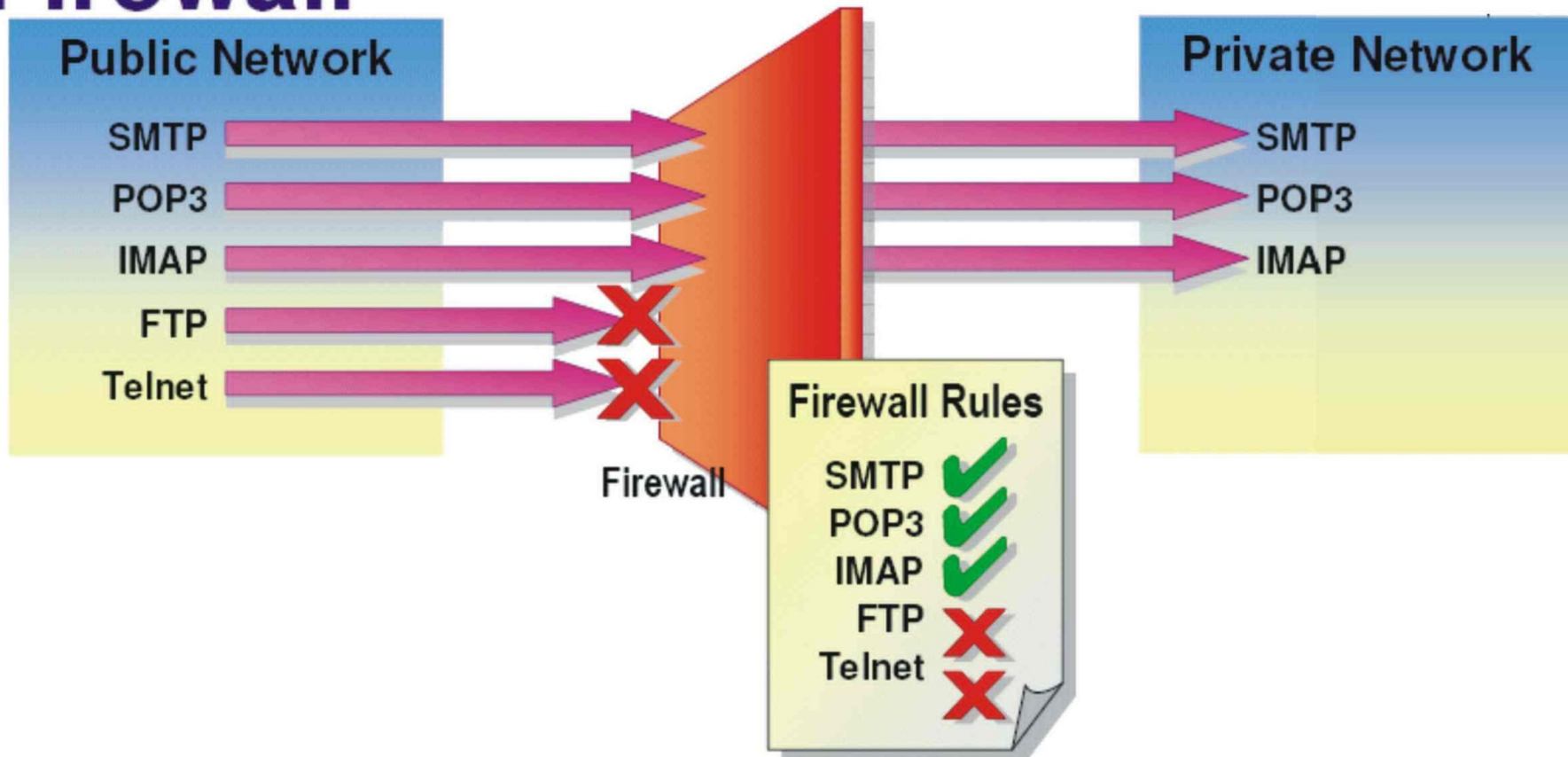
- ✓ São softwares destinados a segurança de sistemas computacionais.
- ✓ Surgem como alternativa as corporações de softwares de código aberto provenientes de pesquisas em centros acadêmicos.

Ferramentas de Segurança

- ✓ **Firewalls**
- ✓ **Sistema de Detecção de Erros (IDS)**
- ✓ **VPN**
- ✓ **Controle de Conteúdo da Web**
- ✓ **Criptografia**
- ✓ **Monitoramento de Redes**
- ✓ **Sniffers**

Parede de Fogo

Firewall



Parede de Fogo

- ✓ Conhecido como “Parede de Fogo”.
- ✓ Protege máquinas individuais e a nível de rede.
- ✓ Há três classes:
 - filtragem de pacotes
 - proxy de serviço
 - inspeção com informações de estado
- ✓ Em grandes corporações, pode ser ativado tanto em fronteiras de redes como em topologias departamentais aumentando sua funcionalidade.
- ✓ Há soluções de Firewall Bridge na forteira da rede, sendo estratégico, pois não tem IP.

Sistema de Detecção de Erros

- ✓ Possibilidade de detecção de intrusos na rede.
- ✓ Usando os “Host Intrusion Detection Systems” é possível avaliar até que ponto um sistema violado foi corrompido.
- ✓ Informações confrontadas dão condições de:
 - Detectar intrusos;
 - Verificar a integridade dos arquivos;
 - Identificar portas de rede;
 - Identificar Trojans

VPN

- ✓ É solução de segurança fim-a-fim entre roteadores, firewalls, estações de trabalho e servidores.
- ✓ VPN + Linux = custo inferior a qualquer solução em outra plataforma.

Controle de Conteúdo da Web

- ✓ É solução de segurança fim-a-fim entre roteadores, firewalls, estações de trabalho e servidores.
- ✓ Lista negra com sites e conteúdos não interessantes à corporação.

Criptografia é...

- ✓ A ciência e arte de escrever mensagens em forma cifrada ou em código
- ✓ Se o cracker usar máquina Linux com conexão rápida, ele pode instalar um scanner de portas de rede como o nmap e sua presença não será notada.

☐ 7b ≈ H & Z H 0 2 ♠ QCH 🌟 🕸 🏆 🧬 🏳️ AA ☐ ☐ / 🏆

Isso é sua senha que um cracker acabou de identificar
mesmo sendo criptografada

Monitoramento da Rede

- ✓ Acompanhamento dos eventos de uma rede, a fim de diagnosticar problemas para obter estatísticas para administração e otimização de desempenho.

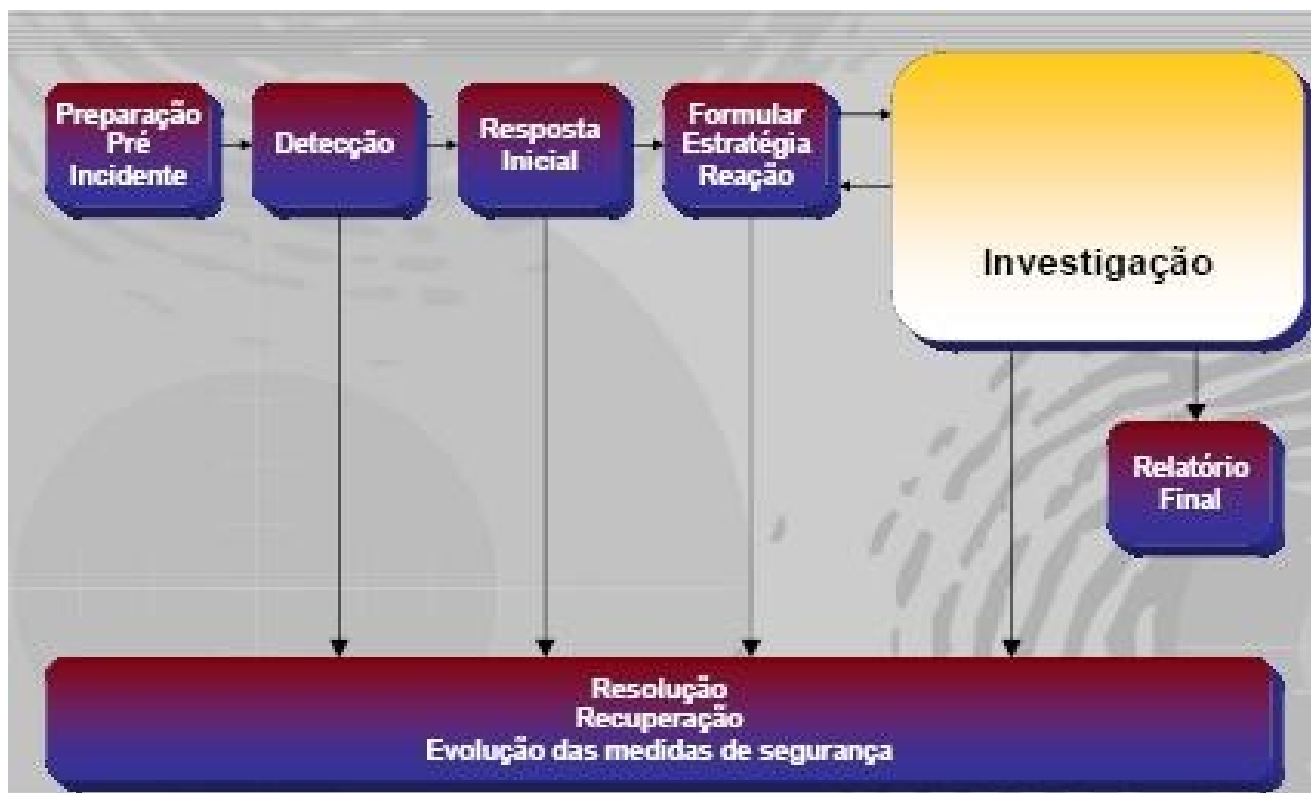
Sniffers



- ✓ Maneira efetiva dos crackers obterem informações sensíveis (como senhas de usuários) em locais de rede com conexões inseguras.

Investigação Corporativa

Ferramenta de Análise Forense



Caso de Injúria Identificada

- ❑ **CASO:** Uma diretora de RH começou a receber cartas ameaçadoras para que ela deixasse o seu cargo.
- ❑ **PROBLEMA:** As cartas eram enviadas por correio postal. Haviam 2000 suspeitos.
- ❑ **DESAFIO:** Não havia como investigar as máquinas pois as cartas eram enviadas de modo tradicional.
- ❑ **SOLUÇÃO:** Com o EnCase Enterprise e um mandato de busca e apreensão foi possível procurar na rede palavras chaves
- ❑ **RESULTADO:** Com uma semana de trabalho identificou-se 5 suspeitos e após uma semana de INVESTIGAÇÕES foi possível identificar o cabeça do grupo.

Ataque a Corporações

- ❑ O Banco de Dados da UCLA (Universidade da Califórnia) alertou mais de 800 mil pessoas que suas informações pessoais podem ter sido acessadas por crackers.
- ❑ Haiva interesse nos números de seguro social.
- ❑ Os criminosos exploraram uma “falha desconhecida do software” tendo tido acesso ao banco de dados da faculdade desde outubro de 2005.

Estatísticas de Ataque

- ❑ Índices estatísticos mostram o grande volume de ataques, e na grande maioria dos casos, é a desconfiguração do site que faz a diferença.
- ❑ Nem sempre a melhor ferramenta é tudo que se necessita para um projeto de segurança
- ❑ Pensar em segurança de sistemas tem uma fórmula algébrica de recursos:

“ **capacitação + metodologia + ferramental =
*bom projeto de segurança*** ”

Depoimento

□ Abril/2001

- “... É uma atitude de um desequilibrado...”

Fernando Néri

Presidente da Módulo Security, qualificando um ex-funcionário que divulgou esquemas das redes de grandes clientes para a imprensa.

□

.

Conclusão

- ❑ No mundo do software de código aberto o conceito de segurança por obscuridade não é aceito, pois a segurança está na transparência do código fonte aberto.
- ❑ O fato de aderir aos padrões internacionais e fundamentado em pesquisas acadêmicas torna o código aberto uma solução sustentável e confiável.
- ❑ Hoje, toda corporação tem como alternativa em projetos de segurança de sistemas computacionais, softwares de código aberto podendo usá-los confiando em sua qualidade e funcionalidade

Bibliografias

- **Pereira, Marcos B. N.** Aspectos da Análise forense. MBA. Disponível em <http://www.forensedigital.com.br>
- **Nemeth, EVI; Snyder, Garth; Seebass, Scott; Hein, TrentT.** Manual de Administração do Sistema UNIX. Bookman. 2005
- **Gelbeck, Clovis.** Notas de aula da disciplina Seminário em Processamento de Dados. PUC-RJ: Rio de Janeiro, 2001

Segurança em Ambientes Corporativos utilizando a Plataforma Operacional Linux

Rosane Caldeira

e-mail: rosane.caldeira@ifms.edu.br