Aumentando a Segurança da Informação com Softwares Livres em uma Universidade

Carla Elaine Freitas Santos[1], **Jerônimo Aguiar Bezerra**[2]

[1]Ponto de Presença da RNP na Bahia (PoP-BA)
Rede Nacional de Ensino e Pesquisa (RNP)

[2]Centro de Processamento de Dados
Universidade Federal da Bahia (UFBA)

carla@pop-ba.rnp.br, jab@ufba.br

Abstract. *A University's computers network is pictured by its complexity, due to high amount of users, computers and services needed daily. Furthermore, others aspects of a IT environment makes it a target of continuos suspicious actions, compromising a security of the stored informations. This article describes a solution for the security control of a large environment, including the three pivot of security: firewall, network management and IDS. The solution showed use only free softwares.*

Resumo. *A rede de computadores de uma Universidade é caracterizada por uma complexidade, resultante da grande quantidade de usuários, computadores e serviços necessários no seu dia-a-dia. Além disso, outras características do ambiente de TIC universitário torna o mesmo alvo constantes de ações mal-intencionadas, comprometendo a segurança das informações armazenadas. Esse artigo descreve uma solução para o controle da segurança de uma rede de alto porte, englobando os três eixos de segurança: firewall, gerência de rede e IDS. Toda a solução apresentada utiliza apenas softwares livres.*

1. Introdução

Um dos grandes avanços tecnológicos das últimas décadas está relacionado com a comunicação pessoal. A criação da Internet e a sua popularização no meio da década passada permitiu a comunicação mundial de forma rápida, eficiente e barata. Dessa forma, a sociedade tem observado a importância da Internet tanto no sentido de trocas de informações, quanto como forma de negócios. Isso tem ocasionado um aumento acelerado dos serviços oferecidos através da Internet, como serviços Web, e-mail, Voz sobre IP, dentre muitos outros. A Internet, então, tornou-se uma complexa rede, com usuários do mundo inteiro e com os mais diversos objetivos, inclusive ilícitos.

Atualmente, estar conectado à Internet significa também ter uma grande preocupação com a segurança das informações pessoais, ou institucionais no caso de uma organização. A análise do tráfego de rede faz-se necessária para o bloqueio de pacotes maliciosos ou suspeitos, atuando como uma camada inicial de proteção do sistema. Além disso, a análise de tráfego permite também a verificação de anomalias da rede, como um aumento repentino do *throughput* de rede, que pode indicar a ação de algum *worm*; e a detecção de tentativas de intrusão ao sistema, através de sistemas de detecção de intrusão de rede (NIDS - *Network Intrusion Detection System*).

Neste cenário, um ambiente de TIC (Tecnologia da Informação e Comunicação) de uma Universidade é também marcado por uma extrema complexidade estrutural, envolvendo na maioria das vezes grandes quantidades de usuários, computadores e serviços. A Universidade com o seu papel de ser produtor de novas tecnologias está envolvida com o desenvolvimento de novos serviços e pesquisas, além dos tradicionais serviços já oferecidos, como os sistemas acadêmicos para os seus usuários e os demais serviços para o público externo.

O fornecimento de uma rede de alta qualidade é uma outra característica das redes acadêmicas. Políticas de QoS (*Quality of Service*), por exemplo, são utilizadas para manter a qualidade da rede, necessária para alguns serviços oferecidos, como VoIP (Voz sobre IP) e videoconferência. Isso aliado com o fato de possuirem redes de alta velocidade, uma diversidade de serviços e heterogeneidade de aplicações utilizadas, torna o ambiente de TIC universitário alvo constante de ações *crackers*.

Este artigo tem o objetivo de ilustrar as medidas tomadas e as ferramentas livres escolhidas para o fortalecimento da segurança de um ambiente de TIC de uma Universidade, centradas em três eixos: *firewall*, gerência de rede e IDS.

2. Os três eixos da Segurança da Informação

2.1. Firewall

Um *firewall* é um conjunto de *software* e *hardware* combinados para proteger os recursos computacionais internos e as informações sigilosas de uma organização contra acessos não autorizados. Existem dois tipos de *firewalls*: filtro de pacotes e *firewall* de aplicação. Um filtro de pacotes tem o objetivo de bloquear os acessos indesejáveis a partir de decisões de filtragem que são feitas, normalmente, basedas nos endereços IP e portas de origem e destino, tipo de mensagem ICMP (*Internet Message Control Protocol*) e *flags* do protocolo TCP (*Transmission Control Protocol*). Os *firewalls* (ou *gateways*) de aplicação fazem uma análise acima dos cabeçalhos, examinando o conteúdo do pacote.

Uma combinação entre os dois tipos de *firewalls* asseguram um nível mais refinado de segurança, aumentando a proteção do sistema, quando bem configurados. Neste trabalho não será apresentado nenhum *firewall* de aplicação, pois ainda não foi implementado, mas uma sugestão interessante de ferramenta é o Squid. Algumas configurações interessantes para serem implementadas incluem medidas *anti-spoofing*, bloqueando pacotes com dados do cabeçalho falsos; criação de redes DMZ (*DeMilitarized Zone*) para a localização de servidores; restrição dos serviços acessados de e para a rede DMZ; controle do protocolo ICMP; medidas contra ataques *syn flood*, etc.

A solução de *firewall* escolhida foi o **Netfilter**. Netfilter é o filtro de pacotes, disponível a partir da série 2.4 do *kernel* do Linux. Algumas características do Netfilter são: capacidade para monitorar o tráfego da rede, NAT (*Network Address Translator*), redirecionamento, marcação e modificação da prioridade de pacotes, e balanceamento de carga; características fundamentais para a implementação de um ambiente seguro.

O Netfilter tem uma arquitetura modular que permite a adição de novas funcionalidades através de módulos. Alguns módulos interessantes utilizados foram:

- `psd`: para a detecção e controle de *scan* de portas TCP e UDP;

- `time`: permite a filtragem baseada no hora e/ou data de chegada do pacote;
- `connlimit`: permite a adição de regras de restrição do número de conexões TCP simultâneas, úteis no controle de ataques *syn flood* e da carga em um servidor;
- `ipv4options`: permite o uso de regras utilizando opções do cabeçalho IPv4, evitando ataques como *source routing*.

O Netfilter possui uma interface modo texto para o gerenciamento das regras, conhecida como **iptables**. Apesar de uma ser excelente ferramenta para *troubleshooting* de problemas, o iptables não é eficiente para o gerenciamento e criação das regras em ambientes de redes complexos, como o de uma Universidade. Para o gerenciamento das políticas do *firewall* foi escolhido o aplicativo **Firewall Builder**. Suas principais vantagens são: interface gráfica para a criação das regras, suporte a vários tipos de *firewall* como o iptables e o pf do OpenBSD, o que permite uma fácil migração, caso necessária, e uma estrutura orientada a objetos (*hosts*, endereços e redes são tratados como objetos), facilitando o processo de desenvolvimento e manutenção das regras.

2.2. Gerência de Rede

Gerência de rede é um conjunto de atividades voltadas para o planejamento, monitoramento, avaliação e controle dos serviços e aplicações oferecidos na infra-estrutura de rede de uma organização. Tem como objetivos principais maximizar o desempenho, alocar recursos diante de demandas, minimizar falhas, documentar e manter configurações, além de zelar pela segurança dos elementos que compõem a rede.

Diversos são os controles necessários para o bom gerenciamento da rede, que são classificados de acordo com o seu objetivo. Existem alguns guias de boas práticas para a gestão de ambientes de TIC no mercado, com recomendações de controles para a gestão, como o CobiT. Simplificando a estrutura proposta por esses guias, os grupos de controles adotados foram divididos nas seguintes gerências:

- **Gerência de desempenho**: o objetivo é quantificar, medir, analisar e planejar o desempenho dos componentes da rede e serviços;
- **Gerência de falhas**: o objetivo é detectar, registrar e reagir às condições de falha;
- **Gerência de configuração e documentação**: o objetivo é documentar as informações dos dispositivos de redes e serviços e manter a configuração dos mesmos;
- **Gerência de problemas e incidentes**: objetiva garantir que os problemas e incidentes são resolvidos e a causa investigada para prevenir qualquer reincidência;
- **Gerenciamento de logs**: o objetivo é criar uma estrutura segura para o armazenamento dos logs dos componentes da rede e uma metodologia de verificação dos mesmo.

O protocolo SNMP (*Simple Network Management Protocol*) é utilizado como base para o monitoramento, sendo responsável pela comunicação entre a estação de gerência e os agentes monitorados. A sua escolha é justificada por ser uma aplicação bastante utilizada e estável para o seu propósito, além de possuir já implementada uma série de MIBs padrões, que contém objetos importantes para o monitoramento de um determinado componente da rede, como a MIB-II e a HOST RESOURCES. Uma ferramenta livre com suporte ao SNMP é o Net-SNMP. Esse pacote contém ferramentas para realizar consultas SNMP, um *daemon* para receber as consultas e um *daemon* para receber *traps*.

Com base na divisão apresentada anteriormente, serão detalhadas as soluções adotadas nas próximas seções.

Gerenciamento de Desempenho

Para a quantificação, medição e análise dos dados de monitoramento são utilizadas as ferramentas Cacti e NTOP. Compreendem dados de monitoramento, a utilização da memória, CPU e rede de um *host*, por exemplo.

O **Cacti** é uma aplicação para o monitoramento da utilização dos recursos dos componente de uma rede. Algumas características do Cacti são interface Web para configuração, controle de acesso as informações, geração de gráficos a partir dos dados coletados.

O **NTOP** (*Network Traffic Probe*) é um aplicativo que funciona como *sniffer*, ouvindo os pacotes que passam pela interface de rede, gerando gráficos e estatísticas a partir desses dados. O NTOP é uma excelente ferramenta para monitoramento em tempo real das conexões, onde além da carga de rede usada no momento, é possível visualizar as sessões ativas, tipos de pacotes, taxas de entrada e saída, etc. Sua utilização no *firewall* permite uma visualização geral do tráfego da rede da organização.

Gerenciamento de Falhas

A detecção de falhas em qualquer componente da rede ou serviço é realizada com a ferramenta Nagios. Nagios é uma aplicação livre para monitoramento de uma rede de computadores. Sua principal função é realizar a verificação de hosts e serviços, enviando notificações quando ocorrer algum problema com a entidade monitorada e/ou tomar uma ação reativa ao acontecimento. Outras funcionalidades são: a capacidade de gerar relatórios sobre o monitoramento realizado, como por exemplo relatórios de disponibilidade, e a capacidade de gerar mapas da topologia da rede a partir da definição de hierarquias entre as entidades gerenciadas, funcionalidade esta que será também importante para a detecção de elementos inacessíveis, devido à indisponibilidade de elementos em posições superiores na árvore topológica.

Gerenciamento de Configuração e Documentação

A documentação de todos os componentes da rede, dos serviços e suas configurações é uma importante tarefa para facilitar administração do ambiente de TIC. Além disso, a documentação eficiente e organizada de todas as modificações e instalações realizadas auxilia na detecção de problemas e forma uma base de conhecimento para futuras modificações planejadas.

Uma ferramenta wiki é bastante interessante para o desenvolvimento em grupo de conteúdo, pois permite a rápida modificação de documentos e através do recurso de controle de versão possibilita a recuperação de uma ocasional perda de conteúdo. É utilizada, então, o TWiki para a gestão da documentação interna.

Gerenciamento de Problemas e Incidentes

A ocorrência de problemas no ambiente de TIC de um Universidade é frequente devido a quantidade de usuários, serviços e computadores presentes. Para o gerenciamento dos problemas e incidentes é importante uma ferramenta que permita a criação de chamados, documentação da solução encontrada para resolver o problema/incidente,

escalonamento de chamados entre funcionários e o acompanhamento dos mesmos. Uma aplicação livre que possue todas estas características é o RT (*Request Tracker*), escolhido por além de apresentar as características mencionadas anteriormente, é customizável, possui níveis de acesso as informações e permite a criação de chamados através de um e-mail ou de um formulário Web.

Gerenciamento de Logs

Os arquivos de registro do sistema, conhecidos como logs, são muito importantes na administração de redes, pois neles são registrados eventos relacionados aos vários componentes dos sistemas, como mensagens de erros, alertas, violações do sistema, entre outros. Contém muitos detalhes úteis ao administrador tanto para acompanhar o funcionamento do seu sistema como para ajudar na solução e prevenção de problemas. Adicionalmente, os logs desempenham um papel fundamental na segurança da rede, na medida em que podem registrar eventuais tentativas de ataque, alertando assim o administrador para que sejam tomadas medidas preventivas.

Porém, os arquivos de log apresentam uma vulnerabilidade evidente: devido ao fato deles serem armazenados no próprio sistema, que eventualmente pode vir a ser comprometido, eles podem ser alterados ou até mesmo apagados. Aliás, esta costuma ser uma das primeiras ações realizadas pelos *crackers* na tentativa de cobrir seus rastros e esconder as suas atividades. Uma solução para minimizar este problema é a implementação de um servidor com um maior nível de proteção para a centralização das mensagens de logs de todos os componentes da rede.

A solução livre para a implementação de um servidor de log é constituída pelas ferramentas livres: **syslog-ng**, como o servidor de log propriamente dito; **logrotate** para o controle do crescimento dos arquivos de logs; **stunnel**, para a implementação de um canal seguro, com criptografia para o envio das mensagens para o servidor; e o **swatch** para a análise dos logs em busca de alguma anomalia ou problema.

2.3. Sistema de Detecção de Intrusão

Vírus, *worm*, *rootkit* são termos constantemente presentes para as pessoas envolvidas com TIC. Situação esta que torna-se preocupante devido à dificuldade cada vez maior de detectar a presença de um *malware* (software malicioso) em um sistema comprometido e a sofisticação agregada aos *malwares* com a adição de uma grande quantidade de recursos, como por exemplo a gravação de um vídeo registrando as ações de um usuário no momento. Muitas vezes o usuário não percebe que seu computador está infectado e, consequentemente, não tem noção do que está acontecendo em seu sistema, inclusive se este está atacando outros computadores.

Portanto, é fundamental realizar uma análise do tráfego passante na rede de uma organização, verificando a existência de tráfego malicioso. Esta análise poderá inclusive detectar tentativas de intrusão, possibilitando que o administrador tome uma ação para combater a mesma, se necessário.

Para monitorar qualquer tipo de atividade suspeita passando pela rede, ou dentro dos servidores, são usados softwares chamados de IDS (*Intrusion Detection System*). Os IDS são divididos em duas classes: HIDS (*Host Intrusion Detection System*) ou NIDS (*Network Intrusion Detection System*). O HIDS se baseia no monitoramento do servidor

analisando o comportamento do sistema operacional e das aplicações e as modificações no sistema de arquivos. Uma ferramenta para verificação dos arquivos do servidor, detectando alterações não planejadas é o AIDE, que armazena um banco de dados com o HASH ou MD5 de todos os arquivos selecionados, e periodicamente, verifica se houve alguma modificação no HASH, ou seja, uma alteração nos arquivos.

Por outro lado, o NIDS analisa o tráfego de rede. Funcionando como um *sniffer*, captura o tráfego da rede e o analisa de acordo com vários padrões, chamados de assinaturas. Essas assinaturas são periodicamente atualizadas a cada descoberta de vulnerabilidade ou vírus. A partir da análise, o NIDS toma certas reações, como por exemplo, envia pacotes TCP RST para finalizar uma conexão, bloquea o endereço IP no *firewall*, envia emails para o administrador ou apenas registra um alerta em um arquivo ou banco de dados. Automatizando a verificação dos alertas, o NIDS pode ser configurado para abrir um chamado automaticamente, na ferramenta de gerenciamento de problemas RT, para alguns tipos de alertas. O Snort é um dos principais *softwares* para essa função. Possui atualizações periódicas, algumas livres e outras pagas, e todas as características citadas anteriormente.

Para gerenciar os alertas gerados pelo NIDS, já que a quantidade de registros gerados é muito grande em um ambiente universitário, foi escolhido o software BASE, que é uma aplicação Web para a geração de vários tipos de relatórios dos alertas.

3. Conclusão

Manter a segurança de um ambiente de TIC envolve o desenvolvimento de complexas medidas para o controle da ocorrência de ações indesejadas sobre a rede e serviços. O uso de ferramentas para o auxílio às atividades de administração de rede tem um importante papel na garantia do funcionamento pleno do ambiente. Este artigo mostrou que o Software Livre tem amadurecido bastante neste sentido, ilustrando a implementação de um ambiente seguro e controlado utilizando apenas aplicações livres.

As consequências diretas do gerenciamento eficaz da segurança do ambiente de TIC são a otimização do uso dos recursos, garantindo, assim, que as informações suportem os objetivos da organização, os riscos sejam adequadamente controlados e que haja um retorno aos investimentos realizados. E no caso específico da Universidade, o seu principal objetivo: a satisfação do usuário no acesso aos serviços.

Referências

Galstad, E. (2006). Nagios. Disponível em `http://www.nagios.org/`. Acesso em 26 Fev 2006.

Group, F. B. (2006). Firewall builder. Disponível em `http://www.fwbuilder.org/`. Acesso em 26 Fev 2006.

Inc., S. (2006). Snort - the de facto standard for intrusion detection/prevention. Disponível em `http://www.snort.org/`. Acesso em 26 Fev 2006.

Security, B. I. (2005). syslog-ng. Disponível em `http://www.balabit.com/products/syslog_ng/`. Acesso em 26 Fev 2006.

Team, N. C. (2006). netfilter/iptables project. Disponível em `http://www.netfilter.org/`. Acesso em 26 Fev 2006.