Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD
Leandro de Oliveira

ESTUDO PARA IDENTIFICAÇÃO DE TRÁFEGO ANÔMALO NAS PORTAS 21 E 80 NOS SERVIDORES FTP e HTTP DO BR ON-LINE- BROL

Brasília
2012

Leandro de Oliveira

ESTUDO PARA IDENTIFICAÇÃO DE TRÁFEGO ANÔMALO NAS PORTAS 21 E 80 NOS SERVIDORES FTP e HTTP DO BR ON-LINE- BROL

Projeto apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como uma das atividades do programa de Metodologia Científica do Curso de Pós-graduação Lato Sensu, Redes de Computadores com Ênfase em Segurança.

Orientador do Projeto: Prof. Dr. Eduardo Gomes de Barros

Brasília

2012

DEDICATÓRIA

Á minha amada esposa, Núbia, que me faz feliz todos os dias.

AGRADECIMENTOS

Ao Dr. Prof. Eduardo Gomes de Barros, amigo e orientador. Pessoa brilhante que tenho como referência profissional.

Aos grandes amigos que conheci durante esse curso e que contribuíram para meu crescimento pessoal e profissional, em especial Bruno Mariano, José Ozete e Renan Rodrigues.

Ao grande amigo, Carlos Caribé, que viabilizou a execução desse estudo dentro do Instituto Nacional de Metereologia

RESUMO

Os avanços tecnológicos viabilizaram grandes conquistas para nossa sociedade, entre elas, a previsão do tempo e do clima que permitem, por exemplo, a prevenção de desastres naturais. A Disponibilidade dos recursos computacionais envolvidos nesse processo é fundamental para que a população tenha acesso ás informações e serviços oferecidos por meios digitais. Esse trabalho buscou identificar tráfegos anômalos direcionados aos serviços de transferência de arquivo na porta 21 e página de internet na porta 80 através da análise de pacotes TCP, registros de segurança gerados pelo sistema operacional, serviços de FTP (File Transfer Protocol) e HTTP (Hypertext Transfer Protocol), em servidores utilizando sistema operacional Linux e ferramentas de captura de tráfego e análise de registros de segurança. Essa análise possibilitou caracterizar o volume mínimo de pacotes trafegados em uma conexão “legitima” utilizando conceitos estatísticos. Concluiu-se que é possível identificar anomalias no tráfego. Constatou-se que o principal objetivo dos hackers é a varredura dos sistemas em busca de vulnerabilidades e que, geralmente, são utilizados meios automatizados para isso.

ABSTRACT

Technological advances have made possible great achievements for our society, including the weather and climate that allow, for example, the prevention of natural disasters. The availability of computational resources involved in this process is critical for the population to have access to the information and services offered by digital media. This study aimed to identify anomalous traffic directed to the services file transfer on port 21 and web page on port 80 by analyzing TCP packets, safety records generated by the operating system, services, FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol) server using the Linux operating system and tools for capturing and analyzing traffic safety records. This analysis enabled characterization of the minimum volume of packets in a connection trafficked "legitimizes" using statistical concepts. It was concluded that it is possible to identify traffic anomalies. It was found that the main objective of the hackers is to scan systems for vulnerabilities and is typically used automated means to do so.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
DDoS	Distributed Denial of Service
BROL	BR On-line
NIC	Núcleo de Informação e Coordenação do Ponto BR
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes
RFC	Request for Comments
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol
RNP	Rede Nacional de Pesquisa
NFS	Network File System
KB	Quilobyte
SSH	Secure Shell
VM	Virtual Machine
SNMP	Simple Network Management Protocol
ARP	Address Resolution Protocol
DNS	Domain Name System
ICMP	Internet Control Message Protocol
S.O.	Sistema Operacional

SUMÁRIO

INTRODUÇÃO

Com o crescimento da Internet mais pessoas, corporações e governos puderam estreitar laços, agilizar processos e realizar negócios. Serviços bancários e serviços governamentais são acessíveis através da rede mundial de computadores.

Infelizmente, todas essas facilidades diariamente são ameaçadas por pessoas mal intencionadas que atuam quase que livremente, protegidos pela anonimidade inerente da Internet.

As principais ações empreendidas pelos hackers são o roubo de senhas de bancos, correio eletrônico e sistemas corporativos, terrorismo, indisponibilidade de sistemas, recursos e serviços por meio de ataques cibernéticos.

Segundo Gallagher et all (2012), ataque cibernético é uma ação empreendida através de meios eletrônicos e informáticos que visa um dano em um alvo também eletrônico. O principal campo de batalha é a rede mundial de computadores, Internet. Uma ação de ataque coordenada pode comprometer a infraestrutura de uma nação, provocar prejuízos financeiros á uma empresa, lesar uma pessoa física, em caso de fraudes e bancarias. Um ataque cibernético pode ser empreendido, financiado e coordenado por pessoas físicas, grupos sociais, empresas e governos. Por acontecer em meios digitais, onde não existem limites geográficos, a guerra cibernética tornou-se uma preocupação de Estado.

Como exemplo de ameaças cibernéticas podemos citar os ataques de negação de serviço (DDoS) que consiste em direcionar um grande numero de tráfego ao mesmo tempo a um serviço disponível na internet como por exemplo sítios de empresas ou órgãos públicos. Quando isso acontece, a infraestrutura responsável pelo serviço não suporta a carga de tráfego e para de responder ás

requisições “reais”. Como os sofridos por diversos órgãos do governo brasileiro em 2011, segundo Portal G1 (2011)

Para empreender um ataque cibernético, o hacker utiliza vários meios para identificar vulnerabilidades nos sistemas computacionais. Entre as formas mais tradicionais utilizadas para identificar vulnerabilidades, a varredura de portas é a mais conhecida. Os principais equipamentos de segurança da informação já possuem proteção contra esse tipo de procedimento malicioso.

Os equipamentos de segurança utilizam assinaturas para identificar um comportamento anômalo no tráfego como, por exemplo, o aumento repentino no volume de acessos a determinados sistemas dentro de uma janela de tempo sem motivo aparente.

Porém, existe uma dificuldade para identificar um comportamento anômalo quando o tráfego possui um número pequeno de pacotes trafegados podendo tornar-se ainda mais difícil quando existe uma janela de tempo muito grande entre tais ocorrências.

A segurança da informação quase sempre está um passo atrás do hacker, já que as vulnerabilidades dos sistemas nem sempre são conhecidas pelos administradores. Aproveitando-se dessa situação, pessoas mal intencionadas dedicam-se a encontrar falhas de segurança nas redes de computadores e sistemas corporativos.

É necessário criar meios de proteção que identifique anomalias no tráfego em uma rede mesmo quando o volume trafegado é pequeno e aparentemente despretensioso. Pois como mencionado acima antes de realizar um ataque bem sucedido o invasor procura por vulnerabilidades em seus alvos.

Objetivos

Conseguir mapear o tráfego da rede direcionado aos servidores de transferência de arquivos e serviço de página de Internet. Identificar o tráfego que possui um volume abaixo do considerado normal para uma conexão real e correlacionar os resultados obtidos com os registros de segurança gerados pelo Sistema Operacional e respectivos programas de FTP e HTTP.

Identificar meios de proteção para os serviços de FTP e HTTP nas portas 21 e 80, respectivamente, evitando comprometimento dos recursos computacionais necessários para o cumprimento da missão do BR On-line(BROL).

Objetivos Específicos

- Analisar o tráfego direcionado ás portas 21 e 80 dos servidores de FTP e HTTP.
- Identificar comportamento anômalo no tráfego direcionado á essas portas.
- Correlacionar os dados obtidos com os registros de segurança gerados pelo sistema operacional e pelas aplicações de FTP e HTTP
- Classificar o tráfego anômalo de forma que seja possível a geração de alertas.
- Sugerir tratativas para o tráfego classificado como anômalo.

Organizações do trabalho

Esse trabalho busca mostrar os processos e procedimentos práticos necessários para mapear um tráfego de rede com o propósito de identificar tráfegos anômalos em uma rede de computadores, especificamente o tráfego direcionado aos servidores de FTP e HTTP.

Para isso, foi realizada uma pesquisa dos principais assuntos relacionados ao tema a fim de facilitar a compreensão dos procedimentos executados. O trabalho está organizado da seguinte forma:

- Introdução;
- Capitulo 1 - Referencial Teórico;
- Capitulo 2 - Ambiente do Estudo, infraestrutura da rede e programas utilizados e características gerais do ambiente computacional;
- Capitulo 3 - Trata dos serviços de FTP e HTTP e da captura do tráfego direcionado á esses dois serviços. Trata também da forma como são gerados os registros de segurança;
- Capitulo 4 - Análise dos dados capturados no capitulo quatro, a fim de identificar comportamentos anômalos e correlaciona os dados com os registros de segurança do sistema operacional e das aplicações de FTP e HTTP;
- Capitulo 5 - Trata da geração de alertas;
- Conclusões
- Referencias

1. REFERENCIAL TEÓRICO

1.1. Registros de Segurança (*logs*)

Segundo CERT (2012), *logs* são registros de atividades gerados por programas e serviços de um computador ainda segundo o mesmo autor eles podem ficar armazenados no próprio computador ou pode ter armazenamento externo.

Segundo Anônimo (2000) *logs* registram eventos em um sistema à medida que eles acontecem para posterior análise.

Segundo NIC (2003) são importantes para a administração segura de sistemas. Eles registram eventos relativos ao funcionamento do sistema e de programas além de atividades que possam afetar a segurança. Os logs podem ser usados para descobrir a causa de um problema.

1.2 Gerências de Registros de Segurança

A gerência de Registros de Segurança é o conjunto dos procedimentos necessários para que os *logs* obtidos retenham informações úteis para análise enquanto necessárias. Segundo NIC (2003), a gerência de Registros de Segurança pode ser dividida em três processos:

- Geração;

- Armazenamento; e
- Monitoramento.

Segundo RNP (1999) uma política deve ser criada para definir quais informações devem ser gravadas, onde será realizada a gravação e onde serão armazenadas para posterior análise.

1.2.1 Geração de Registros de Segurança

Segundo NIC (2003) para que os *logs* gerados pelo sistema sejam úteis para análise, todos os sistemas monitorados devem estar com as informações de data/hora sincronizados através de um protocolo de sincronismo de tempo, como o NTP e possuir um nível de detalhamento suficiente para fornecer as informações necessárias para análise. O administrador do sistema deve tomar as medidas para que o sistema de *log* gere apenas informações necessárias, visto que o volume de dados gerados é muito grande.

Segundo RNP (1999), o administrador do sistema deve determinar quais os programas relevantes na geração de registros e, uma vez selecionados, se os programas mesmos estão efetivamente gerando registros e, se esses registros possuem as informações necessárias. Ainda segundo a RNP (1999), deve-se gerar *logs* com o máximo de informações possíveis e posteriormente determinar quais informações são mais importantes e que necessitam ser registradas.

1.1.3 Armazenamento de Registros de Segurança

Segundo Isoni (2007) os logs devem ser gravados remotamente em vários servidores separados. O armazenamento local deve ser evitado. Isso reduz os riscos de alterações indevidas caso o computador onde os registros são armazenados seja comprometido.

Segundo NIC (2003) Os registros de segurança podem ser gravados em um servidor dedicado. Todavia, como o volume de registros aumenta rapidamente, os logs podem ser gravados em mídias externas.

Segundo Atheniense (2012), além da questão técnica e operacional do armazenamento dos logs, existe a questão legal. O Brasil ainda não possui uma legislação específica sobre o assunto. Os *logs* podem ser utilizados, por exemplo, como evidência em processos judiciais.

1.2 Monitoramentos de Registros de Segurança

Segundo NIC (2003), os Registros de Segurança devem ser monitorados com frequencia, para que anomalias possam ser identificadas rapidamente.

O monitoramento dos *logs* é essencial; o monitoramento pode mostrar uma falha de sistema, um erro em uma aplicação ou padrões incomuns, dentre outras possibilidades

Segundo Isoni (2003), a análise de *logs* é complexa e difícil porque eles nem sempre possuem um padrão. Tanto as aplicações, quanto o sistema operacional geram registros em diferentes formatos.

1.3 *Transfer Control Protocol* / *Internet Protocol* - TCP/IP

Segundo RFC1112 (1999) TCP/IP é um conjunto de protocolos necessários para a comunicação entre computadores em uma rede. A pilha de protocolos TCP/IP possui quatro camadas:

- Camada Aplicação: responsável pelas aplicações que se comunicam na rede. Possui equivalência com as camadas de apresentação e aplicação do modelo OSI. Os principais protocolos dessa camada são: FTP, HTTP, SMTP, DNS, SSH, Telnet, entre outros. A unidade de dados de protocolo dessa camada são os Dados;
- Camada de Transporte: responsável pela comunicação fim-á-fim dos serviços da camada de aplicação. Existem dois protocolos nessa camada: TCP (Transfer Control Protocol) serviço de transporte orientado a conexão, com controle de fluxo e retransmissão em caso de perda de pacotes e, UDP (User Datagram Protocol) que não proporciona comunicação confiável, já que não possui mecanismos de confirmação de entrega dos pacotes no destino e retransmissão em caso de perda de pacotes. A unidade de dados de protocolo dessa camada são os Segmentos;
- Camada de Internet: responsável pela comunicação ponto-a-ponto entre computadores transportando os protocolos das camadas de transporte e

aplicação. Os pacotes possuem informações da origem e destino. A unidade de dados de protocolo dessa camada são os Pacotes ou Datagramas;

- Camada de Enlae de Dados - Camada responsável pela interface de rede trata dos meios mecânicos e elétricos para interligação física de um computador a uma rede. A unidade de dados de protocolo dessa camada são os Bits

1.4. Captura de Pacotes

Um dos possíveis registros de segurança, para análise de tráfego de rede, é obtido a partir dos registros dos pacotes que circulam em uma rede. Há vários aplicativos disponíveis que executam esta captura. Um dos mais usados, e o que será usado neste trabalho, é o *tcpdump*.

Segundo TCPDUMP & Libcap (2012), *tcpdump* é um analisador de pacotes, nativo no Linux e de outros sistemas operacionais da família UNIX, que utiliza a biblioteca libpcap, especializada em captura de tráfego de rede. Também pode ser instalado no Windows, se utilizada à biblioteca Wincap. O tcpdump possui uma série de parâmetros que possibilitam a captura e manipulação de um grande número de informações relacionadas ao tráfego na rede.

Segundo Montes et all (2005), a captura e análise de tráfego da rede é importante para prevenir tentativas de intrusão e verificar padrões de comportamento. Os dados capturados possibilitam analisar o volume do tráfego e a identificação de anomalias.

O monitoramento da rede possibilita identifica um padrão no comportamento do tráfego e permite possíveis variações que podem ocorrer dentro de uma janela de tempo. Como pode ser constatado nas figuras 1 e 2. A primeira mostra o tráfego de entrada e saída de duas em duas horas e segunda imagem mostra o tráfego durante o período de sete dias.

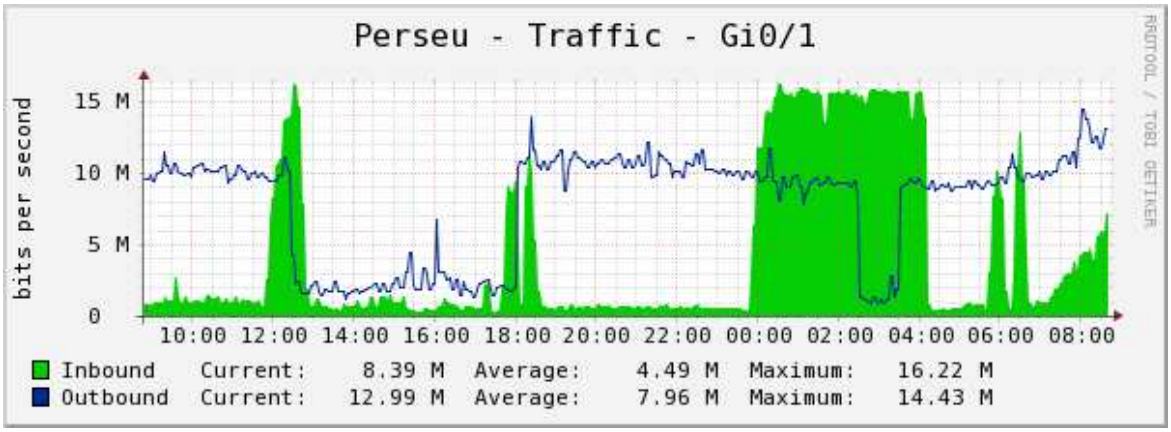

Figura 1 - Monitoramento do tráfego de entrada e saída, duas em duas horas - Cacti - BROL

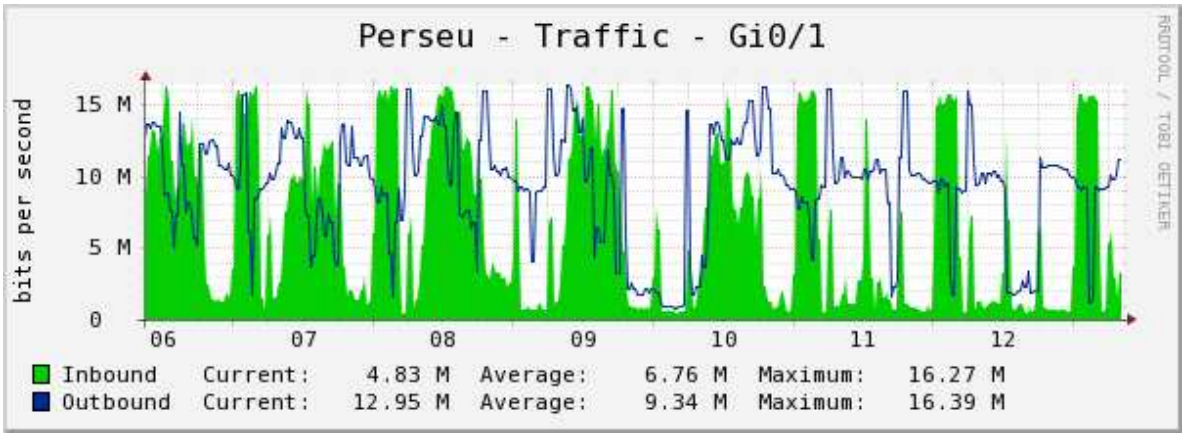

Figura 2 - Monitoramento do tráfego de entrada e saída, semanal - Cacti - BROL

Como pode ser observado nas figuras acima existe um padrão no tráfego, as variações são previsíveis. A variação no tráfego de entrada refere-se à chegada de

dados metereológicos á serem processados, enquanto a variação na saída refere-se ao envio destes dados já processados.

As variações no gráfico do tráfego de entrada e saída chegam a quase noventa graus, porém ocorre em tempos específicos uma mudança nesse comportamento pode sinalizar uma anomalia no tráfego.

Além dos padrões de volume ao longo do tempo pode-se destacar também o tipo de tráfego e protocolo utilizado. Como pode ser constatado nas figuras 3 e 4 o maior tráfego da rede é o protocolo FTP (*File Transfer Protocol).*

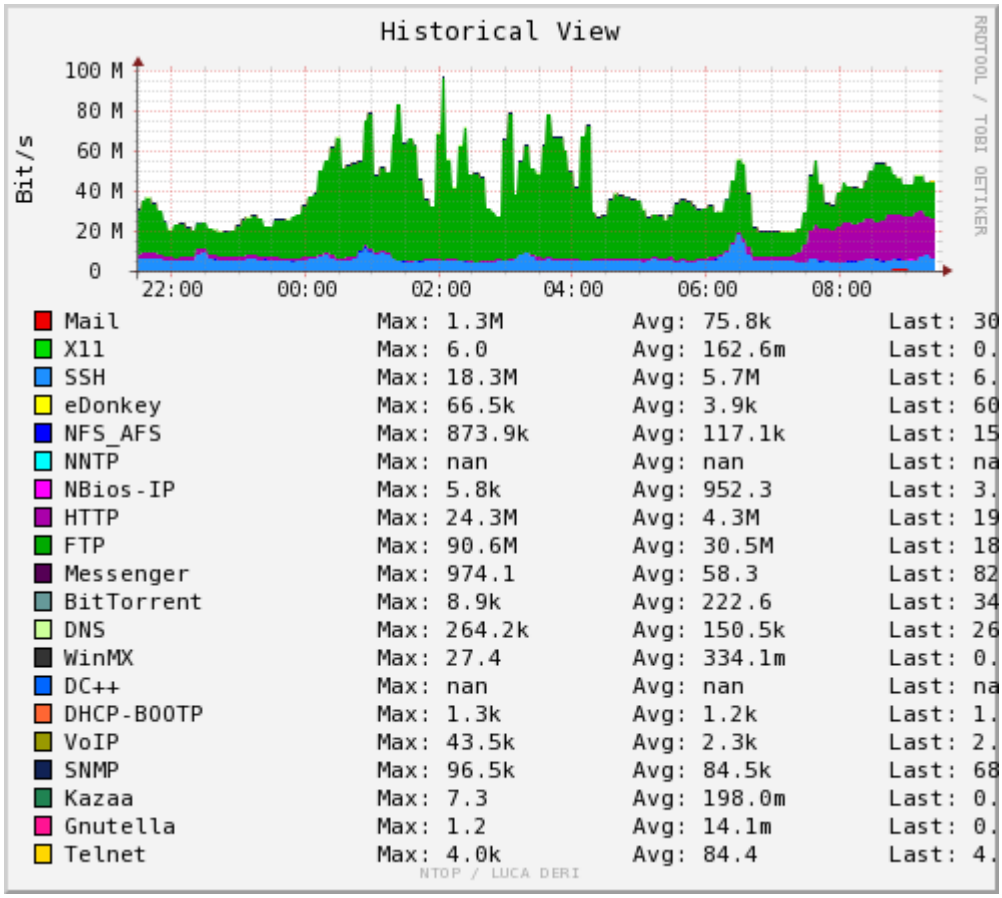

Figura 3 - Volume de dados por protocolo - Ntop – BROL

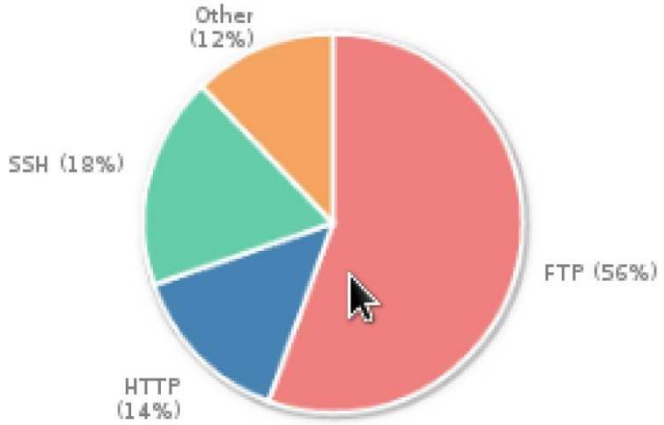

Figura 4 - percentual de tráfego por protocolo - Ntop - BROL

A figura 4 mostra que 56% do tráfego da rede trata-se de transferências de arquivos usando o protocolo FTP, uma mudança nesse comportamento pode sinalizar uma anomalia no tráfego. Além do tipo de protocolo predominante a forma como ocorrem as requisições e o envio e recebimento dos dados possuem características específicas

1.5 Ataques Cibernéticos

Segundo France (2009), o diretor adjunto da divisão de informática do FBI em 2009, Shawn Henry, declarou que a declarou em um congresso em Nova York que a guerra cibernética está entre as três maiores ameaças mundiais, ao lado das armas de destruição em massa e uma bomba em uma metrópole, Ainda segundo a mesma fonte o secretário-adjunto de segurança pública do estado de Nova York, Michael Balboni, descreveu a possibilidade de uma guerra como o Apocalipse e ressaltou o risco que a infraestrutura norte-americana está sujeita

O Brasil investe em pesquisas e desenvolvimento de novas tecnologias para prevenção de ataques cibernéticos de grandes proporções. Os exemplos mais recentes são a criação do Consorcio Brasileiro de Honeypots, as pesquisas e trabalhos desenvolvidos pelo Instituto Nacional de Pesquisas Espaciais (INPE) e pelo Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil (Cert-BR) voltadas para a defesa da infraestrutura tecnológica nacional.

2. BR ON-LINE- BROL

O BR On-line(BROL) é uma instituição governamental vinculada ao Ministério da Agricultura, Pecuária e Abastecimento (MAPA). Sua missão é prover informações meteorológicas à sociedade brasileira e influir, construtivamente, no processo de tomada de decisão, contribuindo para o desenvolvimento sustentável do País. Esta missão é alcançada por meio de monitoramento, análise e previsão de tempo e de clima, que se fundamentam em pesquisa aplicada.

Para concretizar sua missão o BROL necessita de diversos recursos computacionais que funcionam em rede. Estes ativos processam dados internamente e se comunicam com diversos outros sistemas ao redor do mundo recebendo e transmitindo dados.

São estes dados que permitem ao Instituto realizar sua missão fim. O comprometimento dos mesmos irá, definitivamente, prejudicar a qualidade do serviço por ele prestado. A seguir descreve-se a infraestrutura computacional do Instituto, necessária para que realize sua função.

2.1 Redes de Servidores e Armazenamento de Dados do BROL

A rede de servidores e armazenamento de dados do BROL é composta, fisicamente, por duas Salas-cofres onde são oferecidos serviços com Alta Disponibilidade e Alto Desempenho. A figura 5 mostra o esquema das salas cofres abaixo:

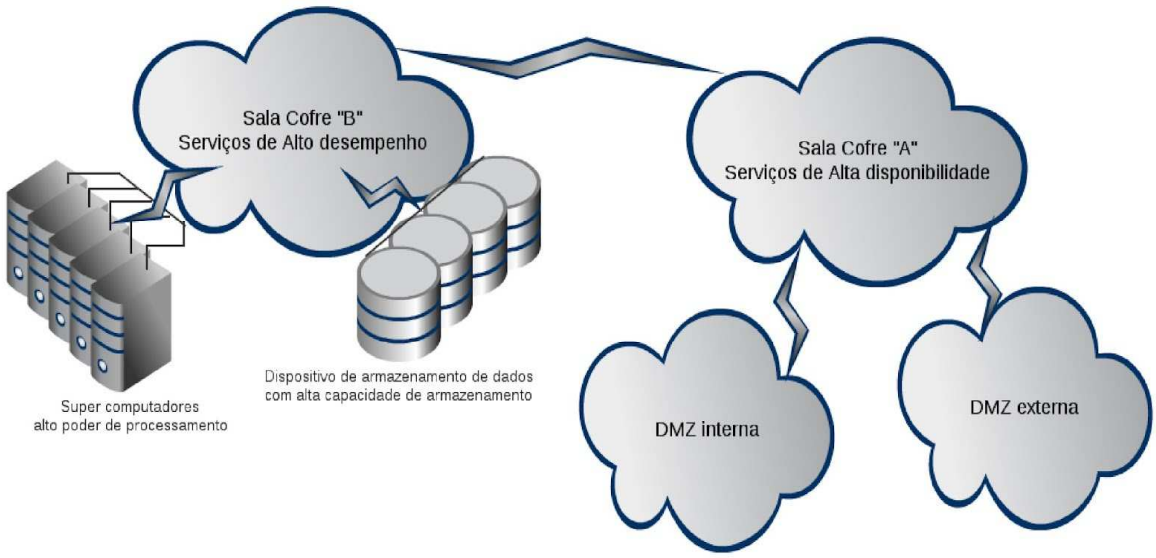

Figura 5 - Esquema das Salas Cofres - BROL

O serviço de alta disponibilidade é responsável por manter os serviços de agrometereologia, com importância estratégica para a produção de alimentos no Brasil, e de fornecimento de boletins com avisos e alertas sobre as condições metereológicas em funcionamento 24 (vinte e quatro) horas por dia durante os 7 (sete) dias da semana. Ela é composta por servidores e dispositivos de armazenagem de dados trabalhando em conjunto de forma que mesmo que um servidor ou uma controladora de armazenamento pare de funcionar, o outro equipamento assume os serviços, sem interrupção.

O serviço de alto desempenho é conseguido através do uso de Supercomputadores, responsáveis pelo processamento dos modelos metereológicos. A capacidade de processamentos destas máquinas chega a 45 teraflops.

Este trabalho foca a análise de parte do tráfego da rede correlacionando os dados obtidos com as informações dos registros de segurança (*logs*) gerados pelos sistemas operacionais dos servidores, focando os serviços HTTP (sítio), FTP

(transferência de arquivos). A figura 6 apresenta um esquema simplificado da rede analisada.

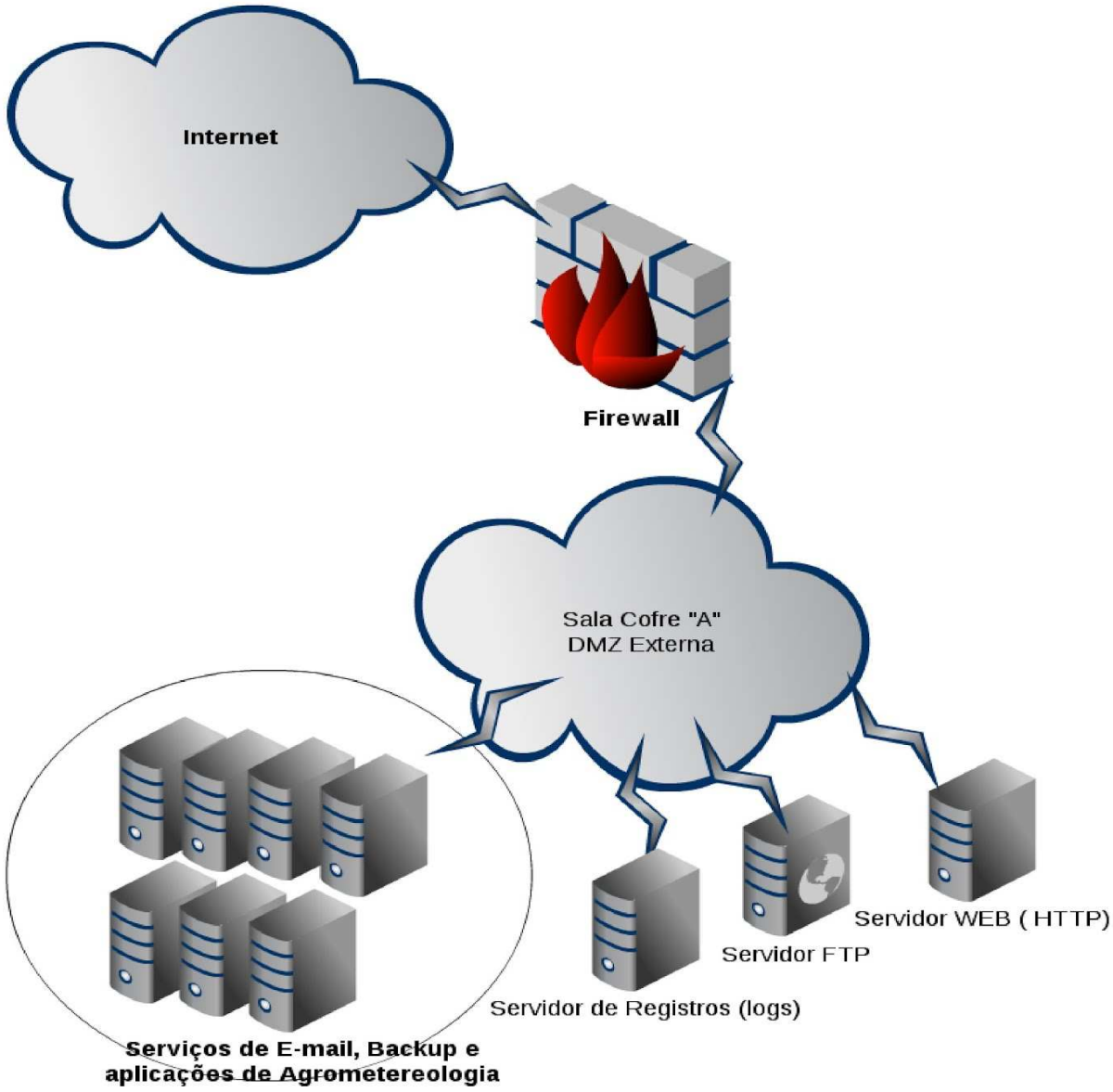

Figura 6 - Rede interna - esquema simplificado - BROL

2.2 Servidores de Registros de Segurança

A rede interna centralizar todos os registros de segurança em uma única máquina. Os eventos são coletados por programas executados nas estações servidoras que os transmite para este servidor central onde eles são armazenados e onde podem ser consultados para posterior análise.

Para coletar, armazenar e analisar os dados de tráfego da rede e os registros de segurança gerado pelos servidores usa-se uma Maquina Virtual (VM) com armazenamento de dados externo disponibilizado através do protocolo de sistema de arquivos em rede NFS. O Sistema Operacional tanto da maquina virtual, como da maquina física é o RedHat Enterprise Edition na versão 6.2 - 64 bits. O Sistema gerenciador de logs usado é o Rsyslog.

2.3 Rsyslog

O rsyslog é utilizado nesse trabalho para tratar os dados dos registros de segurança enviados pelo servidor de logs.

Com o Rsyslog é possível definir quais mensagens que serão coletadas, além da origem e do destino de tais mensagens. No Sistema Operacional RedHat o Rsyslog é configurado no arquivo /etc/rsyslog.conf contendo basicamente o seguinte formato: facilidade.nível destino

- Facilidade: usada para especificar que tipo de programa está enviando a mensagem;
- Nível: especifica o nível de gravidade da mensagem; e

- Destino: especifica para onde deve ser mandada a mensagem.

Segue abaixo a parte da configuração no arquivo /etc/rsyslog.conf nas estações servidoras de transferência de arquivo (FTP) e página de internet (HTTP) para envio dos registros ao servidor de análise de registros.

. @<IP do servidor de análise de log>

Por padrão o Rsyslog envia as mensagens de registro para a porta UDP 514, é necessário configurar o firewall do servidor de registros para aceitar conexões nessa porta. Acrescenta-se, no servidor, a seguinte linha no arquivo /etc/sysconfig/iptables:

-A INPUT -m state --state NEW -m udp -s <IP da maquina geradora dos registros> -p udp --dport 514 -j ACCEPT

Além da configuração do firewall da máquina centralizadora de logs já necessidade de inicializar o syslogd – deamon servidor que fica escutando a porta UDP 514 aguardando mensagens – com a opção -r. Isto pode ser feito ou editando o arquivo de inicialização /etc/init.d/syslog ou o arquivo /etc/sysconfig/syslog.

Se não quiser editar os arquivos de configuração, basta terminar o processo do syslogd e carregá-lo manualmente com a opção -r:

syslogd –m 0 -r

Os arquivos de *log* crescem sem parar. Para facilitar a análise e otimizar o armazenamento em disco, foi utilizado o *logrotate*, uma ferramenta responsável por rotacionar os arquivos de logs. Foi definido que se deseja o rotacionamento diário dos arquivos de logs independentemente do tamanho dos arquivos e que os arquivos gravados não podem ser sobrescritos por 30 (trinta) dias.

Além do rotacionamento dos arquivos o *logrotate* é utilizado para indicar o método de compressão e o local onde os arquivos serão armazenados, no caso deste trabalho na partição provisionada pelo dispositivo de armazenagem externo montada no diretório */log*.

2.4 Registros de segurança dos serviços HTTP e FTP

Este trabalho contempla a análise da parcela do tráfego da rede direcionada aos servidores HTTP e FTP e dos registros de segurança gerados pelos mesmos.

A análise dos registros gerados pelos serviços HTTP e FTP visa identificar anomalias no tráfego que sinalizem um possível ataque cibernético, que pode causar indisponibilidade dos serviços prestados pelo BROL que, dependem dos seus recursos computacionais.

O serviço HTTP é muito importante para o cumprimento da missão do BROL, através dele os usuários acessam as informações metereológicas geradas pelo Instituto. A análise do tráfego do servidor HTTP consiste na captura dos pacotes de entrada e saída em sua interface de rede voltada para a Internet. Os dados gerados

pela análise do tráfego de rede do servidor HTTP são correlacionados com os *logs* gerados pelo *daemon* HTTPD, aplicativo responsável pelo serviço HTTP, encontrado em /etc/httpd.

Por estar em produção, o serviço HTTP possui um tráfego conhecido. Tal tráfego possui um comportamento com pouca variação. Para monitorar o comportamento dos acessos ao sítio, incluindo novas visitas, origem das requisições de acesso entre outras informações, é utilizada o serviço Analytics da empresa Google que mostra de forma gráfica estatísticas do serviço HTTP, como se pode ver na figura 7

Conhecer o comportamento dos acessos ao serviço HTTP é importante porque esse trabalho foca identificar comportamentos que diferem do conhecido, ou seja, as exceções. A figura 7 mostra o numero de visitas representadas por um gráfico. É possível identificar um comportamento semelhante no numero de acessos em determinados dias da semana. É possível perceber uma diminuição nos acessos aos sábados e domingos (dias 14,15,21,22,28,29 de julho e 4,5 de agosto). Mostra também o número total de novas visitas e o número de acessos que são retorno sitio.

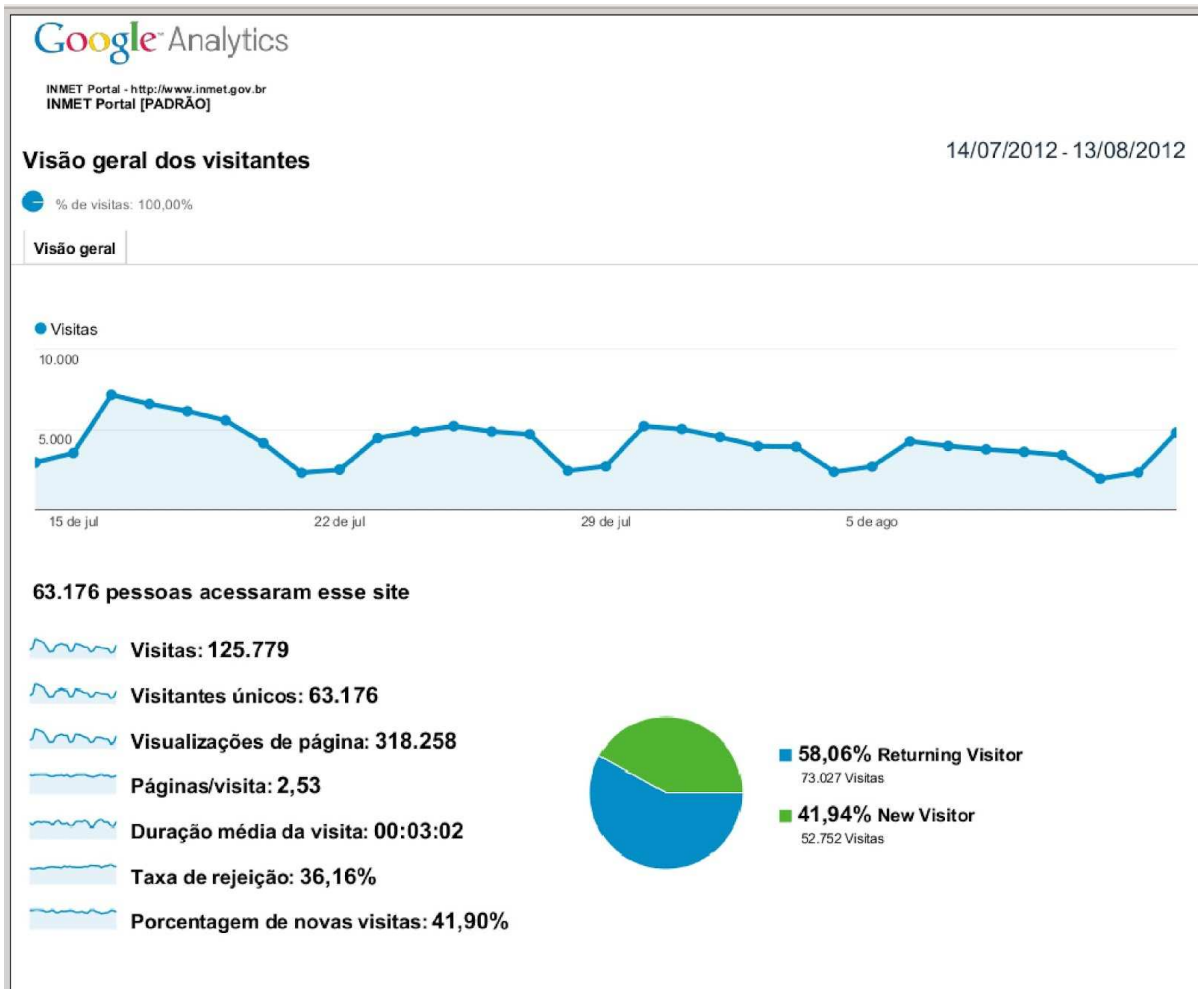

Figura 7 - Gráficos de acesso ao sítio www.BROL.gov.br - Google Analytics

Assim como no servidor HTTP, o serviço FTP possui grande importância para o cumprimento da missão do BROL, é através dele que os dados metereológicos são recebidos de outros centros para serem processados e que, depois de processados, são enviados para órgãos que necessitam destes dados, seja no Brasil ou no exterior.

Os dados são enviados e recebidos através do aplicativo AFD (Automatic File Distributor), que gerencia o recebimento e o envio dos arquivos de forma automática utilizando o protocolo FTP. Os registros de transferência de arquivos são gerados pelo *daemon* VSFTPD e armazenados em /var/log/xferlog e enviados para o servidor

de registros. Existe outro arquivo onde são encontrados registros úteis para análise dos acessos ao serviço FTP encontrado em /var/log/audit/audit.log. O arquivo audit.log recebe registros gerados pelo sistema operacional relacionados a segurança.

A figura 8 apresenta uma captura da tela da interface do aplicativo AFD. A visualização dessa interface é importante, pois através dela é possível identificar falhas no envio de dados (cor vermelha), o que pode sinalizar uma anomalia no tráfego.

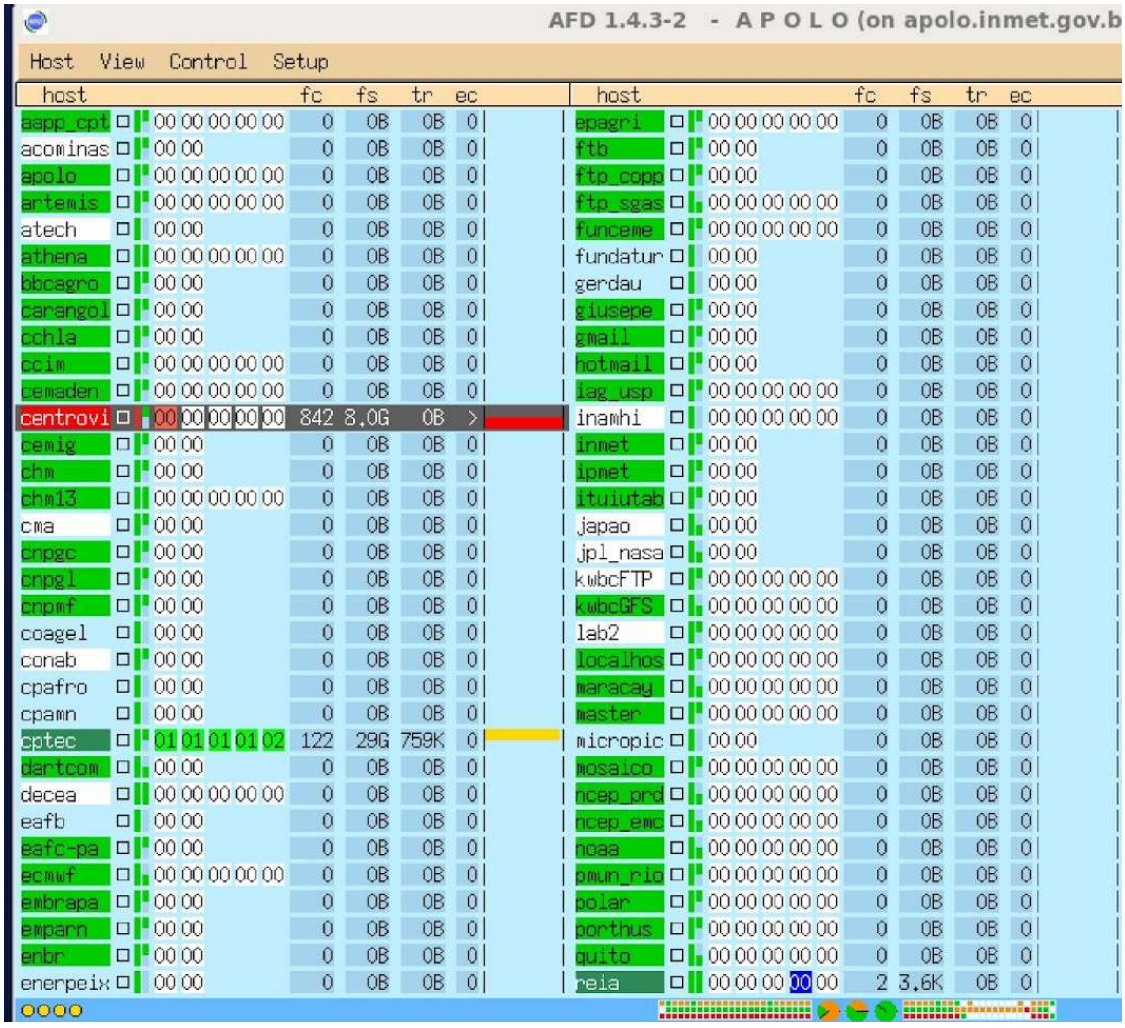

Figura 8 - Interface do aplicativo AFD - Mostrando um erro no envio de dados - AFD

O resultado da análise do tráfego da interface de rede voltada para a Internet do servidor FTP será correlacionada com os registros gerados pelo *daemon* VSFTPD. O arquivo /var/log/xferlog, possui informações da origem e destino do tráfego FTP, tamanho dos arquivos transferidos.

3. COLETA DO TRÁFEGO DE REDE

Este trabalho analisa a parcela do tráfego de rede direcionado aos servidores de FTP e HTTP, os registros de segurança gerados pelos sistemas operacionais das maquinas servidoras e os gerados pelos programas responsáveis pela transferência de arquivos e página de Internet. Usa-se ferramentas de código aberto para identificar, classificar comportamentos anômalos e gerar alertas de acordo com parâmetros pré estabelecidos. A figura 9 mostra o esquema da análise.

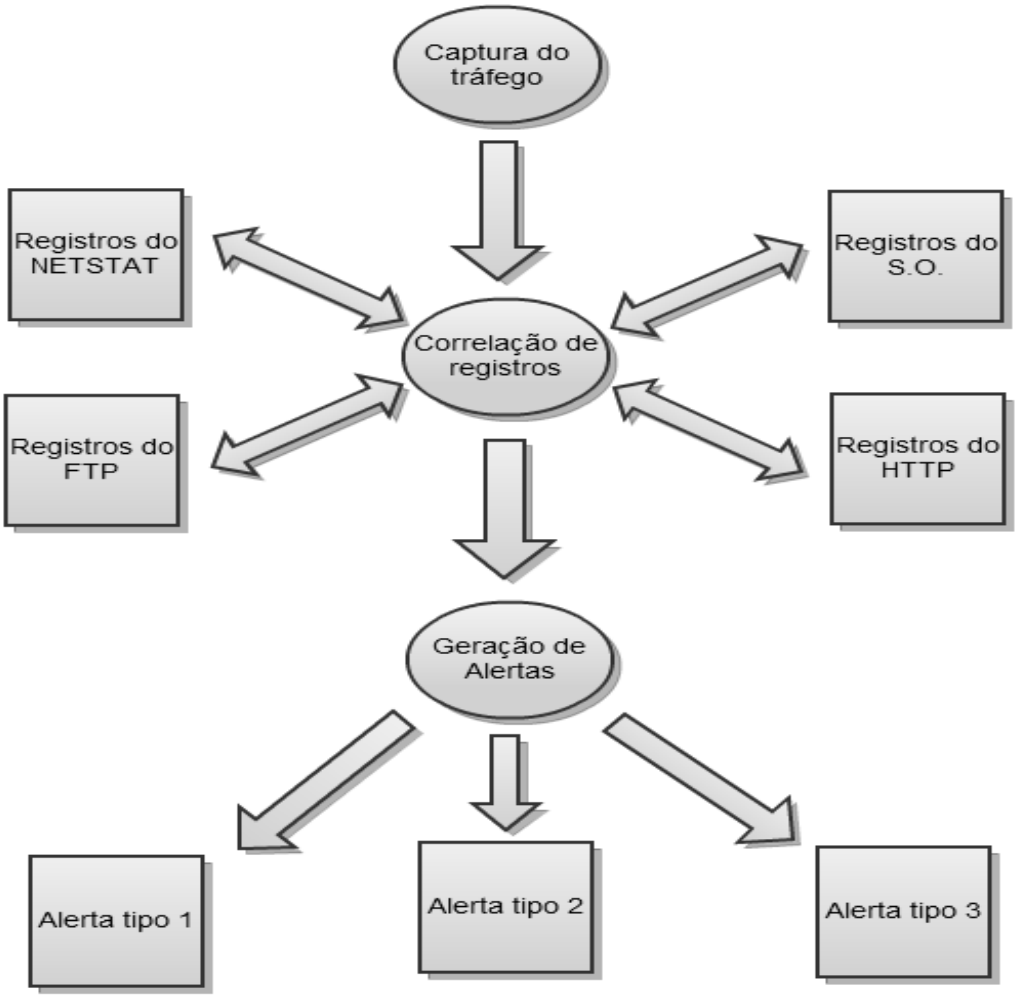

Figura 9 – Digrama do modelo de análise de tráfego

Os servidores HTTP e FTP estão em produção e possuem tráfego legítimo, a análise do tráfego irá focar principalmente as exceções, isto é, a parcela do tráfego que apresenta algum tipo de anomalia seja no volume ou no tipo de tráfego. Para isso, serão utilizadas as ferramentas *tcpdump, o netstat* e programas para análise dos registros.

A ferramenta utilizada para captura do tráfego de rede direcionado aos servidores HTTP e no servidor FTP é o *tcpdump*. Foi criado um pequeno programa para auxiliar a captura do trafego cujo código é:

```
#!/bin/bash
DATA=`date +%Y%m%d%I%M%S`
/usr/sbin/tcpdump -i eth0 -nn -vvv not net 192.168.168 -c 1000000 > tcpdump_<nome do computador>_${DATA}
cd /var
./cap.sh &
```

Usando o código acima foi criado o aplicativo cap.sh, que fará a captura do tráfego de rede. Esse aplicativo será executado tanto no servidor de FTP como no HTTP. Uma vez iniciado o cap.sh captura todo o tráfego direcionado aos servidores. A cada milhão de pacotes capturados rotaciona gerando um novo arquivo com data. Desta forma sempre terá apenas uma instância do cap.sh em execução. Os parâmetros da linha de comando indicam:

- -i nome da interface onde os pacotes serão capturados;

- -nn para que o aplicativo não tente converter endereços IP em nomes;
- -vvv para que um grande número de detalhes do pacote seja gravado;
- -c limita o conteúdo do arquivo para uma determinada quantidade de bytes, neste caso um milhão.

A saída deste processamento é redirecionada para um arquivo cujo nome contém o nome da máquina sendo monitorada seguida da data previamente obtida. Em seguida o aplicativo cap.sh é reiniciado.

O netstat é um programa que obtem informações estatísticas das conexões de rede direto do kernel do sistema. O uso do Netstat também possibilita visualização de dados em todas as camadas da pilha TCP/IP.

Foi criado um pequeno programa para auxiliar capaz de colher estatísticas das conexões de rede a cada 5 minutos nos servidores FTP e HTTP. Veja o código abaixo:

```
#!/bin/bash
DATA=`date +%Y%m%d%I%M`
/bin/netstat  -pntu > /pesquisa/estatistica<nome do computador>_${DATA}
sleep 300
pkill netstat
cd /var
./estatistica.sh &
```

O código acima carrega para a variável local DATA a data atual, com precisão de segundo, obtida com o comando date. A próxima linha executa o comando netstat com os seguintes parâmetros:

- -p exibe o número do processo e o nome do programa de uma conexão
- -n não tenta converter endereços IP em nomes de domínio
- -t lista todas as conexões TCP
- -u lista todas as conexões UDP

A saída deste processamento é redirecionada para um arquivo cujo nome contém o nome da máquina sendo monitorada seguida da data previamente obtida. O aplicativo estatística.sh, que contem o código mostrado acima é executado uma vez a cada cinco minutos (sleep 300).

4. ANÁLISE E CORRELACIONAMENTO DE DADOS

A identificação do tráfego anômalo é feita com a análise do comportamento das conexões. Para isso, usaremos os dados obtidos com o tcpdump, como mostrado no capitulo quatro. Neste capítulo serão apresentados, nas próximas sessões, os testes de laboratório que permitiram avaliar o comportamento normal da rede no BROL. Será utilizado como parâmetro para classificar um tráfego como anômalo calculo do desvio padrão da média do volume de pacotes trafegados em uma transferência com um arquivo de 256 KB que é o tamanho do menor arquivo transferido no servidor FTP na rede do BROL e, a quantidade de pacotes transmitidos em um acesso HTTP. Será caracterizado como tráfego anômalo qualquer conexão que tiver um número de pacotes trafegados inferior a 10% do desvio padrão.

A análise terá duas etapas: Identificação da origem do tráfego anômalo, busca dos endereços IP de origem nos arquivos de registros gerados pelo sistema operacional e pelos programas de FTP e HTTP.

4.1 Quantidades de pacotes trafegados por conexão FTP

Em testes realizados em laboratório, foi constatado que para transmitir 256 KB de uma estação de trabalho X para o servidor FTP ocorre um tráfego onde em média são trocados 355 pacotes, incluindo requisição, login, envio do arquivo e logout.

Foram realizados quatro testes de envios de arquivos de 256 KB ao servidor de FTP, sendo dois de redes internas do BROL e dois de uma rede externa. Esse tamanho foi escolhido porque os arquivos enviados e recebidos através de FTP, na rede do BROL, possuem um tamanho mínimo de 256 KB. Veja abaixo mais detalhes do teste realizado para obter informações de uma conexão “normal” do serviço FTP:

- Na estação de trabalho

Geração de um arquivo de 256 KB:

```
dd if=/dev/zero of=/home/user/teste-ftp bs=256k count=1
```

Envio do arquivo:

```
ftp servidor-FTP
put teste-ftp
exit
```

- No servidor

Antes do cliente abrir conexão:

```
#tcpdump -i eth0 -vvv host <IP rede interna> and not port 22 > teste1
#tcpdump -i eth0 -vvv host <IP rede externa> and not port 22 > teste2
#tcpdump -i eth0 -vvv host <IP rede interna> and not port 22 > teste3
#tcpdump -i eth0 -vvv host <IP rede externa> and not port 22 > teste4
```

Após terminar a conexão:

#wc -l teste1

320 teste1

#wc -l teste2

396 teste2

#wc -l teste3

323 teste3

#wc -l teste4

384 teste4

Para calcular a média de pacotes por transferência de arquivo foi utilizada a média ponderada. Equação 5.1

$$m = \frac{x1+x2+xn}{xn}$$ (4.1 Média ponderada[1])

X=320+396+323+384/4 ≃355 (pacotes por transferência de arquivo de 256 KB)

Para calcular a variância nas transferências foi utilizado o cálculo da variância na equação 5.2

$$\sum (xi - Média)^2 / (n - 1)$$ (4.2 Calculo da Variante [2])

| 320 - 355 | = 35

| 396 - 355 | = 41

| 323 - 355 | = 32

[1] Referência: http://www.brasilescola.com/matematica/media-ponderada.htm
[2] Referência: http://www.infoescola.com/estatistica/variancia-e-desvio-padrao

| 384 - 355 | = 29

Foi utilizada a equação 5.3 para calcular o desvio padrão com os dados dos cálculos da variância.

$$s = \sqrt{\sum (x_i - \text{Média})^2 / (n - 1)} \qquad \text{(4.3 Desvio Padrão[3])}$$

$D^2=(35^2+41^2+32^2+29^2)/4$

$D^2=4771/4$

$D=\sqrt{1192}$

$D=\simeq 34$

| 34 - 355 | = 321 * 0.9 ≃ 288

A média por conexão de pacotes trafegados nos testes foi de ≃355 com um desvio padrão de ≃34. Podemos dizer então que, qualquer tráfego com a mesma origem direcionada ao servidor FTP com menos de 288 pacotes pode ser considerada anômala.

Conexão FTP - Em uma conexão FTP bem sucedida ocorrem a transferência de aproximadamente 355 pacotes entre a origem e o destino (Servidor FTP). Usando o calculo do desvio padrão chegou-se a conclusão que um tráfego direcionado á porta 21 com menos de 288 pacotes trafegados não pode ser considerado normal.

[3] Referência: http://www.infoescola.com/estatistica/variancia-e-desvio-padrao/

Utilizando o programa em shell mostrado abaixo, conseguiu-se identificar no arquivo gerado pelo tcpdump os endereços de origem que continham menos de 288 pacotes trafegados na conexão, lembrando que cada arquivo contem um milhão de pacotes.

```
for file in `ls tcp*`; do
  grep ^[012] $file | tr -s " " | tr " " "|" | cut -d"|" -f18 | grep -v "192.168." | cut -d"." -f1-4 | grep -v ^$ | grep ^[0-9] | sort | uniq -c |  tr -s " " | tr " " "|" >> result.$$
  for line in `cat result.$$`; do
        lcount=$(echo $line | cut -d"|" -f2)
        ip=$(echo $line | cut -d"|" -f3)
        if [ $lcount -lt 288 ]; then
          echo $lcount $ip >> z_ip.all
          echo $ip >> z_ip
        fi
  done
  rm -rf result.*
done
```

4.2 Quantidades de pacotes trafegados por conexão HTTP

Testes para identificar a quantidade de pacotes trocados em conexões de quatro estações de trabalho diferentes acessando o serviço HTTP do BROL em um período de tempo de 5 segundos. Os testes mediram o acesso á pagina do sítio do BROL através de dois navegadores diferentes: Chrome (Google) e Firefox (Mozilla).

Veja abaixo mais detalhes do teste realizado para obter informações de uma conexão “normal” ao serviço HTTP:

- Nos clientes:

Acesso ao sítio do BROL no endereço www.BROL.gov.br durante 5 segundos, utilizando os navegadores Firefox e Chrome. Três estações de trabalho diferentes, duas da rede interna do BROL e duas de redes externas.

- No servidor

Monitorar o tráfego com origem na estação de trabalho, exclui os pacotes gerados pela conexão SSH e direciona para o arquivo “qnt-pacotes-http”:

#tcpdump -i eth0 -vvv host <ip da estação de trabalho 1> and not port 22 > teste1

#tcpdump -i eth0 -vvv host <ip da estação de trabalho 2> and not port 22 > teste2

#tcpdump -i eth0 -vvv host <ip da estação de trabalho 3> and not port 22 > teste3

Após terminar a conexão:

#wc -l teste1 (rede interna)

782 teste1

#wc -l teste2 (rede interna)

1083 teste2

#wc -l teste3 (rede externa)

1154 teste3

Para calcular a média de pacotes por transferência de pacotes em um acesso foi utilizada a média ponderada. Equação 5.1

X=782+1083+1154/3 ≃1006 (pacotes por acesso.)

Para calcular a variância no acesso ao serviço HTTP foi utilizado o cálculo da variância na equação 5.2:

| 782 - 1006 | = 224

| 1083 - 1006 | = 72

| 1154 - 1006 | = 148

Assim como no Item 1 deste capitulo, foi utilizada a equação 5.3 para calcular o desvio padrão com os dados dos cálculos da variância.

$D^2=(224^2+72^2+148^2)/3$

$D^2=77264/3$

$D=\sqrt{25754}$

D≃160

| 160 - 1006 | = 846 * 0.9 ≃761

A média de pacotes trafegados nos testes foi de ≃1006 com um desvio padrão de ≃160. Podemos dizer então que, qualquer tráfego com a mesma origem

direcionada ao servidor FTP com menos de 761 pacotes pode ser considerada anômala.

Utilizando o programa em shell mostrado abaixo, conseguiu-se identificar no arquivo gerado pelo tcpdump os endereços de origem que continham menos de 761 pacotes trafegados na conexão, lembrando que cada arquivo contem um milhão de pacotes.

```
for file in `ls tcp*`; do
  grep ^[012] $file | tr -s " " | tr " " "|" | cut -d"|" -f18 | grep -v "192.168." | cut -d"." -f1-4 | grep -v ^$ | grep ^[0-9] | sort | uniq -c |  tr -s " " | tr " " "|" >> result.$$
  for line in `cat result.$$`; do
        lcount=$(echo $line | cut -d"|" -f2)
        ip=$(echo $line | cut -d"|" -f3)
        if [ $lcount -lt 761 ]; then
          echo $lcount $ip >> z_ip.all
          echo $ip >> z_ip
        fi
  done
  rm -rf result.*
done
```

4.3 Tentativas de acesso á portas não autorizadas

As portas de interesse para este trabalho são as listadas na Tabela 1:

Tabela 1 Portas, protocolos e serviços analisados

Porta	Protocolo	Serviço
21	TCP	FTP
80	TCP	HTTP

Como mencionado no capitulo 4, a obtenção dos registros de tráfego será realizada com o programa pesquisa.sh, com os arquivos de registros em mãos, é possível identificar os protocolos trafegados e as portas acessadas como nos exemplos abaixo:

- Identificação dos protocolos utilizados na conexão pelo IP de origem na conexão:

#cat tcpdump-servidorX_<data> |awk '{print $14, $18}'|sort | uniq -c| sort -rn >> lista_monitoramento

Os IPs que estiverem utilizando um protocolo diferente do TCP e tentando acesso em portas diferentes da porta 21 ou 80 ambas TCP serão enviados para o arquivo lista_monitoramento.

4.4 Correlações dos registros obtidos

A lista gerada contendo informações dos IPs de origem que foi gerada na primeira etapa será correlacionada com os registros gerados pelos programas Netstat e Rsyslog e pelos Daemons responsáveis pelo FTP e HTTP. Essa etapa é importante para determinar se o IP identificado tentou alguma forma de interação com os servidores e/ou serviços FTP e HTTP.

4.4.1 Correlação entre os registros de tráfego e os gerados pelo Netstat

A identificação dos IPs nos possíveis tráfegos anômalos ocorre no nível da camada de transporte da pilha TCP/IP, pois o tcpdump analisa pacotes (frames), unidade de dados dessa camada. O uso do Netstat possibilita a correlação entre informações da camada de transporte e da camada de aplicação da pilha TCP/IP.

Como mencionado no capitulo 4, foi gerado um código para executar o Nestat a cada 5 minutos nos servidores FTP e HTTP. Existe, então, uma janela de 4 minutos sem monitoramento por isso, a comparação entre os arquivos de registros gerados pelo Netstat e os gerados pelo tcpdump deve considerar esse fato. Isso faz com que apenas os registros do tcpdump gerados na hora em que o Netstat foi executado pode ser comparado. Isso pode diminuir os falsos negativos. A busca dos IPs identificados nos itens 1 e 2 do capitulo 5 nos registros gerados pelo Nestat ocorre da seguinte forma:

- Gerar o registro com Netstat:

netstat -pantu > /pesquisa/estatistica<nome do computador>_${DATA}

- Buscar IP no registro gerado pelo Netstat:

#grep <ip_identificado> estatistica-servidor-X_${DATA}

4.4.2 Correlação entre os registros de tráfego e os gerados pelo Sistema Operacional

Assim como no item 4.1 deste capítulo, a busca do IP_identificado nos itens 1 e 2 desse capítulo corre com uma pesquiso nos arquivos /var/log/secure e /var/log/messages gerados pelo Sistema Operacional. Esses arquivos possuem informações de segurança, ou seja, caso o IP_identificado tenha tentado algum tipo de interação com o Sistema Operacional, como acesso via SSH, o evento fica registrado e caso o acesso tenha sido bem sucedido, através dos registros *secure e messages* é possível identificar as ações executadas pelo “invasor”

Semelhantemente, como no parágrafo acima, a busca ocorre com uma pesquisa do IP_identificado nos arquivos *secure e messages:*

- Buscar IP no registro gerado pelo Sistema Operacional:

#grep <ip_identificado> /var/log/secure e;

#grep <ip_identificado> /var/log/messages

4.4.3 Registro de Tráfego e dos Programas de FTP e HTTP

A correlação entre os registros gerados pelo tcpdump e pelos programas de FTP e HTTP é muito importante porque diferente dos arquivos gerados pelo Netstat e pelo Sistema Operacional, esses arquivos de registros possuem informações específicas dos respectivos programas.

As principais informações que podem ser obtidas com os registros gerados pelo programa do HTTP e FTP são:

- Diretório ou página acessado (a)
- Informações de Login
- Arquivos Transferidos (enviados e recebidos)
- Ação executada

De igual modo, como no parágrafo acima, a busca ocorre com uma pesquisa do IP_identificado nos arquivos *access_log* e *error_log* do HTTP e xferlog do FTP

- Buscar IP nos arquivos de registro do FTP e HTTP:

#grep <ip_identificado> /var/log/httpd/access_log;

#grep <ip_identificado> /var/log/httpd/error_log;

#grep <ip_identificado> /var/log/xferlog;

4.5 Identificação da frequencia de tráfego anômalo

O monitoramento da frequencia em que um mesmo endereço IP aparece em um tráfego considerado anômalo possibilita prever uma possível tentativa de invasão.

A análise correlaciona a origem do tráfego com os eventos registrados pelo sistema operacional e pelos programas de FTP e HTTP. Dessa forma pode-se verificar se um mesmo endereço de origem está tentando alguma interação com o sistema. Isso pode caracterizar uma busca por vulnerabilidades por um hacker.

Para isso é necessário comparar os registros gerados anteriormente, na fase de identificação e correlação dos tráfegos anômalos. É importante ter tais registros armazenados e disponíveis para análise e comparação, pois apartir dessa análise de frequencia serão emitidos alertas.

A análise desta etapa busca, também, identificar eventos semelhantes com endereços de origem diferente. Pode haver uma correlação nos eventos e o “invasor” estar utilizando endereços de origem diferentes para não gerar alertas. Porém se o tipo de interação for semelhante, existe a possibilidade da atividade registrada estar sendo empreendida pela mesma “pessoa”.

Para permitir a identificação de tráfego anômalo com origens diferentes requer que se comparem os registros gerados na identificação dos tráfegos anômalos e na fase de correlação dos diferentes registros gerados pelo sistema operacional e pelos

programas de FTP e HTTP e pelo Netstat. . A planilha abaixo mostra o percentual de interações de IPs identificados com outros os registros. A tabela 2 mostra os resultados da análise de um dia:

Tabela 2 Interação de um endereço IP com registros de segurança

	FTP / porta 21	HTTP / porta 80
Netstat	79.2 %	30%
Registros de Segurança do Sistema Operacional	10%	0.1%
Registros do programa de FTP	0%	Não se aplica
Registros do programa de HTTP	Não se aplica	50%

5. GERAÇÃO DE ALERTAS

A etapa de geração de alertas produz três tipos diferentes de mensagens. Em cada caso são levadas em consideração as características do evento envolvido. Os alertas podem ser enviados por e-mail, ou mostrados em uma console de gerência de um programa de monitoramento, ou ainda interagir diretamente com equipamentos e programas de segurança, como Firewall, Roteador e sistemas de Detecção de Intrusão (Intrusion Prevention System -IPS).

A geração de alertas contribui para a segurança do sistema computacional estudado nesse trabalho porque possibilita uma reação ágil e precisa do administrador do sistema ou por meio automatizado com relação determinado evento.

Neste trabalho as mensagens de alertas são identificadas por cores (amarelo, laranja e vermelho), de acordo com as características das ocorrências registradas.

- Alerta Amarelo - Emitido quando uma mesma origem é identificada uma vez nos registros gerados pelo tcpdump. Esse alerta não é crítico, e podem ocorrer falsos positivos nessa fase da análise. O alerta pode ser enviado apenas para um sistema de monitoramento.

- Alerta Laranja - Emitido quando vários eventos semelhantes são identificados e com mesma origem. Esse tipo de tráfego pode sinalizar que um hacker estar tentando interação utilizando métodos semelhantes de reconhecimento

dos servidores e/ou serviços de FTP e HTTP. Esse tipo de alerta envia uma mensagem para um sistema de monitoramento e via correio eletrônico para o operador responsável pela segurança e/ou sistemas envolvidos.

- Alerta Vermelho - Emitido quando vários eventos semelhantes são identificados podendo ou não ter a mesma origem e que ocorram todos os dias, levando em consideração que a análise de todos os dados é feita uma vez por dia. Esse conjunto de eventos pode sinalizar, por exemplo, métodos automatizados de reconhecimento e busca de vulnerabilidades nos servidores e serviços. Esse tipo de alerta deve interagir com equipamentos de segurança como Firewall, IPS e equipamentos de rede como roteadores, além de enviar uma mensagem de alerta para um programa de monitoramento e para o operador responsável pela segurança.

CONCLUSÃO

Este trabalho buscou, inicialmente, mapear o trafego de rede direcionado aos servidores de FTP e HTTP do BR On-lineafim identificar comportamentos inesperados nos acessos que pudessem sinalizar uma ação mal intencionada de um hacker.

Foi possível mapear o tráfego da rede direcionado aos servidores de transferência de arquivos e serviço de página de Internet.

Como demonstrado no item 1 do capitulo 5 e no item 4 do capitulo 2 o trafego direcionado aos servidores de FTP e HTTP do BROL possui características que permitem determinar o volume de pacotes mínimo para uma conexão “normal”. Usando conceitos estatísticos e o calculo do desvio padrão, constatou-se o seguinte:

Foi possível identificar o tráfego que possui um volume abaixo do considerado normal para uma conexão real.

O resultado da execução do programa em Shell mostrado no final do item 1 do capitulo 5 gerou uma lista de endereços IPs para cada arquivo. Os resultados encontrados foram comparados com os demais arquivos do mesmo dia. Desta forma diminuem-se falsos positivos, uma vez que um endereço IP pode ser encontrado em um pacote com menos de 288 pacotes trafegados e no pacote seguinte possuir mais de uma ou mais ocorrências.

Conexão HTTP – Como já mencionado no item 2 do capitulo 5 em uma conexão HTTP bem sucedida ocorrem a transferência de aproximadamente 1006 pacotes entre a origem e o destino (Servidor FTP). Usando o calculo do desvio padrão chegou-se a conclusão que um tráfego direcionado á porta 80 com menos de

761 pacotes trafegados não pode ser considerado normal. Foi possível determinar quais endereços IP de origem possuíam menos de 761 pacotes trafegados.

Foi possível correlacionar os resultados obtidos com os registros de segurança gerados pelo Sistema Operacional e respectivos programas de FTP e HTTP.

Para determinar se houve interação do endereço IP com o sistema operacional ou com os aplicativos de FTP e HTTP foi feito uma busca nos arquivos de registros de segurança do sistema operacional, nos arquivos gerados pelo netstat e nos registros de segurança gerados pelos programas de FTP e HTTP

Sugestões de tratativas para o tráfego anômalo

Existem vários procedimentos que podem ser executados após a identificação do tráfego anômalo. As tratativas vão depender da política de segurança da instituição.

Antes é necessário lembrar que um tráfego anômalo não é, necessariamente, um ataque cibernético, então uma opção de tratamento que não envolva bloqueio imediato seria encaminhar o tráfego para outro servidor, uma espécie de espelho com características semelhantes e com o mesmo conteúdo do servidor principal,. Isso possibilitaria uma análise mais criteriosa e, em um eventual ataque, o servidor principal não seria comprometido.

Sugestões de trabalhos futuros

Sugestão para trabalhos futuros:

- Criação de um sistema que reúna todos os códigos mostrados nesse trabalho e que faça de forma automatizada a análise do tráfego, que aqui foi demonstrada passo-a-passo, cada etapa individualmente.
- O uso de banco de dados para armazenar os registros gerados pelo tcpdump, netstat, vsftpd, httpd e sistema operacional para otimizar a análise das informação.

REFERÊNCIAS

ANÔNIMO. Logs e Trilhas de Auditoria. In ANÔNIMO. Segurança Máxima em Linux. São Paulo, Campos Editora, 2000, p. 512-513.

ATHENIENSE. Alexandre. A Responsabilidade pelo Armazenamento de Logs. Disponível em: <http://www.dnt.adv.br/noticias/provas/a-responsabilidade-pelo-armazenamento-de-logs/> Acessado em: 14 de julho de 2012.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT. **Cartilha para Segurança na Internet,** V 4.0, P 53, 2012, Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 14 de julho de 2012.

COMITER GESTOR DA INTERNET NO BRASIL - NIC. **Praticas de Segurança para Administradores de Redes Internet,** V 1.2, P 19, 2003, Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf>. Acesso em: 14 de julho de 2012.

GALLAGHER. Michael. **Especialistas temem guerra cibernética no futuro**. In E-GOV. Disponível Em: <http://www.egov.ufsc.br/portal/conteudo/not%C3%ADcia-especialistas- temem-guerra-cibern%C3%A9tica-no-futuro > Acessado em: 17 de julho de 2012.

ISONI, M.M et al. E - crime em ambientes digitais informacionais da Internet. Revista Datagramazero, abril de 2007 . Disponível em : <http://www.dgz.org.br/abr07/Art_02.htm>. Acessado em: 14 de julho de 2012.

MONTES, Antonio; SILVA, Lia de Sá; SIMÕES, José Demisio. **Evolução dos Trabalhos de Detecção de Anomalias na Rede**. In WORCAP, São Paulo, out. 2005. Disponível em: <http://mtc-m18.sid.inpe.br/col/dpi.inpe.br/hermes2@1905/2005/10.04.01.42/doc/rev_lilia_worcap2005.pdf >. Acesso em: 15 julho. 2012.

PORTAL G1. **Lista de sites do governo atacados em 2011** . Disponível Em: <http://g1.globo.com/tecnologia/noticia/2011/06/veja-lista-de-sites-do-governo-afetados-por-onda-de-ataques-virtuais.html> Acessado em: 17 de julho de 2012.

PRESSE. France. **Ataques cibernéticos estão entre três maiores ameaças mundiais, diz FBI**. Disponível Em:

<http://www1.folha.uol.com.br/folha/informatica/ult124u487415.shtml> Acessado em: 17 de julho de 2012.

REDE NACIONAL DE ENSINO E PESQUISA - RNP. **Os Logs como Ferramenta e Detecção de Intrusão.** Disponível em: < http://www.rnp.br/newsgen/9905/logs.html#ng-o> . Acesso em: 14 de julho de 2012.

RFC 1112. Requirements for Internet Hosts. Communication Layers 1989. p 7 e 8. Disponivel em <http://tools.ietf.org/html/rfc1122>. Acessado em 12 de Agosto de 2012

TCPDUMP & Libcap. Documentation. Disponivel em: <http://www.tcpdump.org/#documentation> Acessado em: 13 de agosto de 2012