Desenvolvimento e Implementação de Políticas de Segurança: Projeto e Implementação de uma Zona Desmilitarizada

Rafael Pinaud Laufer

Relatório Técnico Final de Bolsa DTI-H

Período da bolsa: de junho/2003 a março/2004

Projeto:

QUARESMA - QUAlidade de serviço em REdes, Segurança, Mobilidade e Aplicações

Processo CNPq 552121/2001-0

Atividade Associada:

Redes Móveis Interconectadas à Internet

Professor Orientador:

Otto Carlos Muniz Bandeira Duarte

Local:

Grupo de Teleinformática e Automação (GTA)

Programa de Engenharia Elétrica, COPPE/UFRJ

Departamento de Engenharia Eletrônica e de Computação - Escola Politécnica

Rio de Janeiro, 13 de outubro de 2004,

Rafael Pinaud Laufer (Bolsista)

Otto Carlos Muniz Bandeira Duarte (Orientador)

Relatório de Atividades

1 Resumo

A maioria dos sítios ainda hoje apresenta uma topologia que consiste apenas de uma única rede protegida por um filtro de pacotes no roteador. Essa topologia é útil e segura para redes domésticas, onde não há necessidade de se oferecer nenhum serviço através da rede. Porém, para redes que necessitam prover serviços, essa topologia não é adequada. Caso ocorra alguma invasão passando pelo filtro e atingindo um dos servidores, a segurança de toda a rede está comprometida, pois não existe nenhum tipo de proteção entre os servidores e as outras estações que impeça o invasor de um ataque geral à rede. Logo, uma maneira de impossibilitar que as estações de trabalho sejam invadidas se torna atrativa. A utilização de uma zona desmilitarizada resolve esse problema, diminuindo o impacto de uma invasão através da segmentação da rede. O objetivo deste trabalho foi justamente projetar e implementar uma zona desmilitarizada em uma rede de produção científica. Para isso, foi realizada toda uma reestruturação lógica e física da topologia da rede de forma a limitar as possíveis proporções alcançadas por uma invasão e, ao mesmo tempo, não impedir a disponibilização dos seus serviços

2 Introdução

Ao mesmo tempo em que ocorreu um enorme avanço na comunicação entre redes, tornando possível o compartilhamento globalizado de seus recursos e informações, a segurança destas redes passou a ser crítica. Se por um lado este compartilhamento permite aumentar o dinamismo das comunicações e a troca de informações, por outro, ele possibilita que pessoas não autorizadas obtenham acesso a dados sigilosos. Por isso, a segurança é considerada essencial no projeto de uma rede, seja esta corporativa, acadêmica ou até mesmo pessoal. As razões dessa nova preocupação estão relacionadas diretamente com o valor dos dados armazenados e ainda com a necessidade de se garantir diferentes níveis de privacidade, integridade e autenticidade para cada tipo de dado.

Para minimizar as chances de que dados sejam comprometidos, um dos passos a serem tomados é analisar a topologia da rede a procura de possíveis falhas de segurança. A adoção de uma topologia que contenha uma zona desmilitarizada vem justamente acabar com uma grave falha que existe em diversas redes, conforme explicado a seguir.

A principal motivação para o projeto e a implementação de uma zona desmilitarizada é que a grande maioria dos sítios ainda hoje apresenta uma topologia que consiste apenas de uma única rede protegida por um filtro de pacotes no roteador. Essa topologia é útil e segura para redes domésticas, onde não há necessidade de se oferecer nenhum serviço através da rede. Porém, para redes que necessitam prover serviços, essa topologia não é adequada. O provimento de serviços a usuários de redes externas se torna problemático à medida que é necessário liberar a passagem de pacotes destinados a essas aplicações no filtro do roteador. Com esta liberação, possíveis vulnerabilidades presentes na implementação do serviço podem ser exploradas por usuários mal intencionados com o objetivo de comprometer o servidor. Diversos tipos de vulnerabilidade existem e são regularmente exploradas nas aplicações.

Entretanto, o risco de comprometimento do servidor sempre existirá. Se um serviço precisa ser disponibilizado, é porque é necessário que usuários o utilizem ou o acessem. Logo, é preciso

que o acesso destes usuários ao servidor seja liberado de alguma forma. Seria, no mínimo, contraditório se existisse um serviço oferecido e nenhum usuário tivesse acesso ao mesmo. É claro que deste modo estaria assegurado que o servidor nunca seria comprometido, mas ele também não teria funcionalidade alguma. O problema de uma invasão se agrava ainda mais quando a topologia usada consiste de apenas uma rede onde se encontram tanto os servidores quanto as estações de trabalho. Caso ocorra alguma invasão passando pelo filtro e atingindo um dos servidores, a segurança de toda a rede está comprometida, pois não existe nenhum tipo de proteção entre os servidores e as outras estações que impeça o invasor de um ataque geral à rede. Desse modo, uma vez comprometido um dos servidores, é criado um ponto de partida para ataques futuros em máquinas internas.

A utilização de uma zona desmilitarizada é uma alternativa para o problema descrito acima. Esta solução segmenta a rede em duas sub-redes ou zonas: a zona desmilitarizada - uma rede exclusiva de servidores que provêem serviços externos - e a rede interna - onde todas as estações de trabalho estarão situadas. Ao colocar os servidores em um segmento de rede separado, pacotes destinados às estações de trabalho vindos tanto da zona desmilitarizada quanto de redes externas precisam necessariamente ser roteados. Sendo o roteador equipado com um filtro adequado de pacotes, é possível agora impedir que máquinas da rede interna venham a ser comprometidas, mesmo que algum servidor seja invadido.

3 Objetivo

A rede do Grupo de Teleinformática e Automação (GTA) da COPPE/UFRJ utilizava a topologia de uma única rede, o que a tornava vulnerável a ataques partidos do servidor. Este projeto foi proposto com o objetivo de implementar uma nova topologia, de maneira que nela fosse incluída uma zona desmilitarizada. Para isso, foi realizada toda uma reestruturação lógica e física da topologia da rede de forma a limitar as possíveis proporções alcançadas por uma invasão e, ao mesmo tempo, não impedir a disponibilização dos seus serviços.

4 Metodologia

Para o projeto, foi feita antes uma análise da situação do laboratório levantando os serviços disponíveis em seus servidores, com o objetivo de saber o que precisava ser mudado. Em seguida, a nova topologia do laboratório com uma zona desmilitarizada foi proposta, incluindo as mudanças necessárias na infra-estrutura da rede.

A topologia do GTA era baseada em uma única rede, tendo ainda algumas máquinas que atuavam tanto como servidores internos quanto externos. Ou seja, existiam alguns serviços disponíveis somente para usuários internos e outros para usuários externos e internos. Isso poderia ser um problema à medida que, se estes servidores fossem comprometidos, ambos serviços internos e externos corriam sérios riscos de disponibilidade e privacidade. Além disso, no caso de uma invasão, não existia nenhuma proteção entre os servidores e as outras máquinas da rede. Logo, tendo penetrado em algum dos servidores, um invasor poderia ter acesso amplo a toda rede.

Um dos passos importantes para reprojetar a topologia da rede foi entender a função de cada serviço. A partir disso, foi possível distinguir quais serviços devem ficar na rede interna e quais devem ficar na zona desmilitarizada. A idéia principal foi que todo serviço que não precisa ser

acessado externamente ficasse dentro da rede interna e, precisando-se acessá-lo de outras redes, ele deveria permanecer na zona desmilitarizada.

Um dos requisitos básicos para a construção de uma zona desmilitarizada foi a segmentação da rede. Isso quer dizer que a única rede foi dividida em duas. Como conseqüência, a faixa de endereçamento também precisou sofrer alterações. Além disso, os serviços foram separados de acordo com a função e a necessidade de disponibilização externa de cada um deles.

Devido a estratégia da zona desmilitarizada, os arquivos dos usuários foram armazenados em um servidor da rede interna. Porém, a rede interna não é acessível tanto da rede externa quanto da própria zona. Logo, uso de tal topologia poderia causar uma grande limitação para os usuários do laboratório que quisessem trabalhar remotamente. Foi então adotada a solução dada pelo termo "túnel coreano". Ele foi aqui empregado para representar uma forma de acessar computadores da rede interna, mesmo que "ilegalmente", a partir da rede externa.

Um túnel coreano para um servidor de SSH da rede interna foi usado para eliminar com a limitação de que usuários conectando-se de redes externas não podem acessar as máquinas internas. O túnel se estabelece da seguinte forma: primeiramente, usuários externos necessitam acessar via SSH o servidor da zona desmilitarizada, se autenticando corretamente, e, em seguida, eles podem tentar o acesso ao servidor interno. Porém, é importante frisar que somente o acesso partindo do servidor da zona desmilitarizada com destino ao servidor da rede interna via SSH é permitido no filtro de pacotes do roteador. Tentativas de acesso ao servidor de SSH interno diretamente da rede externa são barradas.

5 Conclusão

O objetivo deste trabalho foi projetar e implementar uma nova topologia para a rede do Grupo de Teleinformática e Automação (GTA) da COPPE/UFRJ, de maneira que nela fosse incluída uma zona desmilitarizada. Para isso, antes foi feita uma análise da situação vigente no laboratório, de sua topologia e dos serviços prestados tanto interna quanto externamente, para somente depois propor as mudanças necessárias na infra-estrutura da rede.

Apesar do uso de uma zona desmilitarizada melhorar a segurança da rede, ela é também restritiva. Para acessos de fora da rede, nenhum serviço, em teoria, pode ser acessado senão aqueles disponibilizados na própria zona. Como diversos usuários do laboratório acessam suas máquinas remotamente, foi preciso flexibilizar um pouco essa rígida definição. A solução adotada foi criar um túnel coreano conectando usuários externos ao servidor SSH interno através do servidor da zona desmilitarizada. Desse modo, foi assumido o risco de ter a rede interna comprometida, caso alguma vulnerabilidade do SSH fosse explorada, em detrimento de uma maior liberdade para os usuários. Mesmo com esta flexibilização, esse método ainda apresenta a vantagem de correr este risco somente para o serviço de SSH. Usando-se uma única rede, qualquer um dos serviços poderia comprometer a rede.

Referências

[1] D. E. Comer, *Internetworking with TCP/IP: Principles, Protocols and Architecture*, vol. 1. Englewood Cliffs, NJ, EUA: Prentice Hall, third ed., 1995.

[2] A. S. Tanenbaum, *Computer Networks*. Upper Saddle River, NJ, EUA: Prentice Hall PTR, fourth ed., 2002.

[3] W. R. Cheswick, S. M. Bellovin e A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley Professional Computing Series, Addison-Wesley, second ed., 2003.

[4] M. Strebe e C. Perkins, *Firewalls*. São Paulo, SP, Brasil: Makron Books, 2002.

[5] E. D. Zwicky, S. Cooper e D. B. Chapman, *Building Internet Firewalls*. Sebastopol, CA, EUA: O'Reilly & Associates, Inc., second ed., 2000.

[6] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent e W. T. Strayer, "Single-packet IP traceback", *IEEE/ACM Transactions on Networking*, no. 6, pp. 721–734, dezembro de 2002.

[7] S. M. Bellovin, "Distributed firewalls", *;login:*, vol. 24, pp. 39–47, novembro de 1999.

[8] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent e W. T. Strayer, "Hash-based IP traceback", in *SIGCOMM'01*, San Diego, Califórnia, EUA, agosto de 2001.

[9] "The netfilter/iptables Project". http://www.netfilter.org.

[10] "IP Filter". http://www.ipfilter.org.

[11] "Norton Personal Firewall". http://www.symantec.com/sabu/nis/npf.

[12] "Zone Labs, Inc.". http://www.zonelabs.com.

[13] "Wikipedia, The Free Encyclopedia". http://www.wikipedia.org.

[14] R. P. Laufer, "Introdução a Sistemas de Detecção de Intrusão", julho de 2003. Trabalho da disciplina "Redes de Computadores I", do curso de Engenharia Eletrônica e de Computação da Universidade Federal do Rio de Janeiro (UFRJ). http://www.gta.ufrj.br/~rlaufer/production/undergraduate/redesI.

[15] A. T. Pedroza, "Notas de aula da disciplina 'Arquitetura e Projeto de Protocolos'", julho de 2003. Lecionada no mestrado do Programa de Engenharia Elétrica (PEE) da COPPE/UFRJ.

[16] R. Russel, "Linux IPCHAINS HOWTO", julho de 2000. Versão 1.0.8. http://www.linux.org/docs/ldp/howto/IPCHAINS-HOWTO.html.

[17] Fyodor, "The Art of Port Scanning", setembro de 1997. http://www.insecure.org/nmap/nmap_doc.html.

[18] J. Kemp, "Basic Firewall Concepts". http://cc.uoregon.edu/cnews/spring2002/firewall.html.

[19] O. Andreasson, "Iptables Tutorial", 2003. Versão 1.1.19. http://iptables-tutorial.frozentux.net.

[20] W. Puschitz, "Procedure for Patching pam_cracklib.c", dezembro de 2002. http://www.puschitz.com/pam_cracklib_patch.shtml.

[21] H. Eychenne, *Man page of Iptables*, março de 2002.