SEGURANÇA NA WEB

Centro Brasileiro
de
Pesquisas Físicas

Marita Maestrelli Email: marita@cbpf.br
Bernardo Trovão Email: bernardo@cbpf.br
Fernanda Jannuzzi Email: fernanda@cbpf.br

Prefácio

Uma rede local conectada a Internet exige a implementação de várias normas de segurança. Com o surgimento da Internet comercial, o acesso aos detalhes sobre falhas de segurança em qualquer aplicação ficou muito mais fácil.

Segurança tem se tornado uma das principais atribuições dos administradores de redes, pois a cada dia surgem novos vírus e vulnerabilidades são descobertas nos diversos sistemas de rede.

Esta Nota Técnica é uma introdução a segurança na *World Wide Web*, abordando desde o protocolo primário utilizado na Internet (*TCP/IP*), até as estatísticas das pixações feitas nos sites mundiais.

Esta é a primeira das Notas Técnicas que abordarão o tema **Segurança**, e derivou do projeto de Vocação Científica do aluno Bernardo do CAP/UFRJ.

ÍNDICE

INTRODUÇÃO

Atualmente as empresas e instituições que integraram à internet têm enfrentado uma série de problemas relacionados a segurança de seus *Web Servers*, que são as máquinas que oferecem o serviço de HTTP para determinada rede.

Isto é decorrente do crescimento descontrolado da *Web*. Explicaremos no decorrer desta nota técnica de que maneira estes *Web Servers* podem permanecer mais seguros.

Existem uma série de *Servers* (servidores) disponíveis no mercado, apresentaremos dois dos principais com algumas das características relativas à parte de segurança, assim como, o tipo de plataforma que operam, além de algumas sugestões de configuração destes servidores.

Será explicado de maneira geral como as informações trafegam na rede, o perfil de um invasor, as falhas mais comuns na configuração de um Web Server, e dos protocolos utilizados para enviar, receber e intermediar as relações servidor/cliente (usuário).

2-COMUNICAÇÃO NA INTERNET

2.1-TCP/IP -(TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)

É um padrão de comunicação que reúne um conjunto de protocolos tais como *tcp, ip, ftp (file tranfer protocol), telnet, icmp, arp e nfs.*

As informações que trafegam na rede necessitam do *TCP/IP*, por isso ele é utilizado como protocolo primário da rede na internet.

Este protocolo foi dividido em "camadas" bem definidas, cada uma realizando sua parte na tarefa de comunicação (aplicação, transporte, rede, e físico). Este modelo tem a seguinte vantagem: por ter os processos de comunicação bem definidos e divididos em cada camada, qualquer alteração poderá ser feita isoladamente, não precisando reescrever todo o protocolo.

O *TCP/IP* tem como principal característica a transmissão de dados em máquinas que diferem em suas arquiteturas .

Estas são as camadas que compõem o modelo *TCP/IP*.

Aplicação
Transporte
Rede
Físico

-APLICAÇÃO

Nesta camada são necessários protocolos de transporte para garantir o funcionamento das aplicações reais (*DNS, WWW, SMTP, POP, NFS, FTP).*

Esta camada trabalha com a porta a qual esta ligada a aplicação.

Ex: *FTP* (porta 21), *HTTP* (porta 80), *Telnet* (porta 23), etc.

-TRANSPORTE

Utiliza dois protocolos para a comunicação *Host-to-Host (TCP/UDP).*
Esta camada também tem como função organizar e controlar o fluxo de dados transmitidos para que o protocolo não se perca no meio de tantos pacotes.

-REDE

A camada chamada de rede ou Internet, tem como principal função direcionar os dados aos seus respectivos endereços. Esta característica é chamada de roteamento, que também tem como vantagem evitar o congestionamento da rede, pois trabalha com endereço *IP* de origem e destino.

-FÍSICA

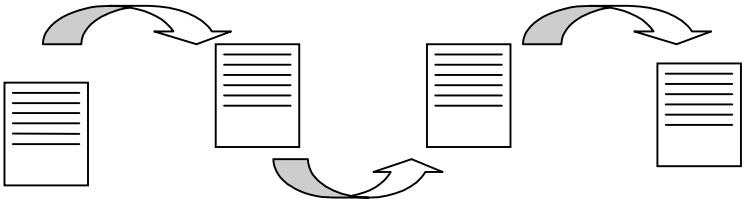
Esta camada está com o seu funcionamento baseado na placa de rede, que dependendo do meio em que está funcionando trabalhará com diferentes padrões.

2.2- A APLICAÇÃO WWW

2.2.1 – DEFINIÇÃO

World Wild Web ou *Web* é o nome dado a todos os documentos *HTML* depositados nos servidores *HTTP* interconectados a internet. Esses documentos assim como os *links* que os compõem, formam uma "teia" (*web)* de informações.

(fig. 1)



A *Web* foi desenvolvida em 1989 e liberada em 1991 por seus criadores no *CERN (European Laboratory for Particle Physics)* com o objetivo de compartilhar os arquivos dos usuários de modo mais gráfico.

Os visualizadores gráficos são utilizados para carregar páginas na Internet. É o que chamamos de *browser* ou navegador. Podemos citar diversos exemplos de navegadores como o *Netscape, Internet Explorer* e até mesmo o pioneiro deles, o *Mosaic*.

Com o crescimento explosivo da *We*b, houve a necessidade de aumentar as técnicas utilizadas para a navegação, logo, falhas foram ficando mais claras e públicas. Com isso o *WWW* começou a ser um freqüente alvo de invasões realizadas por piratas da rede. Essas invasões podem ser motivadas por exemplo, com algum descuido na hora de configurar um servidor *web*; ou causado pela inexperiência de alguns programadores das linguagens para *WWW (Perl, Java, Java Script, Asp),* que cometem erros sutis em suas programações, gerando aberturas que facilitam o trabalho do invasor; ou até mesmo falhas dos próprios navegadores que quando são descobertas são bastante exploradas pelos invasores. Isso demora muito a acontecer, e quando a empresa é informada, a mesma providencia um *PATCH* para a correção do problema. Até todo esse processo se desenvolver, demora muito tempo, e os estragos causados neste espaço de tempo, podem ser grandes.

2.2.2 - WEB SERVERS

É um *host* com software apropriado que proporciona serviços web a usuários de uma rede.

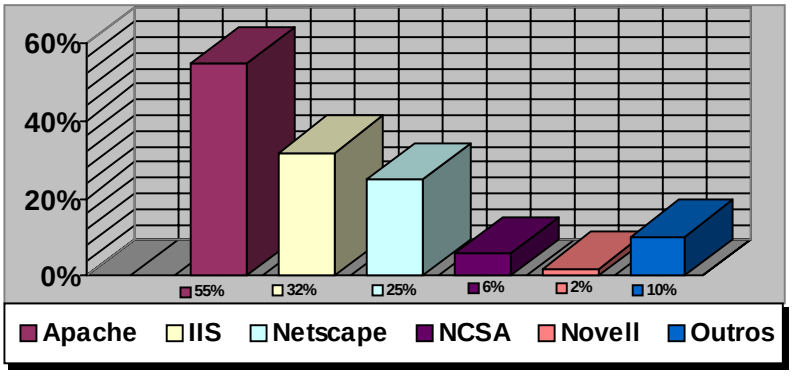
(fig. 2)

Cada Servidor *Web* possui tem características próprias, sendo necessário observar os procedimentos incluídos na documentação de cada um. Entretanto, existem alguns tópicos comuns a qualquer servidor *Web* que permitem configurar os ambientes particulares de cada instalação. Alguns desses tópicos referem-se a especificações do tipo:

- A pasta ou diretório raiz do Servidor.
- A pasta ou diretório onde vão residir os *scripts*, ou programas executáveis.
- A pasta ou diretório onde os documentos (textos *HTML*) e figuras estão.
- Número máximo de processos e usuários simultaneamente.
- Os "alias" para identificar, dentro dos programas, os componentes e recursos do Servidor, sem necessidade de saber o verdadeiro nome deles.
- O nome default da página inicial, ou *Home Page*.
- As opções de *Log* e segurança.
- Os filtros incorporados ao servidor.
- A estrutura de permissões e privilégios do Servidor.

Cada tipo de plataforma necessita de um *web server* específico

Existem inúmeros servidores *web*, no entanto apenas cinco se destacam realmente o Apache, *IIS*, Netscape, NCSA e Novell . Na figura 3 observa-se a utlização deles na Internet. No apêndice 1, enumeramos vários *Web Servers* e as plataformas que eles atuam.



(fig. 3)

Abordaremos nesta nota técnica os dois *Web Servers* mais utilizados. APACHE e IIS.

-APACHE

O APACHE é o melhor e mais popular *web server* no mundo. Muitos *sites* na *Internet* o usam e isso se dá pela sua grande segurança e excelente desempenho. Até mesmo em sua versão *Windows*, ele pode ser usado para fazer grandes servidores. A tabela abaixo está mostrando a relação entre grandes instituições e os servers utilizados.

Servidor	***Instituição***
Apache	Javasoft, FBI, Financial Times, O Banco de dados de Cinema, W3 Consórcio, A Família Real, Serviço de Automatização da Biblioteca Universitária de Oxford M.I.T, Universidade de Harvard e a Universidade de Texas em Austin
IIS (Internet Information Server)	Compac, Nasdaq, A Liga de Futebol Nacional, Exxon e Tesco

A principal ameaça aos web server são os programas que procuram por vulnerabilidades nos *servers*, tais como *bugs* ou “portas” que estejam disponíveis para invasão. Estes programas são perigosos principalmente pelo fato de serem muito fáceis de usar.

O que torna realmente um servidor seguro ou não é a maneira a qual ele é configurado, muitas vezes um *site* na *internet* é invadido não por problemas do *web server* e sim da maneira como ele foi configurado.

Existem alguns pontos na sua configuração que devemos analisar e configurar de forma correta para que não haja furos na segurança deste *web server*.

A primeira maneira diz respeito não só ao Apache, mas a todos os servidores web. Consiste na maneira a qual o *daemon* de *httpd* e “startado”.

Normalmente, o processo "pai" e “startado” com permissões de root, logo ele poderá "escutar" a porta 80, que e a porta padrão do serviço *http*. Quando há solicitação de conexão na porta 80, e gerado um processo "filho" cujo dono e grupo são definidos no arquivo httpd.conf.

A idéia é que para ficar mais seguro se troque o dono e o grupo do processo "filho" para nobody através deste arquivo de configuração.

Uma outra preocupação e com relação à permissão dos diretórios e dos arquivos. O diretório CGI ter permissão 711, ou seja, ele pode ser executado e não listado, mas os *scripts* lá contidos, têm que ter permissão 755 para poderem ser executados corretamente.

Os arquivos de configuração contidos na raiz do servidor, devem ter apenas permissão para o root de ler e escrever.

O Apache trabalha basicamente com três arquivos de configuração. são eles o access, conf, httpd.conf e srm.conf. E importante saber trabalha-los, pois, se configurados corretamente, será possível controlar diversos mecanismos para aumentar a segurança no seu servidor, tais como:

- Desabilitar listagem automática dos diretórios
- Negar os links simbólicos de seguirem fora da árvore do diretório de documentos, impedindo assim que arquivos confidenciais sejam visualizados
- Desabilitar os SSI, impedindo assim que usuários remotos possam executar comandos arbitrários
- Impedir que usuários remotos possam navegar sem preocupações por seus sistema de arquivos
- Evitar que as configurações dos usuários prevaleçam sobre as do sistema

Como dito anteriormente, nenhum servidor *web* e totalmente seguro. Os *bugs* são a maior prova disso. Aqui relacionamos três *bugs* do *Apache.*

- ✓ Permite a qualquer usuário remoto executar comandos *UNIX* arbitrários no servidor. Versões afetadas: 1.02 e inferiores

- ✓ Usuários locais podem executar comandos *UNIX* com a permissão igual a do servidor *Web*. Versões afetadas: anteriores a 1.2.5

- ✓ Permite ao usuário enviar *cookies* muito grandes para o servidor Web, ocasionando o estouro da pilha. Versões afetadas: anteriores a 1.1.3

- ✓ Permite ao usuário visualizar o conteúdo de paginas

Para a correção dos *Bugs* os implementadores do *Apache* recomendam instalação de *patches*.

-IIS

O IIS (*Internet Information Server*) é o segundo *Web server* mais utilizado na internet. Este server tem como funções estabelecer um modelo de segurança e oferecer recursos de monitoração no Windows NT. A segurança deste server consiste basicamente em controlar o acesso à informações contidas no sistema, através de permissões especiais de acessos às pastas e programas, impedindo assim que usuários façam utilizações indevidas ou visualizem arquivos de acesso restrito.

O mais importante em relação a parte de segurança do server é o modo com que ele é configurado, não se pode de nenhuma maneira tornar acessíveis informações do sistema relativas a localização de arquivos de configuração, pastas que contenham informações confidenciais como senhas ou qualquer outro tipo de informações que facilitem ou permitam a entrada de invasores.

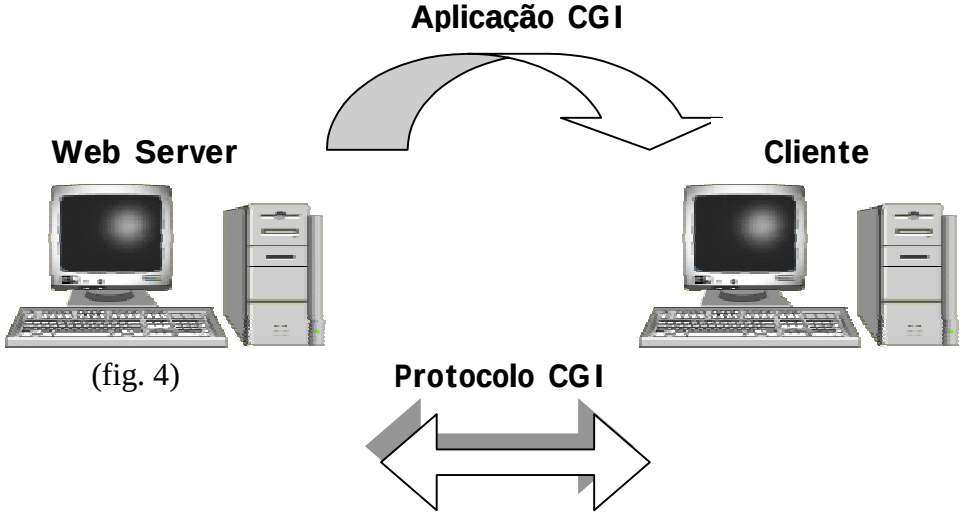
O *IIS* da Microsoft possui uma série de bugs, alguns já foram sanados através de patchs disponibilizadas na própria página da empresa. Até este momento foram descobertos cerca de 14 *bugs*. A seguir serão explicados 2 deles.

- ✓ Relativo ao *active server pages* (*asp*), que funciona criando documentos dinâmicos através da combinação de *html* com *scripts*. Quando este recurso é utilizado e o *Web server* que estiver rodando for o IIS 4.0, é possível visualizar todo o conteúdo do diretório digitando um ponto (.) no final do endereço. Nestas pastas podem estar contidos arquivos de acesso restrito e a apropriação indevida dos mesmos pode acarretar por exemplo no roubo de senhas. Este *patch* está disponível na página da Microsoft.
- ✓ Relativo ao ataque DoS (*Denial of Service*). Este ataque consiste em sobrecarregar o CPU invadida, enviando solicitações que provoquem falhas no inetinfo.exe do *IIS*. Ao ser corrompido este processo será iniciado usando 100% da capacidade da CPU pertencente ao *server*, dificultando a aceitação de solicitações e tornando o *server* mais lento, no decorrer do processo o servidor travará sendo necessário reinicializar o sistema. A Microsoft disponibilizou os *patches* para correção que podem ser encontrados no próprio site da Microsoft.

2.2.3 - EXECUTANDO PROGRAMAS NA *WEB*

-CGI

O *cgi* é um protocolo comum o qual o servidor *HTTP* (*web server*) usa para intermediar a transferência de um programa entre ele e o cliente *HTTP* (seu *browser*).



(fig. 4)

O *cgi* gera problemas aos *web servers*, às redes que os hospedam e até mesmo os clientes de *HTTP*. Este perigo não está ligado ao protocolo *cgi* e sim aos *scripts cgi* contidos neste diretório. Esses sim, são a maior fonte de *bugs* de segurança e por isso precisam ser escritos cuidadosamente.

Na verdade, o que pode gerar isso são alguns erros sutis na codificação, permitindo assim que informações de servidores ou do sistema apareçam, ou comandos arbitrários gerados a partir desses *scripts*.

Exemplos de *cgi* conhecidos como furo de segurança:

Script	***Versões afetadas***	***Uso***
count.cgi	1.0-2.3	contador de página
webdist.cgi	1.0-1.2	distribui software
php.cgi	até 2.0	Linguagem de *scripts*
Anyform	1.0	cria formulários
FormMail	1.0	envia dados/e-mail
Phf	Todas	Phone book

Recomendamos para maior segurança nos *scripts*:

Colocar todos os *scripts* em um único diretório (configurado no arquivo /conf/srm.conf).
Usar programas como *TRIPWIRE* para monitorar mudanças ocorridas nos *scripts*.
A permissão dos scripts é 711(*) e do diretório CGI 755(*)2.
Desative os *scripts* que não são mais utilizados.
Dentro do seu código evite dar mais detalhes sobre seus *scripts*, não assuma tamanho de dados na entrada e analise sempre os dados de entrada do usuário.
Chame os programas utilizando caminhos absolutos.

(*) permissão para o usuário ler, escrever e executar, para o grupo e outros apenas de execução.
(*)2 permissão para o usuário ler, escrever e executar, para o grupo de executar e ler e para outros apenas de execução.

2.2.4 - WEB CHATS

Ao entrar em um *web chat*, geralmente o usuário não imagina os riscos ao qual fica exposto.

O *Hacker* pode tentar atacá-lo por diversos motivos.

Ele pode tentar um ataque que nada tem a ver o usuário. É simples, o pirata só tenta burlar regras impostas por responsáveis pelo *chat* como:

Dar efeitos diferentes ao texto (cor, tipo de texto).
Entrar em uma página que o limite de usuários já esta esgotado.
Entrar em salas restritas à assinantes de determinado provedor.
Enviar mensagens a todos os usuários da sala simultaneamente e repetidamente.

Outra forma de ataque é feita diretamente com a intenção de prejudicar ou pelo menos investigar um usuário ou vários deles. Entre eles podemos citar:

Clonar seu *nick* (apelido no *chat*).
Apagar a lista de nomes das pessoas que estão no *chat.*
Visualizar seu *HD* (*hard disk*).
Rastrear seu *IP* e a partir dai poder monitorar e/ou "administrar" sua maquina.
Executar aplicações que possam atrapalhar desempenho da sua máquina

O mais alarmante disso é que esses ataques podem ser feito por qualquer pessoa, sem que seja necessário grande conhecimento técnico.

Outros fatores que contribuem para a falta de segurança dentro destes *chats* é a demora dos provedores em desenvolverem proteções contra para estes tipos de ataques (os chamados *filtros*), e a facilidade com que estas informações são disponibilizadas na *Internet* por meio de sites *hackers*, tem instruções detalhadas de como fazer, através das linhas de comando, ou como instalar e configurar determinados programas que executem este tipo de função.

Como dito no parágrafo acima, essas ocorrências podem surgir tanto por linhas de comandos (como por exemplo comandos de HTML) como softwares especializados neste tipo de atitude. Entre esses programas, podemos citar:

Robot Mask® UOL v1.2 News
Envia mensagens em todas as salas do chat do UOL.

Robot Mask® MANDIC v1.2 News
Envia mensagens em todas as salas do chat da MANDIC.

Robot Mask® WORLD v1.2 News
Envia mensagens em diversas salas de bate papo, STI, CORREIO, ETC.

Chat Mask Server v1.1
WebChat Pessoal, é um chat rodando direto do seu hd.

DynIP Client v3.0
Converte seu IP por um Domain Name.

Omni Httpd PRO v2.01
Servidor Pessoal, que através do envio de fotos no chat, rastrea IPs

IpTracer
Rastreia IP em salas de chat.

Chat Buster
Outro ratreador de Ips em salas de chat. Esse se apresenta mais eficaz que o acima pois funciona em mais chats que o anterior.

2.2.5 - INVASORES

-HACKERS

Quando iniciamos os estudos sobre segurança, vimos que a maioria das referências associam o termo *"hacker"* a piratas da rede, salvo uma, que deu a melhor definição para este termo.

Um *hacker* não é necessariamente uma pessoa que seja pirata de rede, e sim uma pessoa com extrema capacidade de associação e compreensão, dotada com extrema competência em uma área específica, por isso o termo é muito utilizado para caracterizar os piratas da rede, pois geralmente são muito inteligentes e dedicados quase que integralmente em seus objetivos ou suas atividades.

Os *hackers* são indivíduos inteiramente ligados à seus projetos de atacar redes por diversos motivos, entre eles podemos citar a destruição de redes, utilização dos recursos que ela oferece, hospedar programas em uma determinada rede para que através desta ele possa invadir outras, roubo de informações, descobrir falhas nos sistemas para que esta informação possa ser passada, assim, outros hackers poderão invadir da mesma forma ou até para provar aos outros que ele pode descobrir qualquer falha e invadir qualquer sistema.

Normalmente, estas pessoas possuem algumas características comuns. A grande maioria dos piratas de computador são jovens com idade entre 16 e 25 anos.

Eles também apresentam algumas outras características, como:

Ser especialista em *HTML* e em linguagens de programação da *Internet* tais como *CGI*, *DHTML*, *JAVA* , *PERL*, além de outras linguagens como *C*, *C++*, programação *Shell*.
Ter conhecimentos avançados em *TCP/IP*.
Conhecer minimamente todos os sistemas operacionais, principalmente *LINUX*, *UNIX* e *WINDOWS*.
Preferir as linhas de comando aos ambientes gráficos.

Os ataques, em sua grande maioria, ocorrem de madrugada, pois dificilmente os administradores estarão controlando seus sistemas. Outra característica destes ataques é que raramente deixam rastros.

2.2.6 - SEGURANÇA

Interna e externamente o servidor *Web* cada vez mais freqüentemente é o elemento intermediário da comunicação entre o usuário final e a aplicação de acesso ao Banco de Dados para operações ou de consulta. A busca por mecanismos que assegurem que somente as transações legítimas sejam acatadas, sem abrir mão de formas de acesso baratas, universais e de amplo uso, tem sido uma preocupação constante de quem implanta serviços neste contexto.

-SHTML *(SECURITY HYPER TEXT MARKUP LANGUAGE)*

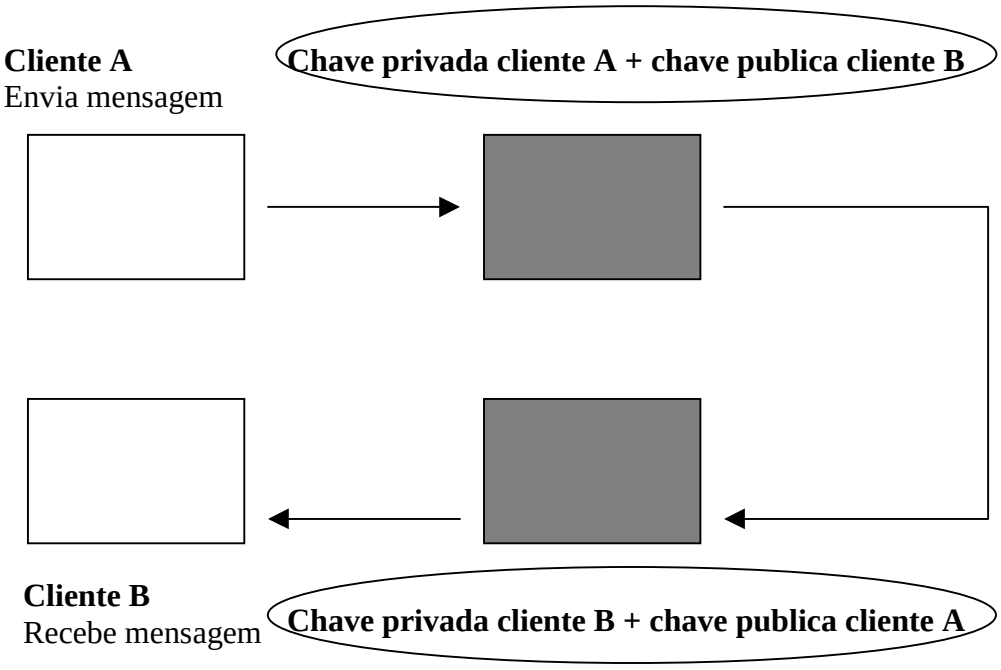
O shtml tem como função tornar os documentos html interativos. O que possibilita este dinamismo é o recurso *SSI* (*Sever Side Includes)* que é utilizado pelo shtml. O *SSI* trabalha executando na pagina *scripts* e *CGI*s que estejam contidos no servidor. O que diferencia este recurso do html é a possibilidade de aplicar, diretamente no código, variáveis de um programa *CGI*, contido no servidor, em uma homepage. Através do *SSI* é possível carregar para o usuário variáveis que possam conter por exemplo datas, horas, mensagens e etc que se modificam automaticamente. Porém para se obter acesso na construção deste tipo de página, faz-se necessária autorização por parte do *Web Server*.

-CRIPTOGRAFIA

A criptografia é um conjunto de técnicas utilizadas para transformar as informações que trafegam na rede, em textos cifrados para mente-las em sigilo. Ela trabalha codificando a informação de modo que apenas quem tiver conhecimento da chave utilizada, poderá decodificá-la.
Atualmente existem dois métodos de encriptação, que utilizam algoritmos baseados em chaves: simétrica e assimétrica.

A criptografia de chave simétrica trabalha utilizando uma única chave para codificar e decodificar a informação. Este tipo de criptografia é mais utilizado nas conexões temporárias ou em conexões seguras, como por exemplo no preenchimento de dados sigilosos na internet. Como a chave utilizada é única, ela deve ser mantida em segredo. A segurança dos algoritmos simétricos residem nesta chave e divulga-la significa que qualquer um pode tanto cifrar como decifrar qualquer mensagem que utiliza este sistema criptográfico.

Já a criptografia de chave assimétrica utiliza duas chaves diferentes para encriptar. Estas chaves são denominadas de privada, que é a qual apenas o usuário tem conhecimento, e a pública que é transmitida para o destinatário de modo que apenas este possa decodificar a informação. O esquema abaixo ilustra este processo:



(fig. 5)

2.2.7 – INSEGURANÇA

-JAVA APPLETTS HOSTIS

Se você costuma navegar pela Internet em busca daquela informação que você necessita ou daquela imagem maneira, acautele-se. Você pode estar sendo infectado por um vírus transportado por um *Java Applet. Java Applets* hostis *Java* é a maior onda do momento. Trata-se da primeira linguagem de programação realmente portável, estável, barata e fácil de usar, pelo menos para quem conhece C. Todavia existe uma serpente também neste paraíso. Problemas de segurança sérios podem ser acarretados a partir do simples e aparentemente inocente acesso a uma página *WWW* cheia de vistoso recursos multimidia que para serem apreciados requerem que você permita o envio para a sua máquina, de código que será localmente executado.

Java tem mecanismos intrínsecos de segurança mas o fato de implicar no envio de código executável para o *browser* abre espaço para toda uma série de ataques. E estas brechas tem sido usadas.

Os mecanismos básicos de segurança do ambiente Java implicam em que o código recebido seja limitado a certas ações e contexto, tais como:

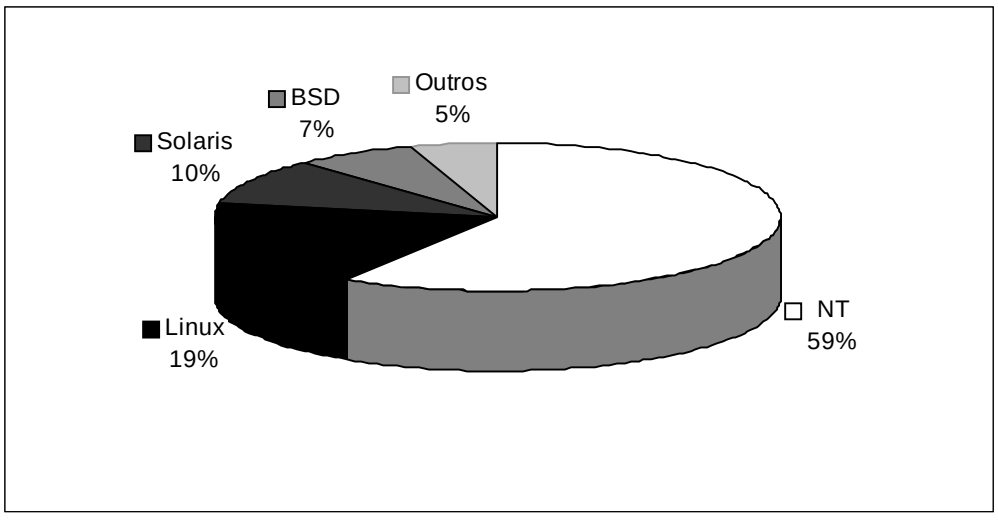
- executar cálculos, iterações, etc...
- desenhar dentro dos limites definidos pelo *HTML* na janela do cliente
- desenhar janelas marcadas como janelas *Java* fora da janela do navegador
- comunicar via interface de soquetes com o *host* que carregou o *applet*

A equipe da Universidade de Princeton tem testado os *browsers Netscape* e *Microsoft* Explorer e em cada nova versão novos furos tem sido apontados. Os mais significativos são os seguintes: *DNS spoofing* (como um computador engana um servidor fazendo-o acreditar que ele é outro nodo ou cliente), o envio de código executável não confiável para sistemas remotos que executam comandos que não era suposto executar (mais poderosos do que o definido no contexto *Java*) e vários defeitos nos primeiros *browsers* que também permitem que as ações comandadas saiam fora do contexto limitado anteriormente referido provendo acesso a variáveis e arquivos do sistema.

Assim, aquela página *WWW* vistosa que você buscou num endereço qualquer pode conter o ovo da serpente que será aninhada e nascerá nas entranhas de sua máquina. *Applets Java* potencialmente hostis podem ingressar numa Intranet enganando o *firewall* via *DNS spoofing*. Claro que sempre é possível desabilitar os Java scripts em seu browser. Isto pode ser feito selecionando a opção *"Security Preferences"* do menu de *"Options"* e então clicando na caixa *"Disable Java"* mas então perde-se o efeito pretendido para a página. Um servidor *proxy* para *http* poderia também ser configurado para impedir a passagem de arquivos com classe Java.

3 – ESTATÍSTICAS DE PIXAÇÕES EM PÁGINAS NA INTERNET

A seguir serão exibidos uma série de gráficos que representam os sistemas operacionais mais atacados e quais os *Web Servers* que operam nesses *hosts*.
(Todos as informações destes gráficos foram obtidos no período de um ano, de agosto de 99 até agosto de 00)



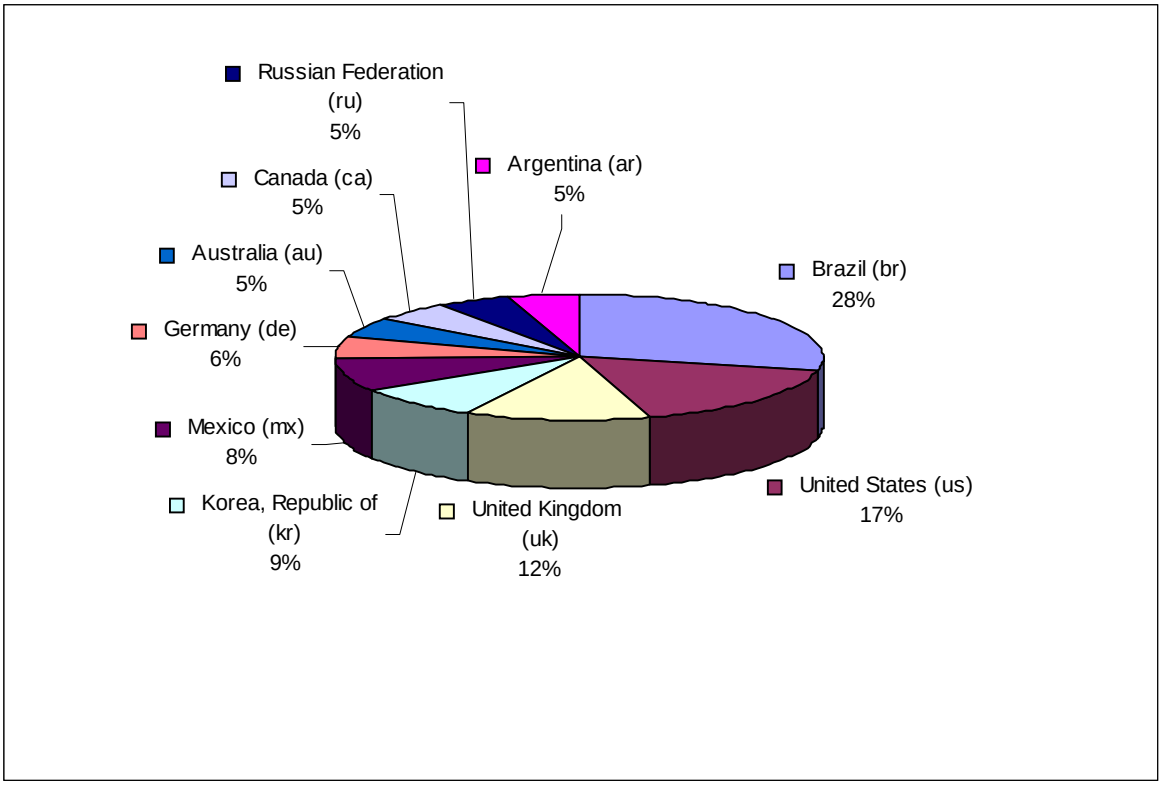
(fig. 6)

Será mostrado através de tabela e gráfico os domínios mais atacados

Tabela com números relativos ao ano 2000

Brazil (br)	453
United States (us)	269
United Kingdom (uk)	191

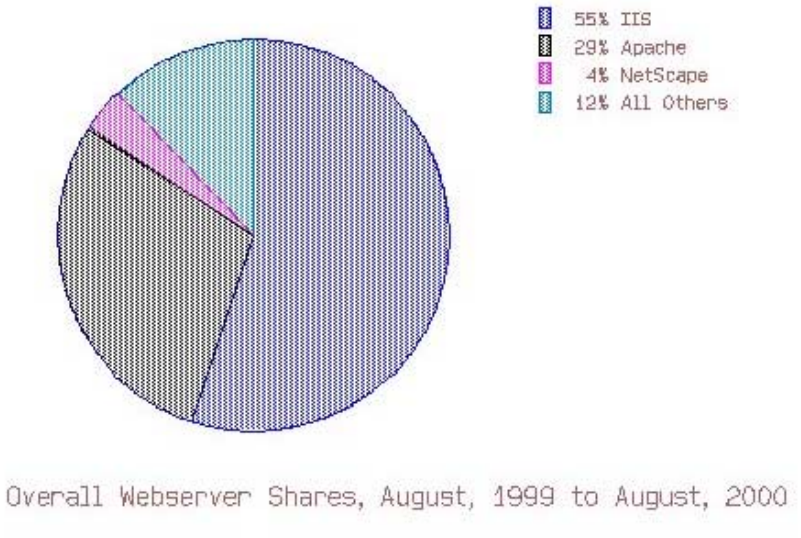
Korea, Republic of (kr)	141
Mexico (mx)	134
Germany (de)	89
Australia (au)	81
Canada (ca)	80
Russian Federation (ru)	80
Argentina (ar)	73



(fig. 7)

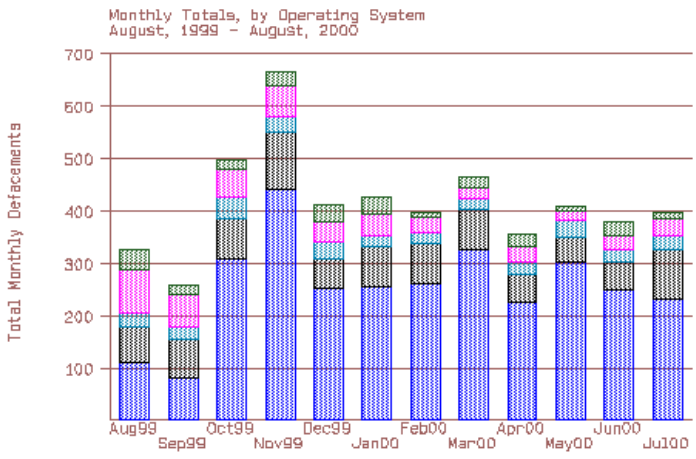
O gráfico acima refere-se aos domínios mais invadidos. Note que o Brasil lidera esse ranking. Espera-se que ocorra uma reviravolta neste quadro a curto ou médio prazo, pois alguns sites já estão começando a investir em segurança.

Web Servers Pixados



(fig. 8)

No gráfico acima é possível observar que o *IIS* é o *Web server* com o maior índice de invasões, este servidor trabalha nas plataformas Windows NT, que por sinal é o sistema operacional com o maior número de invasões. Logo em segundo vem o Apache, porém é preciso lembrar que este *Web Server* trabalha em diversas plataformas, o maior número de invasões ocorre quando este servidor está instalado em máquinas que utilizam o Windows NT como sistema operacional.



(fig. 9)

O gráfico acima representa a quantidade de *Web Servers* rodando sob os sistemas operacionais mais atacados. A parte inferior representa o sistema com a maior incidência, o Windows NT, o segundo (de baixo para cima) diz respeito ao Linux, o terceiro ao Solaris, o quarto ao BSD e o último a todos os outros sistemas disponíveis.

4-CONCLUSÃO

No decorrer do desenvolvimento deste trabalho, concluímos através de inúmeras pesquisas, que o servidor Apache é o mais seguro e eficiente, por sua confiabilidade, versatilidade de plataformas de operação, além de ser gratuito . Existem outros bons web servers disponíveis no mercado, porém não tão seguros, devido ao grande número de falhas em sua programação como é o caso do IIS.

É preciso esclarecer que apesar de ser o mais seguro, não é 100% livre de falhas. Portanto, é preciso atualizar-se continuamente pois a cada dia são descobertos novos bugs. Os invasores de sistemas estão ficando cada vez mais numerosos e com mais recursos, todo o dia são lançados dezenas de programas de invasão, transformando a rotina dos administradores de web servers em uma eterna monitoração.

Sugestões:

1. Manter-se, atualizado participando de listas de discussões e de boletins de segurança.
2. Monitoração permanente da rede; através de logs confiáveis.
3. Redundância de servidores e/ou backup diários.
4. Ter uma política de segurança.

5- Bibliografia

Devido ao caráter instável das paginas na internet, não garantimos a acessibilidade de todos os sites.

1- Hackersclub - "www.hackersclub.com"

2- Microsoft - "www.microsoft.com.br"

3- "www.cciencia.ufrj.br"

4- "latam.iis.net"

5- "www.hackersnews.com.br"

6- "www.hackers.com.br"

7- "Sistema X - "http://members.nbci.com/rogeriox/"

8- Anti-hackers – "http://www2.uol.com.br/cgi-bin/anti-hackers/builder/builder.cgi"

9- Attrition – "www.attrition.org/mirror/attrition"

10 - Formas de Ataque
Liana Tarouco
POP-RS/CERT-RS-UFRGS

GLOSSÁRIO

TELNET
O telnet é um programa/protocolo utilizado para estabelecer uma comunicação remota com outra máquinas. Este recurso permite uma conexão simples e sem interface gráfica.

TCP (Transmission Control Protocol)
É um dos protocolos que compõem o TCP/IP, responsável pelo transporte de informações pela rede.

IP (Internet Protocol ou Protocolo da Internet)
Responsável pela identificação das máquinas, redes e encaminhamento das mensagens entre elas. O IP é responsável pelo roteamento dos pacotes entre dois sistemas que utilizem os protocolos do tipo TCP/IP. É o mais importante dos protocolos utilizados na internet.

FTP (File Transfer Protocol ou Protocolo de Transferência de Arquivos)
Um protocolo padrão da Internet que é usado para transferência de arquivos entre computadores remotos.

NFS (Network File System ou Sistema de Arquivos de Rede)
Protocolo para compartilhamento de dados numa rede independente da máquinas UNIX.

DNS (Domain Name System ou Sistema de Nome de Domínio)
O DNS funciona como um catálogo de endereços na Internet. Ao requisitar no servidor de internet um endereço, ele procura em seu catálogo se ano conseguir encaminha este endereço para outros servidores e se nenhum servidor da rede conseguir identificar o endereço, ele é considerado inexistente e a pesquisa para enviando uma mensagem de erro para o browser.

SMTP (Simple Mail Transport Protocol ou Protocolo de Transporte de Mail Simples)
Protocolo utilizado para a transferencia de correio eletrônico de um computador para outro em uma rede TCP/IP.

POP3 (Post Office Protocol)
Protocolo usado pelo correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

HTTP (HiperText Transfer Protocol ou Protocolo de Transferência de HiperTexto)
É o protocolo mais utilizado na web, pelo qual os documentos são enviados do servidor para o Browser.

UDP (User Datagram Protocol)
Neste protocolo, os pacotes são enviados ao destino sem uma preocupação se os dados chegaram completos ao destino. Por não Ter esta preocupação durante a comunicação, o UDP é mais rápido que o TCP, porém menos confiável.
É bastante útil para evitar sobrecarga quando durante a transmissão, perder um pacote ou outro não significa muito.

PERL (Practical Extraction and Report Language)
Linguagem de programação desenvolvida para
processamento de textos. Também é umas das linguagens mais utilizadas para se escrever
scripts CGI.

Java
Linguagem orientada à objetos, que permite o desenvolvimento de aplicações e Applets Java muito utilizada na Web. Gera código intermediário (byte codes) que são interpretados em tempo de execução.

Javascript
Linguagem de formulação de scripts relacionada à linguagem Java. Não é totalmente orientada à objetos é interpretada. Oferece recursos avançados na construção de páginas na Web em conjunto com a linguagem HTML.

ASP (Active Sever Pages)
Linguagem de programação da internet desenvolvida pela empresa Microsoft, que permite entre outras coisas a manipulação de banco de dados via web e a criação de páginas HTML mais dinâmicas.

DHTML (HTML dinâmico)
É uma linguagem avançada de edição de documentos para Web, que permite atribuir dinamismo e interatividade aos documentos.

Windows
Sistema operacional da Microsoft, no qual os aplicativos são apresentados de maneira bem amigável ao usuário através do uso de janelas que podem ser redimensionadas e movidas.

Unix
Sistema operacional desenvolvido pela AT&T. O Unix é escrito em linguagem C, também desenvolvida pela AT&T. Esse sistema tem como principais vantagens o modo multiusuário, e a grande capacidade de processar.

Linux
Conhecido como "Unix para PC". Foi desenvolvido em 1991, por Linus Torvald, estudante de Ciência da computação na Finlândia.

C
Linguagem de programação que pode manipular o computador em baixo nível. A linguagem C pode ser compilada em
quase todos os computadores, permitindo o seu uso em uma ampla variedade de micros, minis e computadores de grande porte.

C++
Versão orientada a objetos da linguagem C, criada por Bjarne Stroustrup. O C++ tornou-se popular por combinar a programação em linguagem C tradicional com a técnica de orientação à objetos.

Host
O Host é computador qualquer
computador ligado à rede, não necessariamente um servidor.

SSI (Server Side Includes)
São comandos extensivos a linguagem HTML que são processados pelo servidor Web antes da página HTML ser enviada. No lugar do comando é enviado apenas o resultado do comando no formato normal de texto HTML.

Bug (Erro. Inseto voador, em inglês)
Este termo foi associado a ocorrência de um erro na programação ou fabricação de um Software ou Hardware.

APÊNDICE 1

Nome	***Plataforma***
AOLserver Digital	UNIX, HPUX, Linux, IRIX, Solaris
ArexxWebServer	Amiga
Alibaba	Windows 3.x, NT, Windows
Amiga Web Server	Amiga
Apache	Linux, FreeBSD, Solaris, IRIX,Digital UNIX, BSDI, AIX,NetBSD, IBM OS/2, SCO,HPUX, NT CERN httpd UNIX
Commerce Server/400	AS/400
EIT httpd	UNIX
EMWAC HTTP Server	NT
EmWeb Embedded Web Server	Digital UNIX, BSDI, AIX, SCO, HPUX, Embedded, NT, Linux, Windows 95, FreeBSD, IRIX, Solaris
Enterprise Server	Novell NetWare
Enterprise Web Secure/VM	VM/CMS
EnterpriseWeb/MVS	MVS

EnterpriseWeb/VM	VM/CMS
GLACI-HTTPD	Novell Netware
GN Gopher/HTTP	UNIX
HTTPd for OS/2	IBM OS/2
HTTPS	NT (baseados em Intel e Alpha)
Internet Information Server	NT
Java Server	IBM OS/2, HPUX, NT, Linux, Windows 95, IRIX, Solaris
KA9Q	MSDOS
Lotus Domino Go Webserver	Digital UNIX, AIX, IBM OS/2, HPUX, NT, Windows 95, IRIX, Solaris
NCSA HTTPd	NetBSD, Digital UNIX, BSDI, AIX, SCO, HPUX, FreeBSD, IRIX, Solaris
Netscape Enterprise Server	Digital UNIX, AIX, HPUX, Windows, NT, IRIX
Netscape Netsite Servers	Windows, IBM OS/2 e NT
Open Market Web	UNIX
Oracle Web Application Server	HPUX, NT, Windows 95, Solaris
OS2HTTPD	IBM OS/2

Phttpd	UNIX
Plexus	UNIX
Purveyor	NT
Roxen Challenger	NetBSD, Digital UNIX, BSDI, AIX, SCO, HPUX, Linux, FreeBSD, IRIX, Solaris
SerWeb	Windows
Spinnaker	NT, Windows 95
Spyglass MicroServer	Embedded, NT, Linux, Solaris
The Major BBS	MSDOS
Viking	NT, Windows 95
vqServer	Be OS, NT, Linux, Windows 95, Solaris
WebControl	NetBSD, Digital UNIX, BSDI, AIX, Windows 3.x, SCO, HPUX, Embedded, NT, Linux, MS-DOS, Windows 95, FreeBSD, IRIX, Solaris
WebControl (TM)	NetBSD, Digital UNIX, BSDI, AIX, Windows 3.x, SCO, HPUX, NT, Linux, MS-DOS, Windows 95, FreeBSD, IRIX, Solaris
WEB4HAM	Windows
Windows httpd	Windows

WebSite Professional	NT, Windows 95
WebTen	Macintosh
WN	UNIX
Xitami	NetBSD, Digital UNIX, BSDI, AIX, IBM OS/2, Windows 3.x, SCO, HPUX, NT, Linux, MS-DOS,VMS, Windows 95, FreeBSD, IRIX, Solaris
Zeus Web Application Server	Digital UNIX, AIX, HPUX, NT, Linux, IRIX, Solaris