PROVIMENTO DE UMA REDE DESMILITARIZADA (DMZ)

ROSSETO, Paulo Sergio – Paulo.rosseto@hotmail.com[1]

RESUMO

Este trabalho tem o propósito de demonstrar sobre a importância de uma rede desmilitarizada, a fim de garantir proteção as redes internas de uma empresa ou corporação, para tanto foi realizado um levantamento bibliográfico sobre as redes de computadores, os serviços de rede (web, FTP, e-mail), firewall e a própria DMZ (zona desmilitarizada), efetuado testes confrontando os resultados.

Palavras Chaves: demonstrar, rede desmilitarizada, redes internas .

ABSTRACT

This work aims to demonstrate the importance of a network demilitarized in order to ensure protection of the internal networks of a company or corporation, for that was based on a literature on computer networks, network services (web, FTP , e-mail), and their own firewall DMZ (demilitarized zone), conducted tests comparing the results.

Keywords: show, demilitarized networks, intranets.

INTRODUÇÃO

Este estudo tem como principal objetivo demonstrar a importância da segurança da rede em uma organização, provendo informações sobre como posicionar uma rede desmilitarizada e evitar por em risco as informações corporativas, utilizando-se de recursos disponíveis com segurança e controle.

Como objetivos secundários tem-se a aquisição de novos conhecimentos, explorar um ambiente de virtualização, para demonstrar uma rede de computadores, através da utilização do software virtualbox, visualizando o processo de transferência

[1] Aluno do Curso de Tecnologia em Processamento de Dados. 1S/2011.

de pacotes em uma rede de computadores, através de simulação, neste caso empregando o software Packet Tracer.

A metodologia a ser utilizada consistiu em dividir o estudo em uma série de etapas, e consiste no (1) levantamento bibliográfico com ênfase em redes de computadores, serviços de rede, WEB, FTP, firewall e rede DMZ, no (2) desenvolvimento do estudo através de dois cenários e (3) a discussão comparando-se os resultados dos cenários testados. (projeto e implantação, através do packet tracer e virtualbox, respectivamente).

PROVIMENTO DE UMA REDE DESMILITARIZADA (DMZ)

Uma rede de computadores tem como objetivos básicos prover a comunicação confiável entre os vários sistemas de informação, melhorar o fluxo e o acesso às informações, bem como agilizar a tomada de decisões administrativas facilitando a comunicação entre seus usuários, (TANENBAUM, 2003, p. 03).

Uma rede de computadores é formada por um conjunto de módulos processadores (MPs) capazes de trocar informações e compartilhar recursos, interligados por um sub-sistema de comunicação,(Zem, 2011).

Já o sub-sistema de comunicação, como mostra a Figura 02, irá constituir-se de um arranjo topológico interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com a finalidade de organizar a comunicação (protocolos), (Zem, 2011).

Segundo (TANENBAUM, 1994, p. 04).“Objetivo é a redução de custo, uma vez que computadores de pequeno porte, os mais utilizados atualmente na construção de modelos de redes, têm uma relação custo/desempenho muito melhor do que os computadores de grande porte. Isto se explica pelo fato de que um mainframe, apesar de ser aproximadamente dez vezes mais rápido do que o mais rápido microprocessador de um chip custa muitas vezes mais. Esse desequilíbrio levou muitos projetistas de sistemas a construírem redes constituídas de computadores pessoais potentes, havendo um por usuário, com os dados guardados em uma ou mais máquinas servidoras de arquivos. Esse último objetivo leva à existência de redes com muitos computadores localizados em um mesmo prédio, sendo esse tipo de estrutura conhecida como rede local”.

DMZ, em segurança da informação, é uma sigla para de *DeMilitarized Zone* ou "zona desmilitarizada", em português. Também conhecida como Rede de Perímetro, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.

A função de uma DMZ é manter todos os serviços que possuem ou permitem acesso externo (tais como servidores HTTP, FTP, de correio eletrônico, etc.) separados da rede local, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um invasor. Para atingir este objetivo os computadores presentes em uma DMZ não devem conter nenhuma forma de acesso à rede local.

A configuração é realizada através do uso de equipamentos de *firewall*, que realizarão o controle de acesso entre a rede local, a Internet e a DMZ (ou, em um modelo genérico, entre as duas redes a serem separadas e a DMZ). Os equipamentos na DMZ podem estar em um segmento de rede dedicado ou compartilhar um segmento único da rede, porém neste último caso devem ser configuradas redes virtuais distintas dentro do equipamento, também chamadas de VLANs (ou seja, redes diferentes que não se "enxergam" dentro de uma mesma rede física).

A DMZ pode ser um segmento ou segmentos de rede, parcialmente protegida, que está entre uma rede protegida e uma desprotegida e que contém serviços e informações. Nela podem existir regras de acesso específico e sistemas de defesa de perímetro simulando uma rede protegida para induzir os possíveis invasores para armadilhas virtuais, assim tentando localizar a origem do ataque.

Atualmente as empresas e organizações tem um sistema típico de redes de computadores, com uma configuração onde a rede externa tem acesso a rede interna ficando, assim exposta à ataques com grande potencial de danos ao sistema.

A idéia do trabalho é implementar uma rede desmilitarizada para que os computadores da rede externa não acesse a rede interna.

O desenvolvimento foi realizado no ambiente virtual através dos softwares Virtualbox e Packet Tracer. Foram implementados dois cenários sendo em um deles caracterizando o sistema típico das empresas.

No segundo cenário a rede interna foi separada da rede externa, ficando protegida pela configuração de uma rede desmilitarizada, diminuindo assim o potencial de dano causado por um ataque de um invasor.

Os testes foram realizados nas máquinas virtuais criadas no Virtualbox, onde foram criados os servidores e estações, afim de simular uma situação real na rede de uma corporação.

RESULTADOS E/OU DISCUSSÃO

Os resultados observados após a implantação da rede desmilitarizada foi que o tráfego da rede interna e rede externa ficou restrito entre os equipamentos solicitantes e os equipamentos de destino.

Não ocorreu tráfego de pacotes em outros equipamentos a não ser os solicitados e destinados pelos pacotes, sendo assim, os resultados obtidos na execução dos testes foram satisfatórios para a confirmação do estudo realizado, atingindo plenamente o objetivo esperado do projeto desenvolvido.

CONSIDERAÇÕES FINAIS

A implantação de uma rede desmilitarizada entre a rede interna e a rede externa de uma corporação, efetivamente “isola” a rede interna da web através de uma rede virtual distinta.

REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, A. Redes de Computadores – Tradução da 4º edição. Rio de Janeiro: Elsevier Editora LTDA, 2003.

KUROSE, J. Redes de Computadores e a Internet: Uma abordagem top down 5º Ed. São Paulo: Addison-Wesley, 2010.

COMER, D. E. Interligação de Redes com TCP/IP – Tradução da 5º edição. Rio de Janeiro: Elsevier Editora LTDA, 2006.

SOARES, L. F.G., LEMOS, G., COLCHER, S. Redes de Computadores: das LANs, MANs e WANs às Redes ATM 2° Ed. Rio de Janeiro: Cam pus, 1995.

STALLINGS, W. Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas - Tradução da 5º edição. Rio de Janeiro: Campus, 2005.

http://sites.google.com/site/jlzemfatec/trc_tsi_noturno. Acesso em: 12 de fevereiro de 2011. 23h30.

http://www.infowester.com/firewall.php. Acesso em: 18 de fevereiro de 2011. 22h55.

Software Virtualbox disponível em: http://www.virtualbox.org. Acesso em: 20 de fevereiro de 2011. 22h48.

Informações sobre o software Packet Tracer Disponível em: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html. Acesso em 24 de fevereiro de 2011. 22h50.

SANTOS JUNIOR, A. L. dos. Quem Mexeu no Meu Sistema?: Segurança em Sistemas de Informação. Rio de Janeiro: Brasport, 2008. p.71-73.

PINHEIRO, J. M. S. Redes de Perímetro: Zona Desmilitarizada – DMZ. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php. Acesso em: 02 de maio de 2011. 22h43.