CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
Unidade de Ensino Descentralizada de Leopoldina

Ronaldo Louro Meneguite

Segurança da Informação

CEFET-MG – UNED – Leopoldina

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
Unidade de Ensino Descentralizada de Leopoldina

Ronaldo Louro Meneguite

Segurança da Informação

Orientador: Prof. Alexandre Bartoli Monteiro
Curso Técnico de Informática Industrial

Estagiário: Ronaldo Louro Meneguite
e-mail: ronaldolouro@yahoo.com.br
Endereço: Rua Getomir Pereira Bela, 13
Bairro: Cristo Redentor
Cidade: Leopoldina, MG
CEP: 36.700-000
Telefone: (32)3441-8822

Empresa: Cia. Força e Luz Cataguazes Leopoldina
Supervisor de Estágio: Wilson Pestana Madella
Cargo: Técnico
e-mail: wilson@cataguazes.com.br
Endereço: Praça Rui Barbosa, 80
Bairro: Centro
Cidade: Cataguases, MG
CEP: 36.770-000
Telefone/fax: (32)3429-6278 / (32)3429-6517

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
Unidade de Ensino Descentralizada de Leopoldina

Ronaldo Louro Meneguite

Segurança da Informação

Aprovado em : ___/ ___/ _____

Prof. Alexandre Bartoli Monteiro
Orientador de Estágio
Coordenação de Luis Claudio Gambôa Lopes

Aprovado em : ___/ ___/ _____

Wilson Pestana Madella
Supervisor de Estágio
Cia. Força e Luz Cataguases Leopoldina

ÍNDICE

GLOSÁRIO

Ataque: Evento que pode comprometer a segurança de um sistema ou uma rede. Um ataque pode ter ou não sucesso. Um ataque com sucesso caracteriza uma invasão.

Autenticação: É o processo de se confirmar a identidade de um usuário ou um host, esta pode ser feita na camada de aplicação (através de uma senha), ou mais complexa, utilizando algoritmos específicos.

Bug: Uma falha, ou fraqueza em um sistema de computador.

Cavalo de Tróia: Uma aplicação ou código que, sem o conhecimento do usuário realiza alguma tarefa que compromete a segurança de um sistema, em geral, esta aplicação se apresentação usuário de forma rotineira e legítima.

Denial of Service: Interrupção de serviço.

Engenharia Social: Técnica utilizada por hackers para obter informações interagindo diretamente com as pessoas.

Exploits: Programa ou parte de um programa malicioso projetado para explorar um vulnerabilidade existente em um software de computador.

Firewall: Equipamento e/ou software utilizado para controlar as conexões que entram ou saem de uma rede. Eles podem simplesmente filtrar os pacotes baseados em regras simples, como também fornecer outras funções tais como: NAT, proxy, etc.

HTTP: Do inglês HyperText Transfer Protocol. Protocolo usado para transferir páginas Web entre um servidor e um cliente.

Invasão: Caracteriza um ataque bem sucedido.

NAT: Network Address Translation - Mecanismo que permite a conexão de redes privadas à rede Internet sem alteração dos endereços reservados. Através de um NAT server os endereços de rede reservados são convertidos para endereços públicos quando se torna necessário o acesso à rede Internet. Com este mecanismo, diversos computadores com endereços internos podem compartilhar um único endereço IP.

Scanner: Ferramenta utilizada por hackers ou especialistas em segurança que serve para "varrer" uma máquina ou uma rede, em busca de portas abertas, informações ou serviços vulneráveis.

SMTP: Do inglês Simple Mail Transfer Protocol. Protocolo padrão para envio de e-mail através da Internet.

Stealth: São os programas que tem habilidade de agir sem ser detectado.

Trojan (Cavalo de Tróia)**:** Uma aplicação ou código que, sem o conhecimento do usuário realiza alguma tarefa que compromete a segurança de um sistema, em geral, esta aplicação se apresenta ao usuário de forma rotineira e legítima.

Vírus: São códigos ou programas que infectam outros programas e se multiplicam, na maioria das vezes podem causar danos aos sistemas infectados.

Vulnerabilidade: Estado de um componente de um sistema que compromete a segurança de todo o sistema, uma vulnerabilidade existe sempre, até que seja corrigida, existem vulnerabilidades que são intrínsecas ao sistema. Um ataque explora uma vulnerabilidade.

Worm: Um worm é semelhante a um vírus, mas difere pelo fato de não necessitar de um programa específico para se infectar e reproduzir. Muitos vírus hoje, possuem a característica de worms e vice e versa.

1 APRESENTAÇÃO

Estagiei na Cia. Força e Luz Cataguazes-Leopoldina (CFLCL) uma empresa que faz parte de um grande complexo de energia de nossa região o Sistema Cataguazes-Leopoldina este tem sua principal base de atividade no setor elétrico, onde atua com cinco distribuidoras e duas geradoras. Está presente em Minas Gerais, Rio de Janeiro, Sergipe e Paraíba.

Figura 1: Sede da CFLCL no ano da fundação - 1905

Figura 2: Sede da CFLCL hoje

A Cia. Força e Luz com uma estrutura gigantesca se comparada com as minhas experiências anteriores, me ofereceu uma oportunidade de conhecer desde equipamentos ultrapassados até equipamentos de ultima geração, também lá tive a oportunidade de conviver e aprender muito com profissionais qualificados.

Estagiei em um setor chamado DETE (Departamento de Telemática) ao qual hoje teve seu nome alterado para DETI (Departamento de Infra-Estrutura de T I), este setor é responsável pela implantação, manutenção e suporte a grande parte dos equipamentos pela empresa utilizados, desde aparelhos de fax, impressoras e até em raros momentos em servidores de ultima geração.

Diante de tamanho porte, e estrutura o que me chamou muito atenção foi o sistema de segurança lá adotado. Além do fato já ter certa afinidade anterior a esta área chamada Segurança da Informação, esta experiência foi decisiva na hora da escolha de um tema para o meu trabalho final de conclusão de estagio.

Procurei durante os meus estágios ser uma adição no grupo, me mostrando sempre disposto a aprender tudo aquilo que estavam dispostos a me ensinar, e tenho convicção que isto foi primordial para eu ser hoje quem sou e saber o que sei.

2 INTRODUÇÃO

O mercado de segurança em TI vem crescendo a cada ano e se tornando um dos pilares de sustentação de empresas que investiram montantes consideráveis em toda a infra-estrutura de TI. Toda essa infra-estrutura, cada vez mais complexa e interligada, com múltiplos pontos de acesso, demanda a adoção de soluções de segurança capazes de monitorar as tentativas de violação dos dados gerados por inúmeras transações. Assim surgiu à necessidade de se utilizar melhores mecanismos para prover a segurança das transações de informações confidenciais. A questão segurança é bastante enfatizada, principalmente, quando se imagina, a possibilidade de se ter suas informações, expostas à atacantes ou intrusos da Internet, que surgem com meios cada vez mais sofisticados para violar a privacidade e a segurança das comunicações. Devido a estas preocupações, a proteção da informação tem se tornado um dos interesses primários dos administradores de sistemas.

A Segurança da Informação consiste na certeza de que as informações de uso restrito não devem ser acessadas, copiadas ou si quer lidas por pessoas não autorizadas.

A informação pode existir de diversas formas. Pode ser, impressa, escrita, armazenada de forma eletrônica ou transmitida via e-mail. Independente da forma que é apresentada ou meio pelo qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida de forma adequada.

Durante este trabalho estarei dando maior ênfase a parte da segurança ligada a área de computação, já que a segurança é um tema muito amplo e falar nela como um todo poderia deixar meu trabalho muito superficial.

3 CONCEITOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação é essencial para qual quer empresa seja ela de grande ou pequeno porte, pois as vulnerabilidades existem, os ataques também existem e crescem a cada dia, tanto em quantidade quanto em qualidade.

Uma infra-estrutura de segurança não é só necessária como obrigatória, devendo existir, além de um investimento específico, um planejamento, uma gerência e uma metodologia bem definida.

3.1 PILARES DE UM SISTEMA SEGURO

Os pilares de um sistema seguro são: Integridade, Autenticação, Não-repúdio ou irrevogabilidade e Disponibilidade.

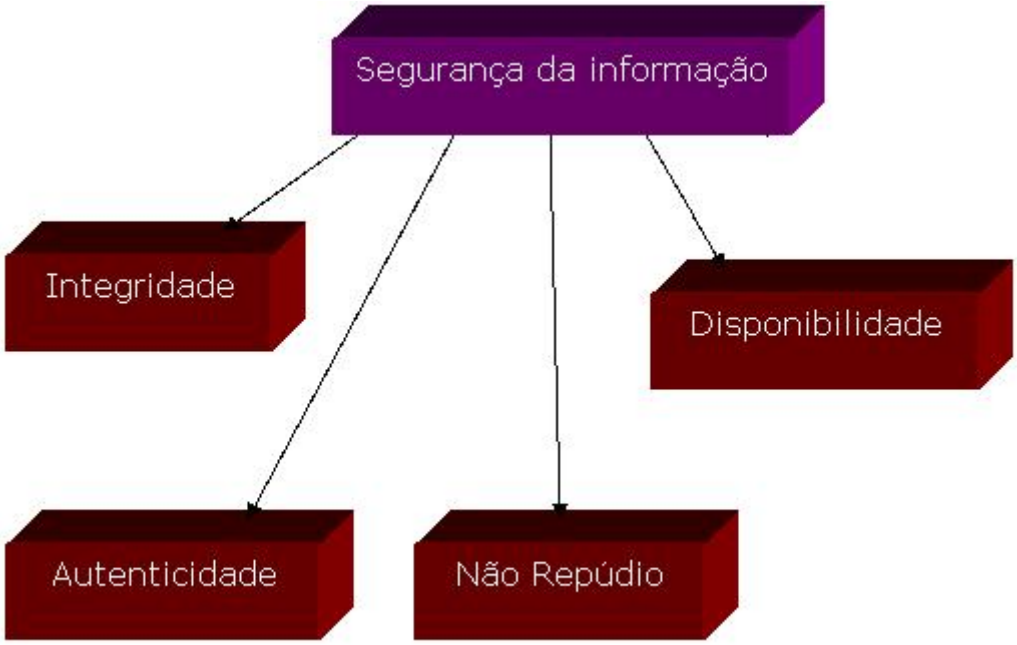

Figura 1: Diagrama da Segurança da informação

3.1.1 INTEGRIDADE

Deve ser possível ao receptor de uma mensagem verificar se esta foi alterada durante o trânsito.

3.1.2 AUTENTICAÇÃO

Deve ser possível ao receptor de uma mensagem, verificar corretamente sua origem, um intruso não pode se fazer passar (personificar) o remetente desta mensagem.

3.1.3 NÃO-REPÚDIO OU IRREVOGABILIDADE

O remetente de uma mensagem não deve ser capaz de negar que enviou a mensagem.

3.1.4 DISPONIBILIDADE

Se refere ao sistema estar sempre pronto a responder requisições de usuários legítimos. Para conseguirmos isto existem diversos artifícios como por exemplo:

3.1.4.1 NO-BREAKS

Figura 2: Exemplo de um No-break gerenciável.

Os problemas de energia elétrica são as maiores causas de defeitos nos sistemas de computadores e na perda de dados. O uso de sistemas de controle de energia tipo No-Break proporcionará a proteção necessária e evitará problemas nos sistemas de computadores, equipamentos eletrônicos e de telecomunicações, centrais telefônicas, etc.

A grande vantagem de usar um no-break é ter garantia de um fornecimento contínuo de eletricidade. Mesmo que ocorra um pique de energia ou o fornecimento seja cortado, você poderá continuar trabalhando até que as baterias do no-break se esgotem, tendo tempo para salvar seus documentos e desligar tranqüilamente o todo o sistema.

Existem dois tipos de no-breaks, os on-line e os off-line. Os primeiros, os on-line, são melhores, pois neles a bateria é alimentada continuamente e o micro é alimentado diretamente pela bateria, tendo um fornecimento 100% estável.

Nos no-breaks off-line a energia da toma é repassada diretamente para o micro, sendo a bateria usada apenas quando a corrente é cortada, não oferecendo uma proteção tão completa quanto o primeiro.

Em geral o no-break sinaliza de forma visual e sonora logo quando a energia é cortada. Conforme a bateria for ficando fraca a sinalização vai se tornando cada vez mais freqüente.

A autonomia das baterias varia de acordo com a capacidade das baterias (medida em VAs) e o consumo elétrico do sistema ligado ao mesmo.

A autonomia ideal para um sistema é de ao menos 15 minutos, o que em geral será suficiente para terminar algo mais urgente e salvar tudo antes de desligá-lo.

Muitos no-breaks vêm com a possibilidade de gerenciamento, através de interfaces inteligentes. Nestes casos, ligando o no-break a uma das saídas do micro (normalmente serial) e instalando o software que o acompanha, você poderá programar o no-break para que salve os documentos e desligue o micro automaticamente no caso de corte de energia.

3.1.4.2 SISTEMAS REDUNDANTES

3.1.4.2.1 HOT-SWAP

Figura 3 : Modulo com tecnologia Hot-swap

Hot-swap é uma tecnologia muito usada em servidores de rede. Ela permite a troca de dispositivos SCSI com o micro ligado, como, por exemplo, discos rígidos. Se o disco rígido do servidor queima, o técnico pode substituir o disco sem a necessidade de desligar e abrir o micro.

3.1.4.2.2 RAID

RAID (Redundant Arrays of Independent Disks - Matrizes Redundantes de Discos Independentes) é uma tecnologia consagrada que oferece capacidade, confiabilidade, alto desempenho e economia no armazenamento de dados on-line. Muito superior a discos

magnéticos, o sistema RAID é de ampla utilização em todo o espectro da indústria de computação, desde o PC até o mainframe. O sistema RAID gerencia um conjunto de discos, mas aparece ao usuário como um único disco grande. A vantagem dos discos múltiplos é que, em caso de falha, os dados são transferidos para um disco próximo e o sistema continua trabalhando, sem perda de dados. A disponibilidade dos dados também é mais rápida. Os múltiplos discos de um sistema RAID podem ser varridos simultaneamente. A procura em um único disco grande demoraria muito mais. A transferência de dados de RAID para RAID também é mais rápida, porque os discos podem ser acessados simultaneamente. A manutenção também é mais fácil com o RAID, e a tolerância de falhas, mais alta. Cada disco pode ser substituído enquanto o sistema trabalha. Com essa capacidade de "hot-swap", os administradores de rede podem economizar tempo e evitar possíveis problemas antes que eles coloquem a operação do sistema em perigo. Há vários níveis ou tipos de RAID para acomodar necessidades diferentes de armazenamento:

RAID 1 - Este nível tem discos duplicados trabalhando lado a lado, em "espelhamento de discos" paralelo. A confiabilidade do sistema é muito mais alta. Se um disco falhar, o outro pode fornecer quaisquer dados necessários. Entretanto, apenas 50% da capacidade do drive está disponível para armazenamento.

RAID 2 - Não é usado por não ser compatível com os drives atuais.

RAID 3 - Este nível usa o striping de dados e um drive de paridade dedicado. Quando os dados são escritos na matriz, um byte vai para cada disco. Cada drive é acessado ao mesmo tempo. A vantagem é uma transferência de dados muito mais alta. A desvantagem é que, como cada drive é usado, apenas uma transação de I/O pode ser processada de cada vez. O RAID 3 é o melhor para grandes requisições de dados.

RAID 4 (RAID 0) - Neste nível, os blocos de dados são divididos ao longo da matriz de discos e, portanto, os discos podem ser acessados em paralelo. O RAID 4 tem uma taxa de I/O maior que o RAID 3, mas a transferência de dados é mais lenta. Os drivers de paridade podem ser utilizados para dar tolerência a falhas do drive de dados. O RAID 4 sem paridade é conhecido como RAID 0.

RAID 5 - De modo diferente do RAID 3, que acessa todos os drivers ao mesmo tempo para a mesma leitura ou escrita, o RAID 5 pode acessar tantos drives quanto possível para leituras e escritas diferentes. Como resultado, oferece a maior taxa de I/O de todos os níveis de RAID.

3.1.4.2.3 FONTE COM REDUNDÂNCIA

Figura 4: Exemplo de fonte redundante.

Este equipamento consiste em 2 módulos de potência projetados para trabalhar de modo a que se um dos módulos falhar o outro continue, garantindo que o computador mantenha o funcionamento mesmo em caso de falha de um dos módulos da fonte.

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança é a formalização de todos os aspectos considerados relevantes por uma organização para proteção, controle e monitoramento de seus recursos computacionais. Também deve ser vista como um canal de comunicação entre usuários e o comitê Corporativo de Segurança da Informação. A documentação gerada precisa explicar a importância da segurança para motivar as pessoas envolvidas a praticá-la.

A divulgação da política de segurança é uma das ferramentas responsáveis pelo sucesso da sua implantação. Seu objetivo é disseminar a política de segurança da informação na empresa, conscientizando os colaboradores e prestadores de serviço para a política de segurança que está sendo implantada.

Deverão ser desenvolvidas palestras de conscientização, cartas, e-mails, cartilhas e eventos objetivando o sucesso da implantação.

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa

informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham.

Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos àqueles que a descumprem.

Antes que a política de segurança seja escrita, é necessário definir a informação a ser protegida. Usualmente, isso é feito através de uma análise de riscos, que identifica:

- Recursos protegidos pela política;
- Ameaças às quais estes recursos estão sujeitos;
- Vulnerabilidades que podem viabilizar a concretização destas ameaças, analisando-as individualmente.

Uma política de segurança deve cobrir os seguintes aspectos:

- Política de senhas;
- Direitos e responsabilidades dos usuários;
- Direitos e responsabilidades do provedor dos recursos;
- Ações previstas em caso de violação da política.

5 INSTALAÇÃO DE UM SISTEMA SEGURO

5.1 INSTALAÇÃO

Um sistema mais seguro começa pela instalação do mínimo possível de pacotes e componentes, especialmente os que implementam serviços de rede. Este mínimo depende fundamentalmente do propósito do sistema em questão e do ambiente de rede no qual ele está inserido. Por exemplo, em princípio um sistema dedicado a servir páginas Web não precisa de um software servidor SMTP, assim como uma estação de trabalho não precisa de um servidor HTTP.

A justificativa para esta recomendação é bastante simples. É comum que serviços não utilizados não sejam monitorados por falhas de segurança, o que aumenta a possibilidade de

não ser aplicada uma correção necessária. A redução no número de pacotes instalados diminui a chance de que o sistema possua uma vulnerabilidade que possa vir a ser explorada por um atacante.

5.2 DESATIVAÇÃO DE SERVIÇOS NÃO UTILIZADOS

Após a instalação a primeira precaução a ser tomada deve ser a verificação se tudo o que está instalado na maquina é realmente necessário, existem programas aos quais por padrão já ativam alguns serviços aos quais não fazemos uso, e cabe ao administrador a localização destes serviços e a desativação e se possível a até remoção dos mesmos.

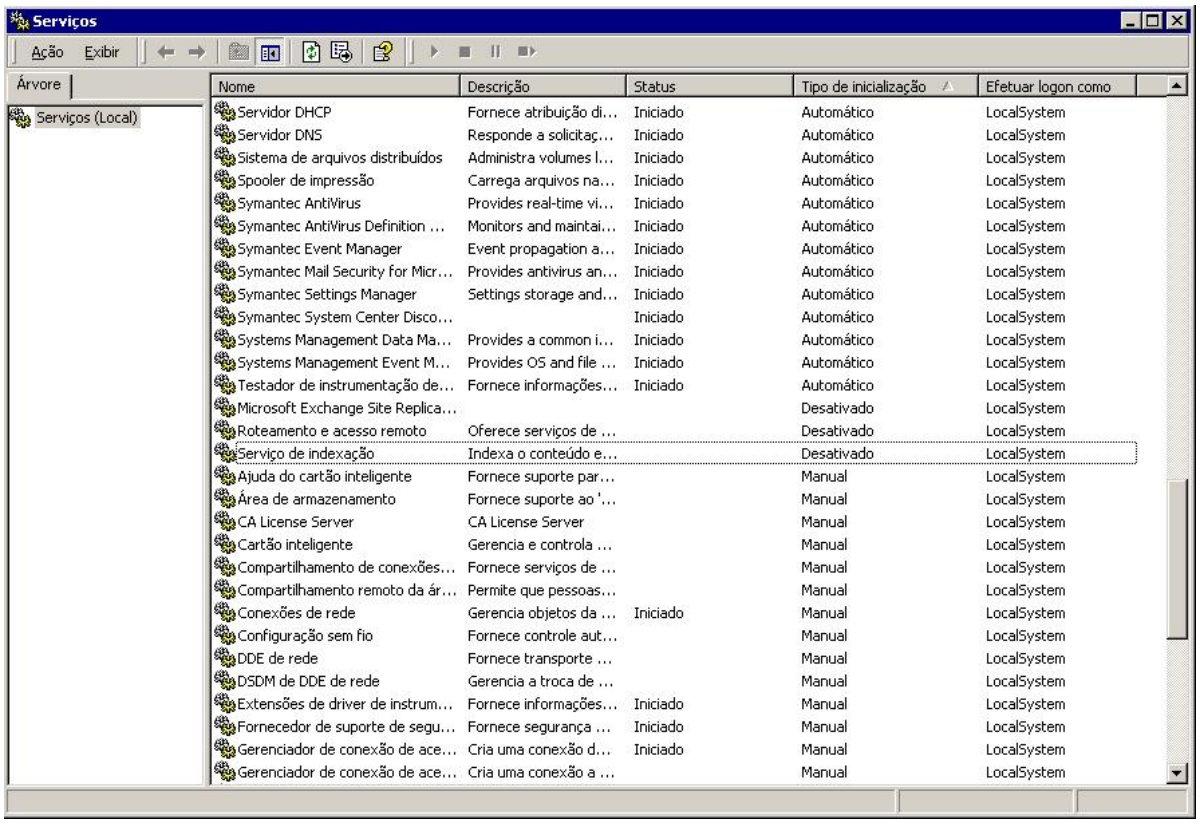

Figura 5: Exemplo da tela de serviços carregados no Windows 2000 Server

5.3 INSTALAÇÃO DE CORREÇÕES

Depois de um sistema ter sido corretamente instalado e configurado, é necessário verificar se não existem correções (patches, fixes, service packs) para vulnerabilidades conhecidas nos componentes instalados. A maioria dos fornecedores de software libera

correções para problemas de segurança que sejam descobertos em um sistema, sem que se tenha de esperar pela sua próxima versão. Na maioria das vezes, estas correções estão disponíveis através da Internet.

A instalação de correções deve ser realizada não só como parte da instalação inicial do sistema, mas também durante o seu tempo de vida, a intervalos periódicos ou sempre que surgirem vulnerabilidades que o afetem.

No Windows temos a opção chama Windows Update, ferramenta a qual busca automaticamente todas as atualizações as quais ainda não foram instaladas.

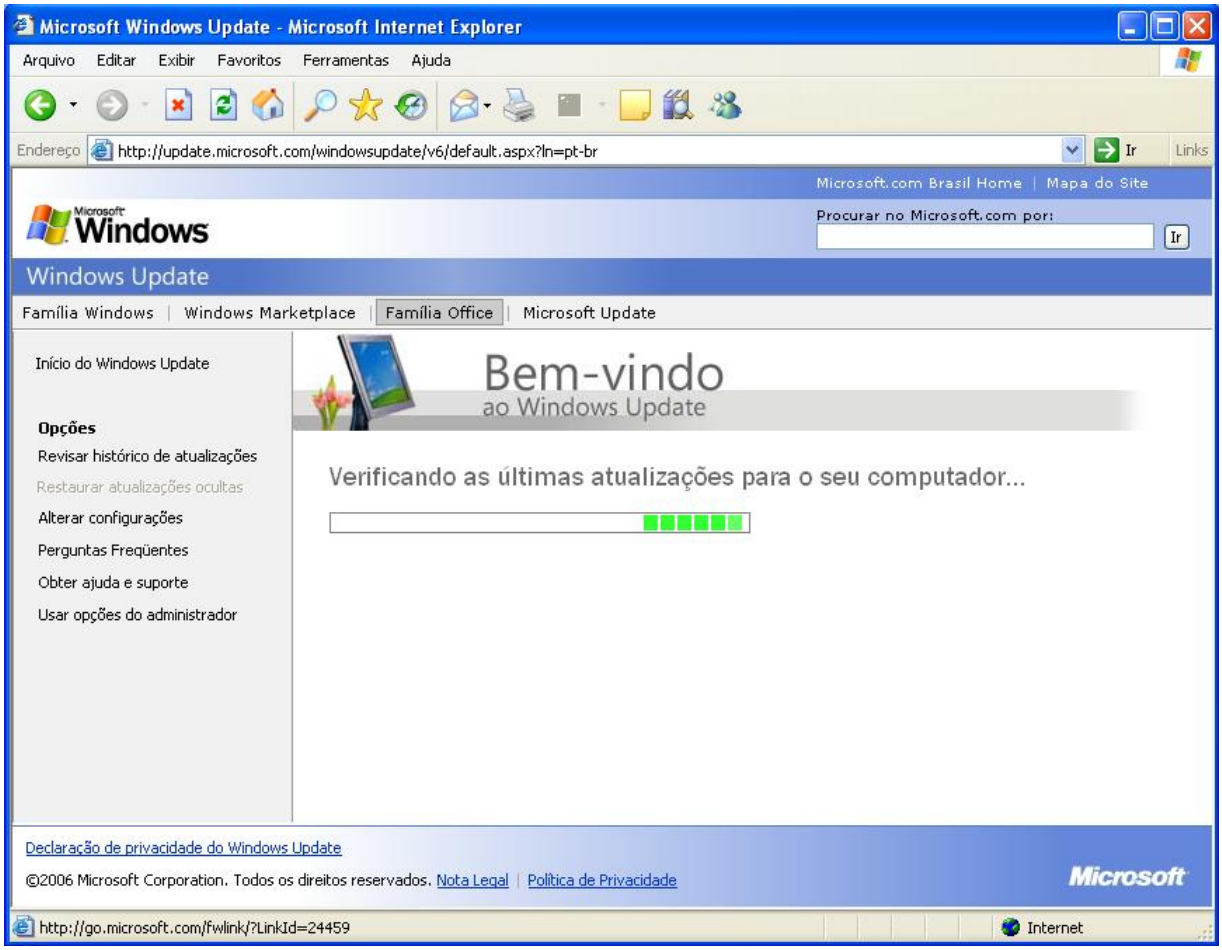

Figura 6: Windows Update em funcionamento

No Linux temos uma ferramenta chamada APT (Advanced Package Tool) com esta ferramenta você pode instalar, remover, reconfigurar e também atualizar pacotes. Num entanto o APT ao contrario do windows update que é praticamente todo automático, deve ser

configurado para saber de onde pegar os pacotes. Para executar esta configuração devemos executar o comando apt-setup ou podemos editar manualmente o arquivo /etc/apt/sources.list.

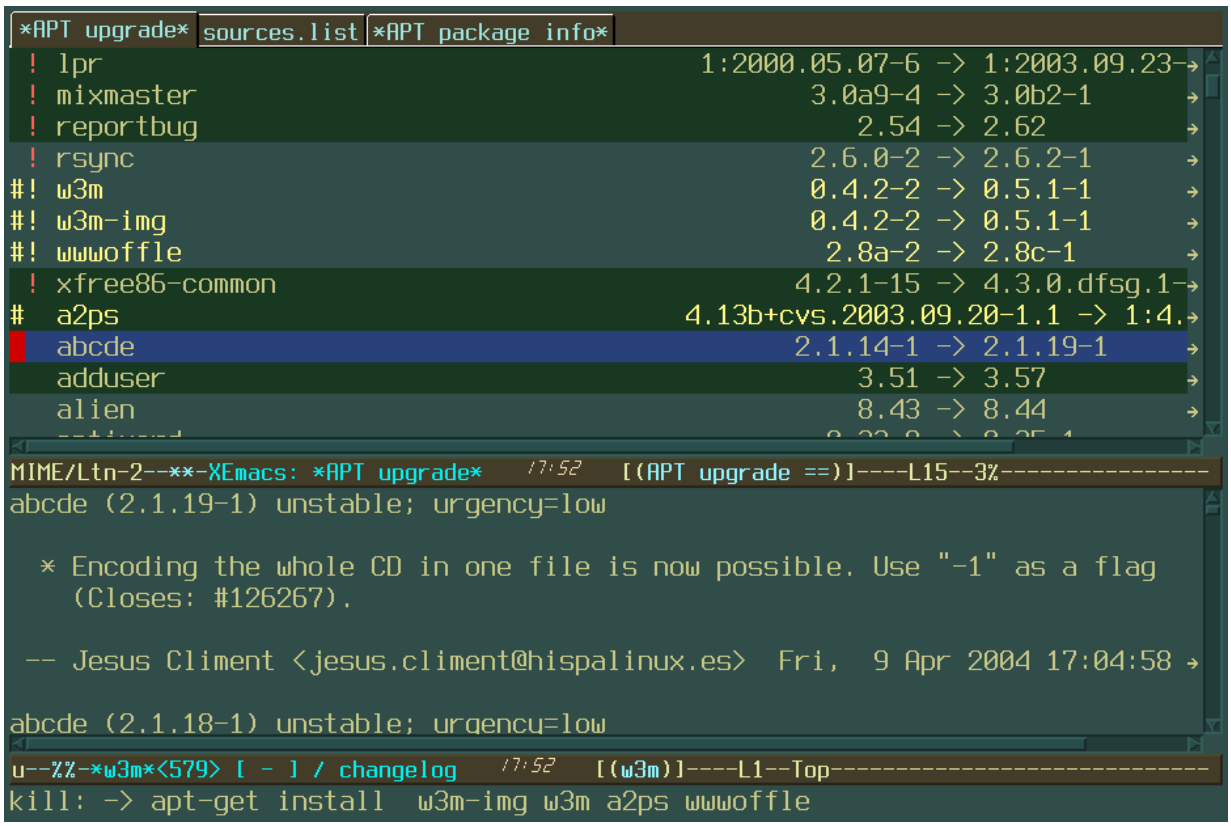

Figura 7 : APT em funcionamento

5.4 GERAÇÃO DE LOGS

Logs são muito importantes para a administração segura de sistemas, pois registram informações sobre o seu funcionamento e sobre eventos por eles detectados. Muitas vezes, o log é o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento fora do esperado pelo sistema.

Daily Traffic Type Report

Home Index Mon, May 15 2006 « Prev Report

Traffic Type by Protocol			
Protocol	Incoming (bytes)	Outgoing (bytes)	Total (bytes)
mail	262,966,330	186,929,863	449,896,193
http	172,092,557	126,605,627	298,698,184
squid	230,996,566	35,897,939	266,894,505
UDP	16,819,266	45,884,659	62,703,925
https	3,144,023	8,856,139	12,000,162
TCP	3,595,891	2,479,915	6,075,806
ICMP	637,662	1,721,583	2,359,245
NetBios	243,327	264,662	507,989
socks	340,324	122,181	462,505
ftp-data	14,174	436,497	450,671
FastTrack	322,414	37,440	359,854
pop3	116,692	110,464	227,156
napster	4,574	3,898	8,472
telnet	1,402	1,146	2,548
snmp	770	1,610	2,380
ssh	1,250	1,030	2,280
UT	122	66	188
other	0	1,680	1,680
TOTAL	691,297,344	409,356,399	1,100,653,743
Elapsed time is 3 seconds.			

Figura 8: Exemplo de Log obtido em servidor de internet

6 AMEAÇAS A QUE ESTAMOS EXPOSTOS

Para conseguirmos nos defender das ameaças às quais estamos expostos, primeiramente devemos conhecê-las, assim teremos mais chances de conseguirmos obter melhores resultados nesta luta por maior segurança.

As principais ameaças a que estamos expostos seriam os vírus, trojans, worms, hackers.

6.1 VÍRUS

6.1.1 CARACTERÍSTICAS

O que comumente chamamos de "vírus de computador" são programas que possuem algumas características em comum com os vírus biológicos:

- São pequenos;

- Um vírus, por definição, não funciona por si só. Deve infectar um arquivo executável ou arquivos que utilizam macros, ou seja, em geral o vírus fica escondido dentro da série de comandos de um programa maior;

- Contém instruções para parasitar e criar cópias de si mesmo de forma autônoma e sem autorização específica (e, em geral, sem o conhecimento) do usuário para isso - eles são, portanto, auto replicantes.

6.1.2 A INFECÇÃO

Há várias manifestações visíveis da atividade dos vírus: mostrar mensagens, alterar ou deletar determinados tipos de arquivos, corromper a tabela de alocação, diminuir a performance do sistema ou até formatar o disco rígido.

Muitas vezes a ação de um vírus só se inicia a partir de eventos ou condições que seu criador pré-estipulou: atingir certa data, um número de vezes que um programa é rodado, um comando específico ser executado, etc.

Um vírus pode atingir um computador a partir de diferentes "vetores" todos previamente infectados: documentos, programas, disquetes, arquivos de sistema, etc.

Arquivos executáveis (_.exe. _.bat, _.com) são particularmente perigosos e deve-se evitar enviá-los ou recebê-los. Após infectar o computador, eles podem passar a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, o vírus vai junto e, quando for executado irá contaminar a segundo máquina.

Arquivos de dados, som (_.wav, _.mid), imagem (_.bmp, _.pcx, _.gif, _.jpg), vídeo (_.avi, _.mov) e os de texto que não contenham macros (_.txt, _.wri) podem ser abertos sem problemas.

Mas, tanto o download (cópia de programas, via http ou ftp) como o serviço de correio eletrônico (e-mail), possibilitam a entrada de arquivos no computador. Assim, a

internet tornou-se um grande foco de disseminação de vírus, worms, trojans e outros programas maliciosos, por facilitar em muito o envio e recepção de arquivos (o que antes era feito basicamente por meio de disquetes).

Como um dos mais populares serviços da Internet é o correio eletrônico, o envio de programas invasores por e-mail é preocupante.

Como regra geral pode-se assumir que não devemos executar arquivos recebidos, especialmente os arquivos executáveis, mesmo que se conheça o remetente e que se tenha certeza que ele é cuidadoso e usa antivírus atualizado.

Mas, na quase totalidade dos casos pode-se admitir que a simples recepção e a visualização de uma mensagem não contaminam o computador receptor.

Figura 9: Exemplo de e-mail com link para um vírus

6.1.3 TIPOS DE VÍRUS

6.1.3.1 VÍRUS DE BOOT (MASTER BOOT RECORD / BOOT SECTOR VIRUSES)

Todos os discos e disquetes possuem uma área de inicialização reservada para informações relacionadas à formatação do disco, dos diretórios e dos arquivos nele armazenados (registro mestre do Sistema, o Master Boot Record - MBR dos discos rígidos ou a área de boot dos disquetes - Boot Sector).

Como essa área é executada antes de qualquer outro programa (incluindo qualquer programa Antivírus), esses vírus são muito bem sucedidos. Para esse sucesso também contribui o fato da infecção poder ocorrer por meio de um ato simples do usuário: esquecer um disquete contaminado dentro do drive A.

Como todos os discos possuem também um pequeno programa de boot (que determina onde está ou não o sistema operacional e reconhece, inclusive, os periféricos instalados no computador), os vírus de boot podem se "esconder" em qualquer disco ou disquete.

A contaminação ocorre quando um boot é feito através de um disquete contaminado. O setor de boot do disquete possui o código para determinar se um disquete é "bootável" ou para mostrar a mensagem: "Disquete Sem Sistema ou Erro de Disco". É este código, gravado no setor de boot que, ao ser contaminado, assume o controle do micro. Assim que o vírus é executado ele toma conta da memória do micro e infecciona o MBR do disco rígido.

A disseminação é fácil: cada disquete não contaminado, ao ser colocado no drive e ser lido pode passar a ter uma cópia do código e, nesse caso, é contaminado e passa a ser um "vetor".

6.1.3.2 VÍRUS DE PROGRAMA (FILE INFECTING VIRUSES)

Os vírus de programa infectam - normalmente - os arquivos com extensão.exe e.com (alguns contaminam arquivos com outras extensões, como os .dll, as bibliotecas compartilhadas e os .ovl). Alguns deles se replicam, contaminando outros arquivos, de maneira silenciosa, sem interferir com a execução dos programas que estão contaminados. Assim sendo, pode não haver sinais perceptíveis do que está acontecendo no micro.

Alguns dos vírus de Programa vão se reproduzindo até que uma determinada data, ou conjunto de fatores, seja alcançado. Somente aí é que começa a sua ação.

A infecção se dá pela execução de um arquivo já infectado no computador. Há diversas origens possíveis para o arquivo infectado: Internet, Rede Local ou um disquete.

6.1.3.3 VÍRUS MULTIPARTITE

É uma mistura dos tipos de boot e de programa, podendo infectar ambos: arquivos de programas e setores de boot. São mais eficazes na tarefa de se espalhar, contaminando outros arquivos e/ou discos e são mais difíceis de serem detectados e removidos.

6.1.3.4 VÍRUS DE MACRO

Quando se usa alguns programas, por exemplo um editor de texto, e necessita-se executar uma tarefa repetidas vezes em seqüência (por exemplo, substituir todos os "vc" por "você") pode-se editar um comando único para efetuá-las. Esse comando é chamado de macro, que pode ser salvo em um modelo para ser aplicado em outros arquivos.

Além dessa opção da própria pessoa fazer um modelo os comandos básicos dos editores de texto também funcionam com modelos. Os vírus de macro atacam justamente esses arquivos comprometendo o funcionamento do programa. Os alvos principais são os próprios editores de texto (Word) e as planilhas de cálculo (Excel).

A disseminação desse tipo de vírus é muito mais acentuada pois documentos são muito móveis e passam de máquina em máquina (entre colegas de trabalho, estudantes, amigos e outras pessoas). Ao escrever, editar ou, simplesmente, ler arquivos vindos de computadores infectados a contaminação ocorre. Assim, verdadeiras "epidemias" podem acontecer em pouco tempo.

Além disso, os macrovírus constituem a primeira categoria de vírus multiplataforma, ou seja, não se limitam aos computadores pessoais, podendo infectar também outras plataformas que usem o mesmo programa, como o Macintosh, por exemplo.

Um outro agravante em relação a esses vírus é a facilidade de lidar com as linguagens de macro, dispensando que o criador seja um especialista em programação. Isso acarretou no desenvolvimento de muitos vírus e inúmeras variantes e vírus de macro, num período curto de tempo.

6.1.3.5 OUTRAS CAPACIDADES

Para tentar impedir a detecção pelos antivírus algumas capacidades foram dadas a qualquer um dos tipos de vírus acima. Assim, cada um desses três tipos de vírus podem ter outras características, podendo ser:

6.1.3.5.1 POLIMORFISMO

Têm como principal característica o fato de estar sempre em mutação, ou seja, esse vírus muda ao criar cópias dele mesmo, alterando seu código. Mas, os clones são tão funcionais quanto seu original, ou mais. O objetivo da mudança é tentar dificultar a ação dos antivírus, criando uma mutação, algo diferente daquilo que a vacina procura.

6.1.3.5.2 INVISIBILIDADE

Têm a capacidade de, entre outras coisas, temporariamente se auto remover da memória, para escapar da ação dos programas antivírus.

6.1.3.5.3 ENCRIPTAÇÃO

Nesses é muito difícil a ação da vacina. Assim mesmo que seja detectado o antivírus vai ter grande problema para removê-lo.

6.2 TROJAN (CAVALOS DE TRÓIA)

O vírus do tipo Trojan tipicamente se disfarça como algo desejável — por exemplo, um programa legítimo. Assim como seu equivalente histórico, porém, ele guarda um poder de ataque oculto. O Trojan geralmente não se replica (embora pesquisadores tenham descoberto Trojans replicantes). Ele espera até que aconteça o evento de gatilho e então mostra uma mensagem ou destrói arquivos ou discos. Como ele geralmente não se replica, alguns pesquisadores não classificam os Trojan Horses como vírus.

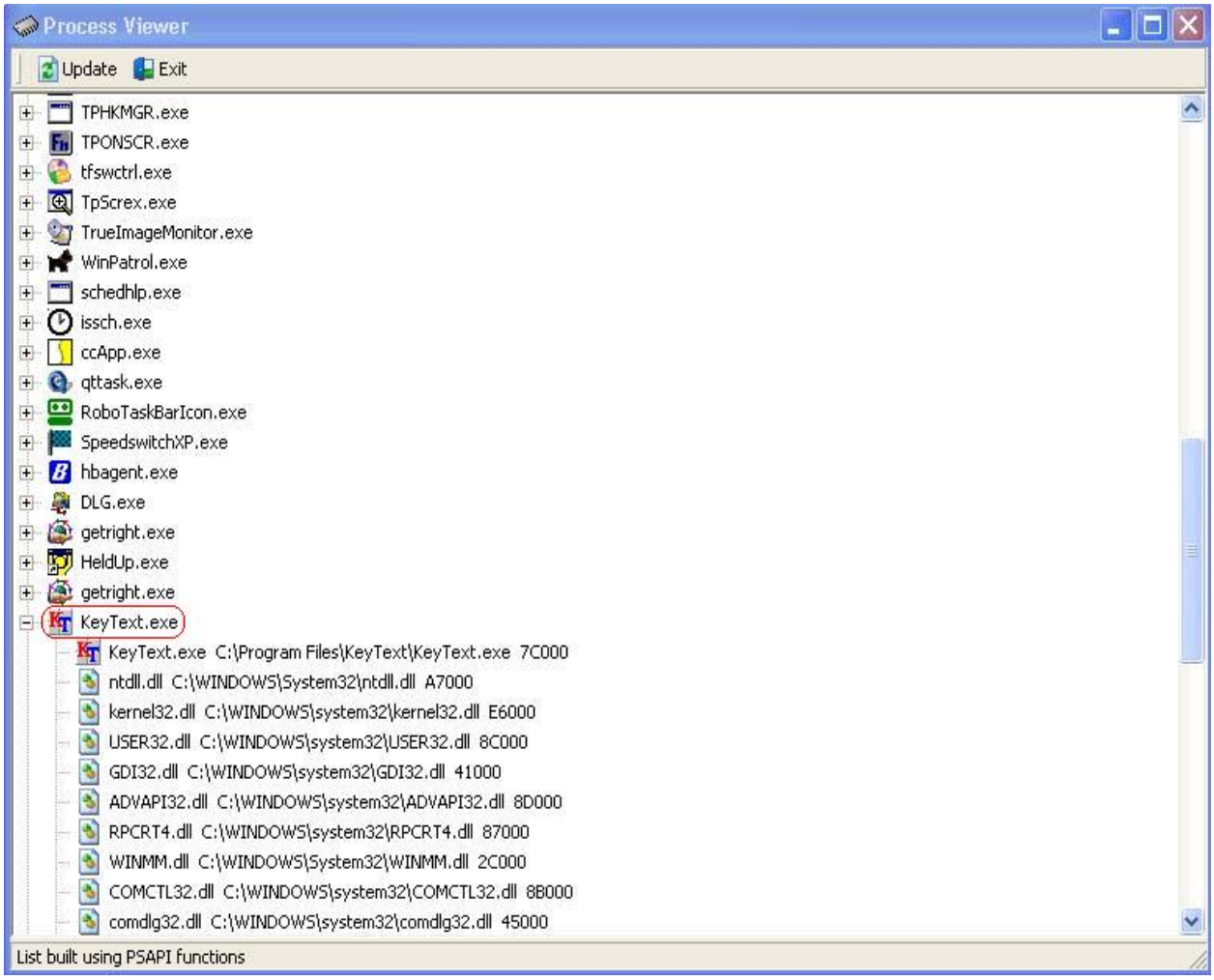

Figura 10: Exemplo de Trojan

6.3 WORMS (VERMES)

O worm é um programa projetado para se copiar rapidamente de um computador para outro, através de alguma mídia de rede: e-mail, TCP/IP, etc. De acordo com Cary Nachenburg, Pesquisador Chefe no Symantec AntiVirus Research Center (SARC, Centro de Pesquisas Antivírus), “Worms são insidiosos porque eles pouco dependem (ou não dependem) do comportamento humano para se espalhar de um computador para outro.”

A maioria dos vírus, dependem de algum tipo de gatilho do usuário, como abrir um anexo, reinicializar uma máquina, ou executar um programa. Worms, no entanto, são capazes de funcionar de forma mais independente. Um exemplo disto é o vírus Explore.zip, que pode identificar programas de e-mail amplamente utilizados, como o MS Outlook, que possam

existir num computador, e sistematicamente começar a enviar cópias de si mesmo para todos na lista de e-mail do usuário.

Além disso, o worm está mais interessado em infectar quantas máquinas forem possíveis na rede, e menos interessado em espalhar muitas cópias de si mesmo em computadores individuais (como os primeiros vírus de computador).

Os worms geralmente são classificados em worms de e-mail ou worms de protocolo, dependendo do vetor primário pelo qual eles se espalham. Ambos os tipos podem ser transferidos, com conhecimento ou não, através da web.

6.4 HACKERS

O perfil típico do hacker é: jovem entre 15 e 25 anos, com amplo conhecimento de redes, conhecimento de programação (geralmente em linguagens como C, C++, Java e Assembler). Contudo, existem diversos tipos de “hackers”, dos que possuem mais experiência para os que apenas “copiam” furos de segurança explorados por outros hackers. São eles:

6.4.1 WHITE-HATS

Os white-hats são os hackers que exploram problemas de segurança para divulgá-los abertamente, de forma que toda a comunidade tenha acesso à informações sobre como se proteger. Desejam abolir a “segurança por obscuridade”, que nada mais é do que tentar proteger ou manter a segurança pelo segredo de informações sobre o funcionamento de uma rede, sistema operacional ou programa em geral. Seu lema é o “full disclosure”, ou conhecimento aberto, acessível a todos.

6.4.2 BLACK-HATS

Ao contrário dos white-hats, apesar de movidos também pela curiosidade, usam suas descobertas e habilidades em favor próprio, em esquemas de extorsão, chantagem de algum tipo, ou qualquer esquema que venha a trazer algum benefício, geralmente, e obviamente, ilícito. Estes são extremamente perigosos e difíceis de identificar, pois nunca tentarão chamar a atenção. Agem da forma mais furtiva possível.

6.4.3 CRACKERS

As denominações para os crackers são muitas. Alguns classificam de crackers, aqueles que têm por objetivo invadir sistemas em rede ou computadores apenas pelo desafio. Contudo, historicamente, o nome “cracker” tem uma relação com a modificação de código, para obter funcionalidades que não existem, ou de certa forma, limitadas. Um exemplo clássico são os diversos grupos existentes na Internet que tem por finalidade criar “patches” ou mesmo “cracks” que modificam programas comerciais (limitados por mecanismos de tempo por exemplo, como shareware), permitindo seu uso irrestrito, sem limitação alguma.

6.4.4 PHREAKERS

Apesar de muitos considerarem um cientista russo chamado Nicola Tesla (que na virada do século realizava experiências assustadoras – até para os dias de hoje – com eletricidade) como o primeiro hacker da história, os primeiros hackers da era digital lidavam com telefonia. Sua especialidade é interferir com o curso normal de funcionamento das centrais telefônicas, mudar rotas, números, realizar chamadas sem tarifação, bem como realizar chamadas sem ser detectado (origem). Com a informatização das centrais telefônicas, ficou inclusive mais fácil e acessível o comprometimento de tais informações. Kevin Mitnick, considerado o maior hacker de todos os tempos, era um ótimo phreaker. Na fase final de sua captura, quando os agentes de governo ajudados pelo Tsutomu Shimomura estavam chegando a um nome, ele conseguia enganar as investigações através do controle que tinha da rede de telefonia da GTE (concessionária telefônica dos EUA).

6.4.5 WANNABES

Os wannabes ou script-kiddies são aqueles que acham que sabem, dizem para todos que sabem, se anunciam, ou divulgam abertamente suas “façanhas”, e usam em 99% dos casos scripts ou exploits conhecidos, já divulgados, denominados “receitas de bolo”, facilmente encontradas em sites como “www.rootshell.com”, ou “xforce.iss.net”. Estes possuem relação direta com a maioria dos usuários da Internet Brasileira. São facilmente encontrados em fórums de discussão sobre o tema, e principalmente no IRC. A maioria não possui escrúpulo algum, portanto, tomar medidas de cautela é aconselhável. Os wannabes

geralmente atacam sem uma razão ou objetivo, apenas para testar ou treinar suas descobertas, o que nos torna, usuários Internet, potenciais salvos.

6.4.6 ALGUNS MÉTODOS DE ATAQUE DOS HACKERS

6.4.6.1 ENGENHARIA SOCIAL

Existe algum método mais rápido e eficiente de se descobrir uma senha? Que tal simplesmente perguntar? Por mais extraordinário que possa parecer, o método mais simples, mais usado e talvez mais eficiente de se recolher informações é simplesmente chegar e perguntar.

Você também poderia subornar, mas dependendo da situação, isto pode lhe custar muito caro, então por que não tentar enganar e obter tais informações? De fato, este método é bastante utilizado, e existem hackers que sabem usá-lo com grande destreza.

Essa tática de ataque é conhecida como “Engenharia Social”. Basicamente, esta é a arte de fazer com que outras pessoas concordem com você e atendam aos seus pedidos ou desejos, mesmo que você não tenha autoridade para tal. Popularmente, pode-se dizer que engenharia social é simplesmente a arte de se contar uma mentira bastante convincente.

Dentro da área de segurança podemos definir engenharia social como a aquisição de informações preciosas ou privilégios de acesso por “alguém de fora”, baseado em uma relação de confiança estabelecida, inapropriadamente, com “alguém de dentro”.

Profissionais utilizam este tipo de aproximação para adquirir informações confidenciais, como organogramas de organizações, números de cartões de crédito e telefone, senhas de acesso, diagrama da rede, etc. com o objetivo de avaliar as vulnerabilidades de uma organização para futuros ataques.

Dizem que o único computador totalmente seguro é aquele desligado da tomada. A arte da engenharia social concentra-se no elo mais fraco da corrente da segurança de computadores: os seres humanos. O simples fato de que se pode facilmente convencer uma pessoa a ligar o computador, torna vulnerável, até mesmo, os computadores desligados.

Na medida em que a parte humana de um sistema de segurança é a mais essencial, não existe computador na face da Terra que não necessite de seres humanos. Isso significa que essa é uma fraqueza universal, independente de plataforma, software, tipo de conexão de rede ou idade do equipamento. Qualquer pessoa com acesso a qualquer parte do sistema,

física ou remota, pode ser uma falha de segurança em potencial. Qualquer informação adquirida pode ser utilizada para um outro ataque de engenharia social. Isso significa que qualquer pessoa, mesmo que não seja considerada integrante da política de segurança pode servir como uma porta de entrada.

Como um ataque de engenharia social pode revelar muitas informações, como se pode tornar um sistema de computadores mais seguro? A resposta é educação e difusão da informação, explicando aos empregados e pessoas ligadas direta ou indiretamente ao sistema a importância de uma política de segurança, evitando assim o ataque de pessoas que poderão tentar manipulá-los para ganhar acesso a informações privadas. Isto já é um excelente começo para tornar segura sua rede ou sistema.

6.4.6.2 DENIAL OF SERVICE (DOS)

Os ataques DoS são bastante conhecidos no âmbito da comunidade de segurança de redes. Estes ataques, através do envio indiscriminado de requisições a um computador alvo, visam causar a indisponibilidade dos serviços oferecidos por ele. Fazendo uma analogia simples, é o que ocorre com as companhias de telefone nas noites de natal e ano novo, quando milhares de pessoas decidem, simultaneamente, cumprimentar à meia-noite parentes e amigos no Brasil e no exterior. Nos cinco minutos posteriores à virada do ano, muito provavelmente, você simplesmente não conseguirá completar a sua ligação, pois as linhas telefônicas estarão saturadas.

Ao longo dos últimos anos, uma categoria de ataques de rede tem-se tornado bastante conhecida: a intrusão distribuída. Neste novo enfoque, os ataques não são baseados no uso de um único computador para iniciar um ataque, no lugar são utilizados centenas ou até milhares de computadores desprotegidos e ligados na Internet para lançar coordenadamente o ataque. A tecnologia distribuída não é completamente nova, no entanto, vem amadurecendo e se sofisticando de tal forma que até mesmo vândalos curiosos e sem muito conhecimento técnico podem causar danos sérios.

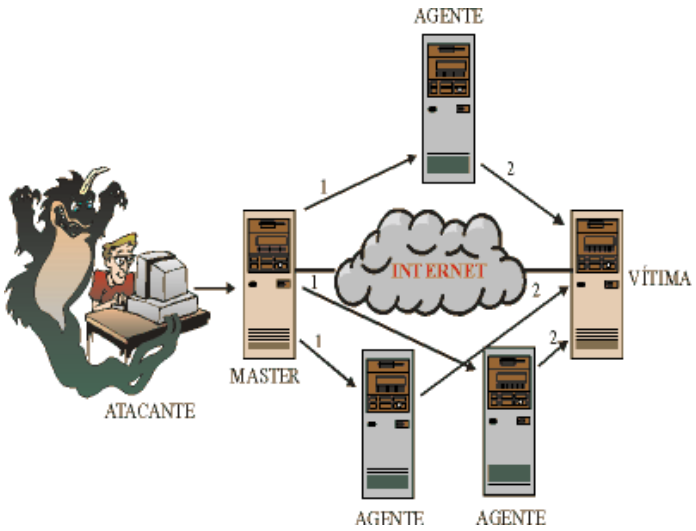

Figura 11 : Diagrama de um ataque DDos

Atacante: Quem efetivamente coordena o ataque.

Master: Máquina que recebe os parâmetros para o ataque e comanda os agentes.

Agente: Máquina que efetivamente concretiza o ataque DoS contra uma ou mais vítimas, conforme for especificado pelo atacante.

Vítima: Alvo do ataque. Máquina que é "inundada" por um volume enormede pacotes, ocasionando um extremo congestionamento da rede e resultando na paralização dos serviços oferecidos por ela.

7 FERRAMENTAS DE AUXILIO A SEGURANÇA

7.1 ANTIVÍRUS

A partir do surgimento dos primeiros vírus de computador e suas conseqüências, começaram a ser desenvolvido em todo mundo diferentes alternativas de prevenção contra estas infecções, recuperando então arquivos infectados ao seu estado original e minimizando os danos causados. Desta forma, começaram a surgir diferentes soluções antivírus com variadas tecnologias. Basicamente podemos concluir que Antivírus é um programa utilizado para descontaminar um computador ou rede que estiver infectado com vírus, worm e códigos maliciosos, bem como fornecer proteção contra novas invasões.

7.1.1 MODO DE DETECÇÃO DOS VÍRUS

Um vírus de computador é igual a qualquer outra aplicação, está composto de uma série de instruções e ao ser executado irá cumprir a ação para qual foi programado.

Um conjunto de instruções que contém o código de malicioso permite sua identificação de maneira única através da forma como é programado. Estes parâmetros constituem o nome de um respectivo vírus.

Algumas soluções antivírus conseguem identificar pequenas alterações no código malicioso original reconhecendo então um vírus modificado.

Algumas empresas antivírus catalogam os vírus individualmente e outras por famílias de vírus, isso faz com que a informação disponibilizada por cada empresa sobre um determinado vírus varie constantemente.

Quando uma solução antivírus detém a tecnologia de detectar um vírus a partir de seu código, pode ocorrer falsos alarmes de detecção, isto é denominado como falso positivo, mais este é um inconveniente necessário, pois esta analise permite detectar vírus desconhecidos quando executados.

Quando uma solução antivírus detecta um vírus a partir de assinatura, é improvável a ocorrência de falsos alarmes ou falso positivo. Mais somente vírus analisados e catalogados são detectados ao serem executados, vírus desconhecidos não são detectados.

7.1.2 PROCESSO DE ATUALIZAÇÃO DO ANTIVÍRUS

O vírus de computador sempre é desenvolvido por um programador inescrupuloso (mal intencionado) que desenvolve esta aplicação maliciosa na maioria das vezes sem um objetivo claro.

Com o surgimento da Internet e seus avançados meios de comunicação que permitem quase que simultaneamente o trafego de qualquer tipo de informação e aplicação, inclusive os vírus.

Um vírus começa a disseminar através da Internet até que seja descoberto (geralmente a partir de seus efeitos), é então analisado pelas empresas de antivírus, são catalogados e então vacinas específicas serão são elaboradas. Todos estes processos são realizados em pouco tempo, é dificilmente ultrapassam horas.

Estas vacinas (atualizações) ficam disponíveis nos servidores das respectivas empresas e seus usuários devem fazer o download dos arquivos necessários mantendo então o antivírus atualizado.

7.1.3 HEURÍSTICA

Pouco tempo depois que surgiram as primeiras soluções antivírus, pode ser observado as limitações no desenvolvimento das analises de vírus através de métodos heurísticos, que se baseiam em complexos algoritmos matemáticos que tentam antecipar as ações que poderiam ocorrer quando um determinado código e executado.

A tecnologia das Analises Heurística implementada por cada solução antivírus, nem sempre tem a mesma eficácia embora todas possui o mesmo objetivo, que é a detecção antecipada de vírus ainda desconhecidos.

7.2 FIREWALL

Firewall é um quesito de segurança com cada vez mais importância no mundo da computação. À medida que o uso de informações e sistemas é cada vez maior, a proteção destes requer a aplicação de ferramentas e conceitos de segurança eficientes. O firewall é uma opção praticamente imprescindível, podendo ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software.

Explicando de maneira mais precisa, o firewall é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e filtragem de dados. A vantagem do uso de firewalls em redes é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

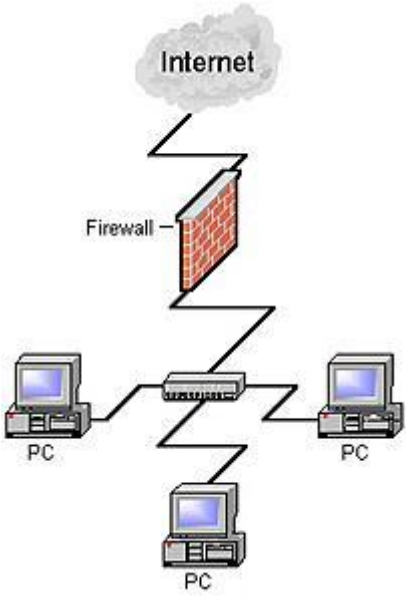

Figura 12 : Ilustração da função de um Firewall

Há mais de uma forma de funcionamento de um firewall, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem dois tipos básicos de conceitos de firewalls: o que é baseado em filtragem de pacotes e o que é baseado em controle de aplicações.

7.2.1 FILTRAGEM DE PACOTES

O firewall que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IPs e dados podem estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados. O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.

Este tipo se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP remoto, endereço IP do destinatário, além da porta TCP usada.

Quando devidamente configurado, esse tipo de firewall permite que somente computadores conhecidos troquem determinadas informações entre si e tenham acesso a

determinados recursos. Um firewall assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.

7.2.2 FIREWALL DE APLICAÇÃO

Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como proxy. Este tipo não permite comunicação direto entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um proxy. Caso não haja, a aplicação simplesmente não funciona.

O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

7.2.3 RAZÕES PARA UTILIZAR UM FIREWALL

A seguir são citadas as 3 principais razões para se usar um firewall:

1 - O firewall pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers;

2 - O firewall é um grande aliado no combate a vírus e cavalos de tróia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados;

3 - Em redes corporativas, é possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram.

7.3 BACKUP

A palavra backup significa cópia de segurança, ou seja, quando fazemos backup estamos criando uma cópia dos arquivos importantes de forma que se ocorrer algum problema nos dados da empresa teremos uma cópia atualizada para restaurar todas as informações danificadas, evitando assim o desperdício de tempo e dinheiro para a recuperação de informações, o que nem sempre é possível, sua re-inclusão e eventual interrupção dos serviços prestados pela empresa por problemas técnicos.

O Backup é a ferramenta de segurança mais importante de seu sistema. Sem o backup, dificilmente temos nosso trabalho recuperado por completo em caso de perda dos dados do disco rígido. É recomendado que o backup seja realizado, pelo menos, uma vez por semana e, em casos de informações importantes, uma vez por dia.

O Winchester/HDD é um dos componentes mais sensíveis do computador, por isso, quando ocorrem quedas ou picos de energia elétrica ele pode ser danificado impedindo recuperação das informações.

Quando um programa qualquer (ICQ ou antivírus, por exemplo) é instalado em um computador, ele pode modificar a estrutura de outros arquivos importantes (como arquivos do sistema operacional, por exemplo) de modo, que ele possa ser executado. Esta alteração pode comprometer o bom funcionamento do computador, danificar arquivos existentes ou provocar a perda de informações importantes.

Existem três possibilidades de perda de dados, falhas técnicas, ambientais e humanas:

- **Falhas técnicas:** falha no subsistema de disco rígido (HD), falha de energia (resultam em dados corrompidos), sobrecarga na rede de computadores que podem gerar falhas de comunicação (resultam em dados corrompidos), falha de software nos sistemas.
- **Falhas ambientais:** descargas elétricas provindas de raios, enchentes.
- **Falhas humanas:** detém 84% das perdas de dados e são devidas à exclusão ou modificação de dados acidental ou mal-intencionada, vírus, roubo de equipamentos e sabotagem.

8 CONCLUSÃO

Todos precisam ter consciência que os computadores quando interligados, são uma porta aberta para o mundo, com a agravante de não se poder ver quem o está olhando. Quem compartilha um universo tão diversificado, deveria, independentemente de qualquer coisa, prevenir-se contra surpresas desagradáveis.

Todos morreremos um dia, uns mais cedo e outros mais tarde. Esta variação de tempo de vida tem muitas influências como: qualidade de vida, localização de moradia, alimentação saudável, prática de esportes, uso de drogas, acidentes, etc. Os sistemas também irão parar de funcionar (crash), esta também é sua tendência natural, devido à influências do meio em que se encontra, má utilização do software, má construção do software (componentes internos, atualizações de versões). Porém isto pode ser prevenido com o auxílio de sistemas antivírus, sistemas firewall (anti-invasão), sistemas de backup, política de segurança, etc.

Não haverá nunca um sistema com falha zero, isto é fato. Pela própria natureza humana no mundo real, até onde conhecemos atualmente não existe ser humano imortal, bem como na natureza binária, no mundo digital. A “segurança da informação” é ponto chave para a estabilidade das empresas e continuidade de seus negócios, e desde os primórdios, onde nem se pensava em computação já existia o dito que “prevenir é melhor que remediar”, portanto, a prevenção contra ameaças digitais nunca é demais, quando se trata de usuários domésticos ou principalmente grandes corporações.

Este trabalho contribuiu muito para meu desenvolvimento profissional, tive a oportunidade de adquirir conhecimentos que com certeza serão muito úteis na minha vida profissional.

9. BIBLIOGRAFIA

THOMAS A. WADLOW, Segurança de Redes - Projeto e gerenciamento de redes seguras Editora Campus - Ano 2000.

ROLF JESS FURSTENAU, Programa de Pós graduação em informática na educação (http://penta2.ufrgs.br/edu/tutorialvirus/virus.swf) - Tutorial sobre os vírus.

MÓDULO SECURITY, O Protal do Profissional da Segurança da Informação (http://www.modulo.com.br).

SYMANTEC CORPORATION; (http://www.symantec.com).

GIORDANI RODRIGUES, InfoGuerra; Segurança e Privacidade (http://www.infoguerra.com.br).

SECURITY FOCUS; (http://www.securityfocus.com).

REDE NACIONAL DE ENSINO E PESQUISA; (http://www.rnp.br/)

EMERSON ALECRIM, Portal Info Wester; (http://www.infowester.com)