REDES DE COMPUTADORES

UNIDADE 8 – Segurança em Redes de Computadores
(Aula 12 – Tipos de Ataques e Contramedidas)

Prof. Ivan Nunes da Silva

1. Histórico resumido da segurança em Redes de Computadores

- **Década de 60/70**
  - Criação da ARPANET;
  - ARPANET liberada para universidades e centros de pesquisa.
- **Década de 80**
  - Militares testam o TCP/IP;
  - ARPANET desmembrada em militar e civil;
  - Explosão na utilização de computadores pessoais;
  - Consolidação das Redes de Computadores;
  - Primeiro vírus experimental - Fred Cohen (1983);
  - Vírus de computadores começam a causar prejuízos às redes de computadores;
  - Primeiro Worm (1988) - Robert Morris Jr. - Paralisou 50% da internet.

2

1. Histórico resumido da segurança em Redes de Computadores

- **Década de 90**
  - Internet toma forma atual e se expande imensamente;
  - Ataques a sistemas atingem grandes proporções;
  - O termo “Hacker” passa a caracterizar os usuários mal intencionados da internet;
  - As técnicas para derrubar sistemas de segurança são difundidas amplamente pela própria internet;
  - Surgem Trojans extremamente eficientes;
  - No fim dos anos 90 os Worms passam a dominar os ataques.

3

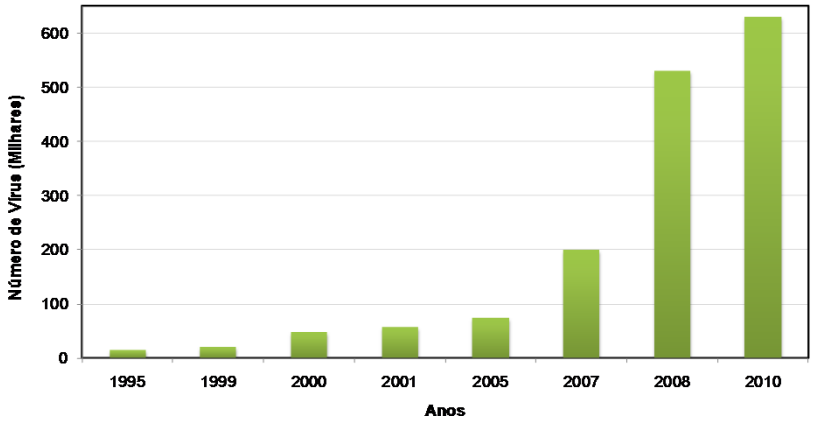
1. Histórico resumido da segurança em Redes de Computadores

- **Anos 2000**
  - Investimentos cada vez maiores em segurança;
  - Formação de profissionais especialistas em segurança da informação;
  - Vulnerabilidades de softwares são expostas diariamente na internet;
  - De uma maneira geral a segurança melhorou muito;
  - Os sistemas ainda estão sujeitos a diversos tipos de ataques: Portas, Vírus, Worms, Trojans...

4

1. Histórico resumido da segurança em Redes de Computadores

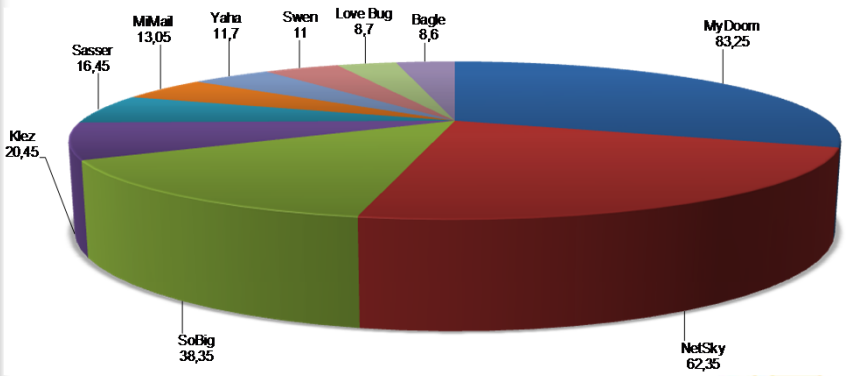
- **Anos 2000**
  - ➔ Estatísticas de vírus conhecidos:



5

1. Histórico resumido da segurança em Redes de Computadores

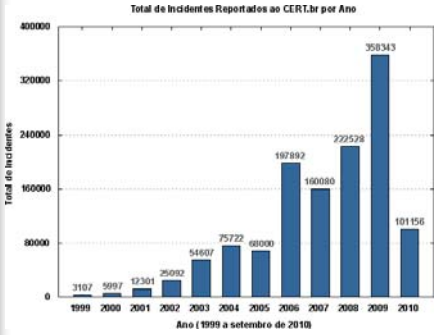
- **Prejuízos**
  - ➔ Lista dos mais danosos ataques (Bilhões de Dólares) http://www.mi2g.com:



6

1. Histórico resumido da segurança em Redes de Computadores

- **Atualmente**
  - ➔ Incidentes no Brasil:



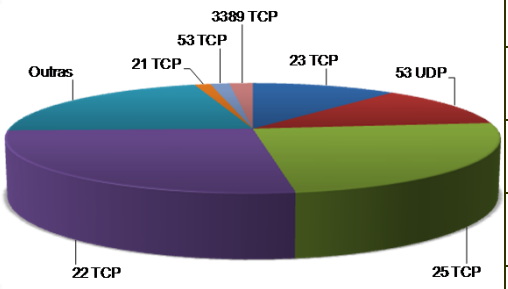
Incidentes no Brasil – Julho à Setembro de 2010

Mês	Total	Worms	Invasões	Ataque à WEB	Port Scans
jul	12661	1150	22	986	7718
ago	14171	1213	5	928	9186
set	13177	904	11	734	8882
Total	40009	3267	38	2648	25786

7

2. Tipos de Ataques

- ***Port Scanning***
  - ➔ Utilização de softwares para obtenção de portas vulneráveis de um sistema:



Porta	Serviço
21,22 TCP	FTP
23 TCP	Telnet
25 TCP	SMTP
3389 TCP	Acesso Remoto
53 TCP, UDP	DNS

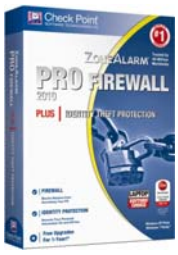
8

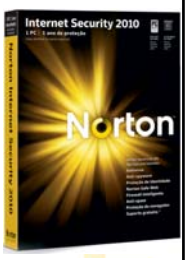
2. Tipos de Ataques

- **Port Scanning**

➔ Contramedidas:

- Manter o Sistema Operacional sempre atualizado;
- Utilizar um Firewall.



9

2. Tipos de Ataques

- **Vírus**

➔ Programa malicioso desenvolvido com o intuito de danificar o sistema:

- **Não se replica sozinho;**
- **Perda de desempenho do computador;**
- **Exclusão de arquivos;**
- **Alteração de dados;**
- **Acesso à informações confidenciais por pessoas não autorizadas;**
- **Perda de desempenho da rede (local e Internet);**
- **Monitoramento de utilização (espiões);**
- **Inutilizar hardware .**

10

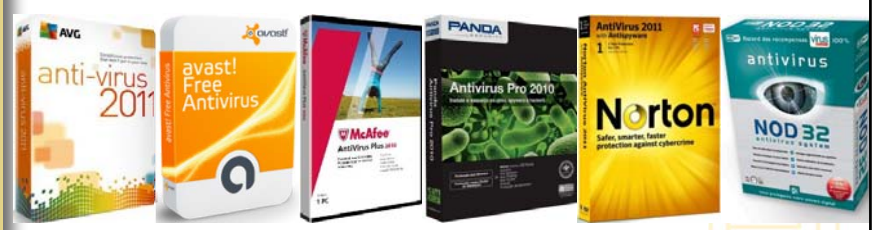
2. Tipos de Ataques

- ***Vírus***
  - ➔ Principais ataques de Vírus:
    - ***Brain*** **(1986) – Vírus de MS-DOS, Infectava disquetes;**
    - ***Lehigh*** **(1987) – Infectava o command.com;**
    - ***Suriv-02*** **(1987) – Infectava arquivos .exe;**
    - ***Jerusalem*** **(1987) – "Sexta-feira 13", apagava arquivos;**
    - ***Christimas*** **(1987) – 500 mil computadores infectados / hora;**
    - ***MacMag*** **(1988) – Primeiro vírus de Macintosh;**
    - ***AIDS*** **(1989) – Criptografava a memória;**
    - ***Tequila*** **(1990) – Primeiro vírus polimórfico;**
    - ***Michelangelo*** **(1992) – Em 6 de março formatava o HD;**
    - ***Chernobyl*** **(1998) – Atacava a BIOS do PC dia 26 de abril;**
    - ***Rugrat*** **(2004) – Primeiro vírus específico para Intel 64 bits;**
    - ***Scob*** **(2004) – Ataca servidores web da Microsoft.**

11

2. Tipos de Ataques

- ***Vírus***
  - ➔ Contramedidas:
    - Não acionar arquivos desconhecidos;
    - Utilizar software antivírus.



12

2. Tipos de Ataques

- **Worms**
  - ➔ Variante de vírus de computador capaz de se auto replicar:
    - **Foram criados inicialmente com o objetivo de vasculhar erros em redes (Xerox, 1978);**
    - **Código malicioso mais ativo atualmente;**
    - **Sua rápida disseminação afeta o fluxo de dados da rede;**
    - **Entre 1980 e 1990 os programadores estavam mais preocupados em se divulgarem;**
    - **Com a chegada do Windows 2000 os Worms tiveram sua capacidade de disseminação aumentada;**
    - **Os Worms podem ser difundidos via e-mail, serviços de mensagens instantâneas, compartilhadores de arquivos, Scripts de páginas web...**

13

2. Tipos de Ataques

- **Worms**
  - ➔ Principais ataques de Worms:
    - ***Morris Worm* (1988) – Paralisou 50% da internet;**
    - ***Melissa* (1999) – Infecta arquivos do Word anexos em emails;**
    - ***BubleBoy* (1999) – Alterava as visualizações dos emails;**
    - ***I Love You* (2000) – Derrubou diversos servidores de emails;**
    - ***SirCam* (2001) – Espalha-se por email redes locais;**
    - ***Nimda* (2001) – Contaminou Outlook e Outlook Express;**
    - ***Code Red* (2001) – Buffer Overflow através da porta 80 TCP;**
    - ***Slammer* (2003) – Coréia do Sul ficou off line por 12 horas;**
    - ***Blaster* (2003) – Utiliza uma falha de segurança para replicar;**
    - ***MyDoom* (2004) – Diminuiu em 10% o fluxo global da internet;**
    - ***Sasser* (2004) – Reinicia computadores afetados.**

14

2. Tipos de Ataques

- ***Worms***

  ➔ Contramedidas:

  - **Worms aproveitam-se de vulnerabilidades dos softwares e Sistemas Operacionais;**
  - **Deve-se manter o computador sempre atualizado;**
  - **Sistemas Operacionais antigos como Windows 95, 98... são mais susceptíveis a ataques de Worms por não possuírem um sistema de segurança eficiente.**

15

2. Tipos de Ataques

- ***Trojans***

  ➔ Trojan Horses ou cavalos de tróia são softwares dissimulados camuflados de aplicativos de usuários:

  - **Transformam o computador em um terminal de internet aberto;**
  - **Estes programas eliminam as proteções que impedem a transferência de informações, abrindo uma *BackDoor;***
  - **Os Trojans são considerados as maiores ameaças já criadas para as redes de computadores, pois permitem o controle total dos computadores infectados;**
  - **A remoção de um Trojan é dificílima, pois ele não infecta outros arquivos e o invasor causa estragos antes mesmo de ser detectado;**
  - **Atualmente os Trojans tem por objetivo a captura de informações financeiras através de *KeyLoggers*.**

16

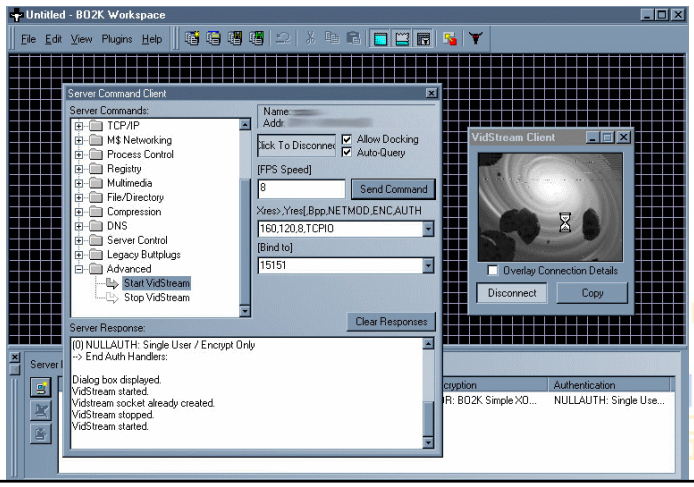
2. Tipos de Ataques

- **Trojans**
  - ➔ *BackOrifice* (1998)
    - **Recebeu esse nome como sátira ao software Back Office da Microsoft;**
    - **Utiliza as portas TCP 31337 e 31338;**
    - **Invisível à lista de programas em execução.**
    - **Funcionalidades: Cria, lista, deleta ou compartilha diretórios, Lista aplicativos ativos, Executa aplicativos do servidor, Compartilha drives do servidor, Copia, deleta e procura qualquer arquivo, Compacta e descompacta arquivos, Visualiza o conteúdo de documentos texto, Captura o que está sendo digitado no servidor, Mostra as senhas do cache, Captura tela, vídeo e áudio, Lista todas as interfaces de rede, domínios, servidores e envios do servidor, Executa plug-ins do BO no servidor, Cria, altera e deleta chaves no registro do Windows...**

17

2. Tipos de Ataques

- **Trojans**
  - ➔ *BackOrifice* (1998)



18

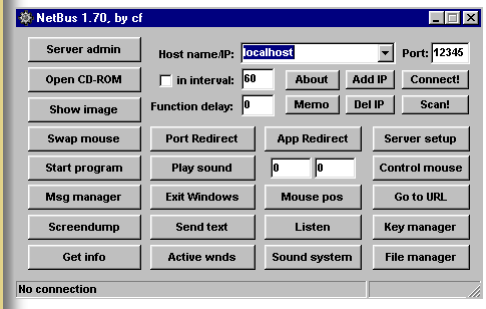
2. Tipos de Ataques

- ***Trojans***
  - ➔ *NetBus* (1998)
    - ➢ **Trojan extremamente eficiente;**
    - ➢ **Permite assumir o controle total da máquina infectada;**
    - ➢ **Invisível à lista de programas em execução;**
    - ➢ **Utiliza as portas TCP 12345, 12346 e 20034;**
    - ➢ **Possui uma interface gráfica de fácil operação;**
    - ➢ **Quando a estação infectada conecta-se na internet, um sinal é enviado até o invasor, que passa a operar remotamente o computador da vítima;**
    - ➢ **Infecta sistemas Windows 95, 98 e NT.**

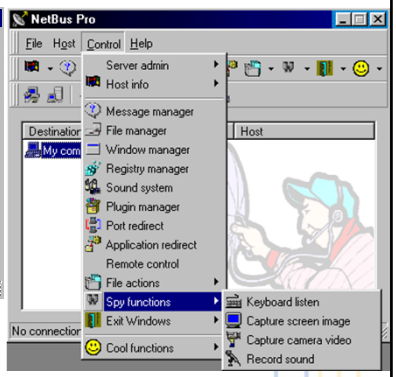
19

2. Tipos de Ataques

- ***Trojans***
  - ➔ *NetBus* (1998)



Primeiras versões



Versão Professional

20

2. Tipos de Ataques

- ***Trojans***
  - ➔ Contramedidas:
    - **Utilizar um Sistema Operacional moderno e constantemente atualizado;**
    - **Utilizar antivírus e Firewall também atualizados;**
    - **Não instalar inadvertidamente arquivos executáveis;**
    - **Sempre desconfiar de emails de remetentes desconhecidos.**

21

2. Tipos de Ataques

- ***Spoofing***
  - ➔ Mascara a identidade real do host por meio de software, fazendo-se passar por outro host:
    - **Mascarar o host permite fazer com que uma máquina não reconhecida em uma rede possa ser reconhecida;**
    - **Permite ao host ficar anônimo enquanto faz um ataque, protegendo seus rastros;**
    - ***IP Spoofing*: muito empregado em invasões a servidores;**
    - ***ARP Spoofing*: Utilizado em redes que utilizam o MAC Address para autenticação;**
    - **O Anti-Spoofing deve ser implementado em regras de roteamento e tradução de endereços nos roteadores.**

22

2. Tipos de Ataques

- **DoS**
  - Denial of Service – Negação de Serviço:
    - **Os ataques causam a interrupção de serviços de um site;**
    - **Um software malicioso envia mensagens aparentemente normais em UDP para um servidor ;**
    - **O código DoS confunde o servidor, fazendo com que ele ache que os pacotes UDP estão vindo dele mesmo;**
    - **Ao tentar responder esse grande fluxo de dados defeituosos, o servidor pára de responder, interrompendo o serviço aos usuários;**
    - **DDoS – Distributed Denial of Services: Ataque DoS ampliado, utilizando diversas estações ;**
    - **Contramedidas: Utilizar softwares IDS (*Intrusion Detection System*).**

23

2. Tipos de Ataques

- **DoS**
  - Casos famosos de ataques DoS à sites em fevereiro de 2000:
    - Yahoo! – Site de busca, 4 horas fora do ar;
    - ETrade, Datek – Compra e venda de ações;
    - ZDNet – Site de tecnologia;
    - Amazon, Buy.com – Lojas virtuais;
    - CNN – Rede de notícias;
    - eBay – Site de leilões pela internet;
    - Time Warner – Site da rede de TV.

Ataques realizados em menos de 8 horas

24

2. Tipos de Ataques

- ***Defacement***
  - Desfiguração de web sites através de falhas de segurança:
    - **Em 17 de março de 2003 a Microsoft anunciou que 75% de todos os servidores IIS 5.0 (Internet Information Servers) estavam vulneráveis a ataques;**
    - **Por padrão, o IIS checa a presença de "..\.." nas URLs solicitadas, pois pode significar tentativas de acesso a diretórios restritos, Ex: www.victimserver.com/../../../file.txt;**
    - **Substituindo-se estes caracteres pelos seus respectivos códigos UNICODE, as ferramentas de segurança do IIS falhavam.**

www.victimserver.com/contents/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/..%c0%af/winnt/system32.cmd.exe?/c%20dir%20/S20c:*contents

25

2. Tipos de Ataques

- ***Defacement***
  - Desfiguração de web sites através de falhas de segurança:
    - **Os *Defacers* buscam atacar os arquivos padrões de índices de uma página web em servidores IIS: default.html, index.html, main.html...**
    - **Sites PHP ("PHP: Hypertext Preprocessor", originalmente Personal Home Page) também possuem vulnerabilidades que permitem ao usuário mal intencionado fazer com que o sistema retorne as senhas padrões de administrador;**
    - **Conhecendo as senhas, é possível se alterar todas as configurações do site, inclusive a página principal;**
    - **Contramedidas: Utilização de servidores IIS e PHP atualizados e confiáveis; Mudar o padrão dos arquivos de índices.**

26

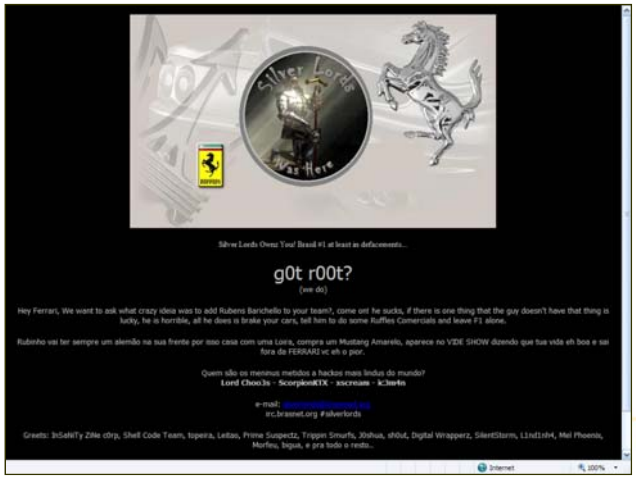
2. Tipos de Ataques

- **Defacement**
  - ➔ Exemplos: Microsoft

27

2. Tipos de Ataques

- **Defacement**
  - ➔ Exemplos: Ferrari



28

2. Tipos de Ataques

- ***Defacement***
  - ➔ Exemplos: Site do candidato José Serra

29

2. Tipos de Ataques

- ***Spam***
  - ➔ Mensagem de correio eletrônico enviada em massa:
    - **Na maioria das vezes apenas incomodam os usuários, pois possuem caráter apelativo comercial;**
    - ***Spams* podem também ser uma porta para outros tipos de ataques como vírus, trojans, worms...**
    - **Os Spammers podem se utilizar de brechas de segurança para instalar servidores de emails não autorizados em servidores de emails particulares;**
    - **Uma vez infectado, o servidor de email pode disparar milhares de mensagens para destinatários selecionados pelo usuário mal intencionado, congestionando a rede.**

30

2. Tipos de Ataques

- ***Spam***
  - ➔ *Phishing*
    - **Principal tipo de ataque realizado atualmente;**
    - **Uma cópia idêntica de um site oficial é enviada por email aos usuários, solicitando geralmente dados bancários e de cartão de crédito;**
    - **O formulário ao ser preenchido pode disparar um outro código malicioso capaz de capturar informações do usuário;**
    - **Este tipo de ataque é muito eficiente pois se utiliza da confiança do usuário na instituição a ser fraudada e na verossimilhança do email.**

31

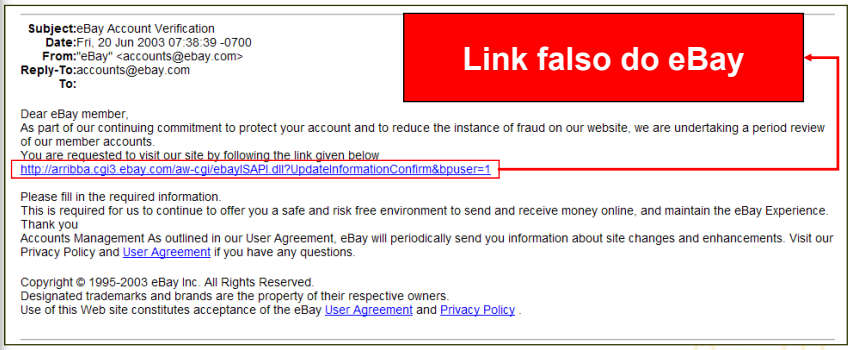
2. Tipos de Ataques

- ***Spam***
  - ➔ Exemplos de *Phishing*

32

2. Tipos de Ataques

- ***Spam***
  - ➔ Exemplos de *Phishing*



33

2. Tipos de Ataques

- ***Spam***
  - ➔ Contramedidas de *Phishing:*
    - **Utilizar um navegador com filtro anti-phishing;**
    - **Desconfiar de links com conteúdo ativo: *.php, *.asp, *.cgi, *.jsp, *.dll, *.exe...**
    - **A maioria dos serviços de email bancários só são enviados com autorização do usuário;**
    - **Procure pela presença de conteúdo seguro: https, wwws, ftps... e um cadeado no link indicando ambiente seguro.**

34

2. Tipos de Ataques

- ***Spyware***
  - ➔ Software espião que trabalha de maneira silenciosa:
    - **Software que colhe informações a respeito dos gostos, hábitos, comportamentos do usuário e enviam estas informações para uma entidade externa;**
    - **Podem também ficar residentes em busca de informações bancárias, cartões de crédito, sendo acionados quando um conteúdo específico é processado;**
    - **Podem ser instalados automaticamente através de sites com conteúdos ativos, principalmente os que possuem barra de navegação ;**
    - **Também podem vir de "brinde" em outros softwares: KazaA, eMule...**

35

2. Tipos de Ataques

- ***Spyware***
  - ➔ Contramedidas:
    - **Utilizar um filtro de privacidade no navegador;**
    - **Utilizar softwares anti-spyware: Adware, Spyware Blaster, AdWareAway, Arovax AntiSpyware...**
    - **Os *Spywares* também podem inspecionar *cookies*, portanto deve-se limpar constantemente o cache de *cookies*;**
    - **A utilização de firewalls pode impedir o envio destas informações ou mesmo a gravação destes softwares.**

36

3. Políticas de Backup

- Consiste de medidas tomadas pelos administradores da rede para proteger arquivos fundamentais;
- Estas medidas devem ser capazes de restaurar as informações mediante um ataque ou perda não intencional de informações importantes;
- As cópias de segurança são indispensáveis para quaisquer tamanhos de redes e tipos de usuários.

37

3. Políticas de Backup

- Tempo, tipo de Backup e mídias:

➔ Tempo
- Diários
- Semanais
- Quinzenais
- Mensais
- Trimestrais
- Semestrais
- Anuais
- Com evento

➔ Tipo
- Normal
- Incremental
- Diferencial

Mídias de Backup		
Tipo	Capacidade (GBytes)	Velocidade (MBits/s)
Fita	75.0	2.85
DVD	8.5	11.10
HD DVD	30.0	36.55
BlueRay	54.0	54.00
HD SATA Barracuda	2000.0	800.00

38

3. Políticas de Backup

- **Ferramentas**

➔ Software:

- **Ferramentas do próprio sistema operacional;**
- **Ferramentas profissionais: Norton System Works, Drive Backup Professional, Ahead Nero...**

➔ Hardware:

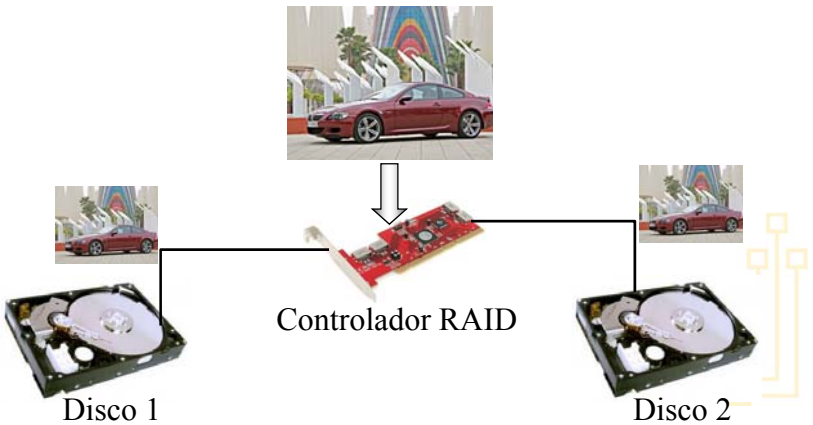
- **Fitas;**
- **CD-Rom, DVD, HD-DVD, BlueRay;**
- **Discos Magnéticos: IDE, SATA, SCSI;**
- **RAID.**

3. Políticas de Backup

- **Ferramentas**

➔ *RAID* (1988): *Redundant Array of Independent Disks*

- **Uma única unidade virtual composta por vários discos individuais.**



3. Políticas de Backup

- **Localização**

➔ Mesmo prédio:

- **Onboard;**
- **Off-board;**
- **Computadores diferentes.**

Hot Plug

HD Externo

41

3. Políticas de Backup

- **Localização**

➔ Prédios separados, conectados por:

- **Fibra óptica;**
- **Canal exclusivo;**
- **Rádio;**
- **Par trançado.**

Backup

Banco de dados

42

4. Medidas de Segurança

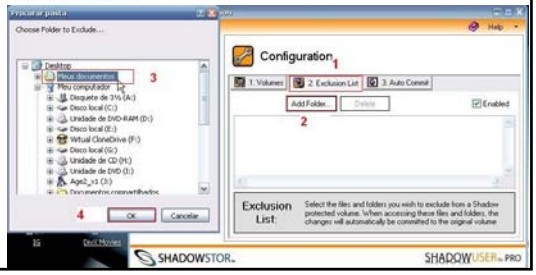
- Utilizar sistemas operacionais compatíveis com o fluxo de informação da rede;
- Firewalls, anti-vírus, anti-spywares devem ser utilizados para evitar ataques e espiões;
- O servidor de email e o DNS devem ser também muito bem protegidos, para se evitar contaminação por *Spams* e Port Scannings;
- A política de Backup deve ser capaz de atender as necessidades de segurança, capacidade e performance que a quantidade/qualidade dos dados exigem;
- Deve-se investir em treinamento pessoal e campanhas de conscientização de segurança, pois o usuário é a peça principal das redes de computadores.

43

5. Se Ainda Assim, Nada der certo...

- ShadowUser Pro (XP) e Shadow Defender (SOs x86 e x64)

- Softwares que fornecem uma blindagem ao sistema;
- Alterações somente realizadas com a ferramenta desligada;
- Pastas de exclusão são as únicas permitidas para alterações.
- Conteúdo do disco protegido está sempre intacto;
- Mesmo diante do mais cruel ataque, ao reiniciar, tudo volta ao normal.



44

Fim da Apresentação

AULA DE 03/12/2013

Não Haverá Aula em Sala

(Reservada p/ Estudo dos Tópicos Abordados na P2)

Data da P2 ➔ 10/12/2013

45