PROPOSTA DE UMA FERRAMENTA DE GERÊNCIA ATIVA DE REDES – NETACT

Rogério Carvalho Schneider, Antônio Rodrigo Delepiane de Vit
UNICRUZ – Universidade de Crua Alta, Departamento de Informática,
Cruz Alta – RS – Brasil
[stockrt, arodrigo]@unicruz.edu.br

Liane Margarida Rockenbach Tarouco
UFRGS – Universidade Federal do Rio Grande do Sul, Departamento de Informática,
Porto Alegre – RS – Brasil
liane@penta.ufrgs.br

Resumo

No processo de gerência de redes, a tomada de medidas administrativas normalmente é auxiliada pelo uso de ferramentas de gerência. Através da geração de relatórios com estatísticas do uso de rede torna-se possível identificar os pontos falhos de um sistema e, a partir destes dados, tomar medidas corretivas embasadas. Sendo assim, o objetivo deste trabalho é apresentar a integração dessa geração de relatórios, a partir de ferramentas já existentes, com uma base de dados histórica, com a finalidade de gerar padrões de rede e utilizar técnicas de identificação de desvios para diagnosticar, de forma automática, as anomalias de rede. O NetAct é uma ferramenta que auxilia na gerência de rede e que tem esta proposta, a de identificar um ponto falho e realizar um processo curativo, de forma autônoma e constante.

Palavras-chave: Gerenciamento, Redes de Computador, Monitoramento, Análise de Padrão Comportamental

Abstract

In the process of network management, the taking of administrative measures normally is assisted by the use of management tools. Through the generation of reports with statisticians of the net use one becomes possible to identify the defective points on a system and, from these data, to take based corrective measures. Being thus, the objective of this work is to present the integration of this generation of reports, from already existing tools, with a historical database, with the purpose to generate network standards and to use techniques of shunting line identification to diagnosis, of automatic form, the network anomalies. The NetAct is a tool that assists in the network management and that it has this proposal, to identify a defective point and to carry through a dressing process, by an independent and constant form.

Keywords: Management, Computer Networks, Monitoring, Pattern Behavior Analysis

Introdução

O uso de redes de computadores em ambientes corporativos e educacionais se faz cada vez mais presente. Esta tecnologia possibilita a comunicação entre os seus participantes dentro de um ambiente de forma prática e com baixo custo, e ainda fornece a possibilidade de se aplicar as mesmas facilidades de comunicação a longas distâncias.

Para que se mantenha a produção em funcionamento, é preciso monitorar a rede, fazer o seu gerenciamento e administração, e para isso uma equipe tecnicamente especializada torna-se necessária. Contudo, muitas vezes, não existe a possibilidade de se efetuar revezamento para monitoria do estado da rede 24 horas por dia. A maioria dos *softwares* livres disponibilizados para a gerência de redes apenas trata do fornecimento

de gráficos para análise humana do estado da rede, sendo este – o operador humano - o responsável pelas tomadas de decisão na administração/gerência da rede. A proposta deste trabalho é apresentar um sistema baseado em plataformas de *software* livre, que se valha das informações fornecidas por *softwares* reconhecidos de monitoria de rede, faça ele mesmo a análise das informações recebidas e tome por si próprio as decisões necessárias (agindo com um atuador), fazendo com que a correção dos problemas de gerenciamento (a eliminação de uma intrusão, por exemplo) seja feita no menor tempo possível, garantindo a manutenção e a estabilidade do acesso para os usuários e informando os acontecimentos ao administrador/gerente da rede.

Uma grande rede não pode ser gerenciada somente por esforços humanos. É necessária a utilização de ferramentas para seu auxílio. Conclui-se, daí, que uma rede que não pode ser gerenciada corretamente possui pouco valor [WAN03].

Implementação

A proposta do NetAct é a de utilizar-se um coletor de informações estatísticas de uso de rede já reconhecido (tal como o *tethereal* [COM05]) e montar uma base histórica de coletas para a definição de *baseline* de padrão comportamental das estações de rede.

A partir da geração do padrão de uso de rede, por cada estação identificada, entra em ação o módulo de atuação, cruzando informações de coletas atuais com a *baseline* gerada em banco de dados. Neste ponto, se uma máquina da rede interna, num determinado momento, saísse de seu padrão comportamental, ela seria isolada da rede com a finalidade de auditoria do *host* e da manutenção do acesso aos recursos de rede, tais como *link* internet e *link* entre segmentos, aos demais *hosts*.

O objetivo principal do NetAct é criar perfis individuais de uso estatístico de rede por parte dos *hosts* integrantes e, com isso, criar um mecanismo capaz de identificar desvios muito intensos de comportamento. Com esta finalidade, o NetAct objetiva principalmente a manutenção do acesso aos recursos de rede por parte dos demais integrantes do sistema sob controle, tendo como foco a proteção e manutenção da conectividade inter-redes, seja entre redes *LANs* (*Local Area Networks*) segmentadas internamente ou acesso ao *link* de internet.

Coleta de informações de uso de rede

O modelo de coleta de informações sobre o uso de rede foi implementado para atuar de modo passivo. O modo passivo compreende a coleta de informação sem a necessidade de instalação ou configuração de *software* adicional nas estações monitoradas. Na realidade, as estações monitoradas não precisam saber que estão sendo monitoradas, por isso não se adotou o uso de SNMP (*Simple Network Management Protocol*) [SNM06] para a coleta de dados de uso de rede.

Para tal modo de coleta torna-se necessário o uso de um sistema de captura de pacotes em modo promíscuo, ou *dump*. A escolha do *software* para a captura dos pacotes de rede foi feita levando em consideração a informação disponibilizada pelo aplicativo. Dentre os testes feitos, duas opções se destacaram: *NetFlow (flow-tools, softflowd)* [CIS06] e *tethereal*.

O *tethereal* foi o escolhido por fornecer um relatório mais compacto e pré-processado, levando em consideração a visão de conversações e não apenas fluxos. Uma visão geral do processo de coleta, geração de histórico e comparação com definição prévia de *baseline*, pode ser vista na figura 1.

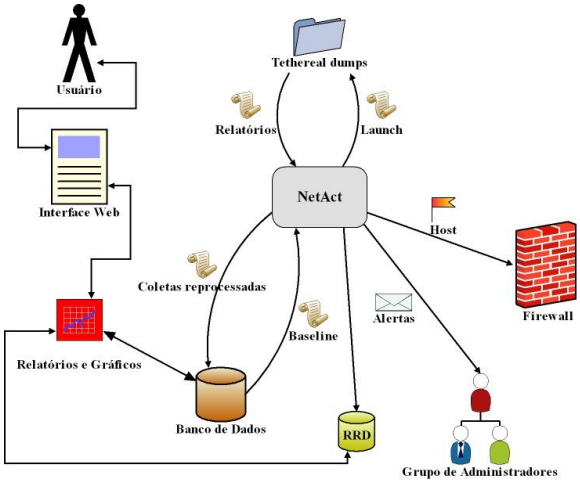

Figura 1. Esquema de funcionamento do NetAct

Após a execução do *tethereal* para captura de estatísticas de uso de rede, em modo passivo, individual por *host* identificado, o relatório pré-processado do *tethereal* é novamente processado pelo NetAct. Esta etapa consiste em uma interpretação que o NetAct faz em cima do relatório gerado, agrupando os resumos de conversações identificadas para esta iteração, e gerando o valor total de conversações originadas, conversações recebidas, *bytes* enviados e recebidos em todas as conversações, bem como *frames* enviados e recebidos em todas as conversações, para cada *host*, em forma de somatório.

Atuação

A atuação do NetAct na rede se resume em identificação do problema, isolamento e alerta. A identificação de *hosts* problemáticos é feita através da avaliação do seu estado atual em comparação ao seu histórico, caso o *host* em questão esteja saindo do padrão e excedendo os limites estabelecidos, este *host* é marcado. A figura 2 ilustra a interface do NetAct, no menu de visualização de gráficos de uso de rede por *host*.

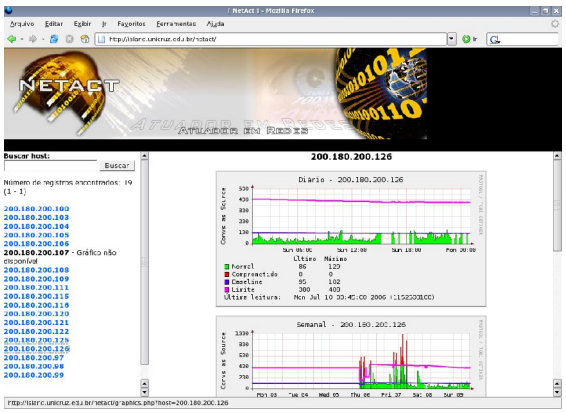

Figura 2. Gráficos e Interface Web do NetAct

Dos dados coletados e armazenados em banco de dados, para a geração da *baseline*, o mais importante para o NetAct é o de conversações originadas. Quando se identifica algum distúrbio no número de conversações que um dado *host* origina, a cada intervalo de coleta, a máquina em questão pode ser considerada como tendo um comportamento anormal, podendo estar comprometida. Quando uma máquina apresenta muitas iniciativas de conexão para diversos *hosts* diferentes ou para um *host* em

específico, isso pode caracterizar uma tentativa de *spread* (disseminação) de vírus/*worm* ou ataque.

O isolamento do problema vem depois da identificação. Cada *host* marcado como tendo comportamento anormal é bloqueado junto ao servidor em questão, através da alteração das regras de *firewall*. O passo seguinte é a notificação do grupo de administradores registrados sobre o desvio de comportamento do *host* identificado, bem como a notificação de seu devido bloqueio junto às regras de *firewall* da máquina.

Resultados e direções futuras

Os sistemas de gerenciamento de redes podem ser montados desde o uso simples de ferramentas ou protocolos específicos a um propósito no auxílio da manutenção de uma rede isolada até sistemas complexos, que cruzam informações de bases de dados distribuídas, ferramentas e protocolos diferentes para geração de relatórios e gráficos em tempo real do uso e estado de uma rede heterogênea e complexa.

O NetAct faz uso de ferramentas prontas, tais como o coletor de estatísticas de rede e o banco de dados escolhidos, e se caracteriza por fazer o reprocessamento, análise e intermédio das informações fornecidas com a finalidade de identificação de desvios comportamentais de tráfego dentro de uma rede de computadores, com o objetivo de efetuar bloqueios e gerar alertas.

Os objetivos iniciais do trabalho podem ser considerados atingidos, pois o *software* NetAct respondeu às expectativas, sendo capaz de identificar máquinas com comportamento anormal, que podem denotar características de máquinas comprometidas, ou por vírus ou por intrusores. O bloqueio dos *hosts* comprometidos e os alertas para grupos de administradores também estão implementados em sua versão atual.

Para trabalhos futuros verificam-se necessidades de alguns ajustes na implementação, podendo ser citados:

- Estudo e implementação de um novo método de geração de *baseline* mais elaborado, levando em consideração as informações de desempenho da rede contra as taxas de utilização da rede pelos *hosts*, e não somente a média de conversações por *host*.

- Inserção da avaliação de taxa de transferência em *bytes*, além da atual avaliação de conversações originadas.

Referências

[CIS06] Cisco NetFlow. ***Cisco IOS NetFlow Overview***. 2006. Disponível em: <http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e7c53.html>. Acesso em: <22 Jun. 2006>.

[COM05] COMBS, Gerald. ***Tethereal ManPages***. 2005. Disponível em: <http://www.ethereal.com/docs/man-pages/tethereal.1.html>. Acesso em: <29 Set. 2005>.

[SNM06] SNMP. ***Simple Network Management Protocol***. Disponível em: <http://en.wikipedia.org/wiki/Simple_network_management_protocol>. Acesso em: <22 Jun. 2006>.

[WAN03] WANDARTI, Daniel Francisco. ***Proposta de um Framework para Gerência de Clusters***. Dissertação de Mestrado. PUC-PR, Pontifícia Universidade Católica do Paraná, Curitba, PR. 2003. p. 79.