Técnicas de Defesa contra Ataques em Redes de Computadores[1]

Fernanda Rafaella Kleine[2]; Raul Alessandro Ferrony Rivas[3]

Resumo Expandido

[1] Trabalho executado com recursos da Chamada Interna nº 03/2013/Câmpus Gaspar (Edital Universal 12/2013/PROPPI).
[2] Estudante bolsista do Curso Concomitante de Informática; IFSC - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina – Câmpus Gaspar; Gaspar – SC; fernanda.kleine@hotmail.com;
[3] Analista de TI - IFSC - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina - Câmpus Gaspar; Gaspar – SC; raul.rivas@ifsc.edu.br.

RESUMO: Ataques de negação de serviço à rede de computadores estão virando rotina. Vários domínios, tanto de instituições públicas como privadas no Brasil e no mundo estão cada vez mais sendo alvo desse tipo de ataque. Com isso, deve-se planejar medidas de segurança para todo o parque computacional a fim de minimizar possíveis problemas ocasionados por tais ataques. Esse trabalho teve como objetivo demonstrar os ataques mais frequentes em redes de computadores e formas de efetivar segurança na rede. Usamos para isso o Sistema Linux para aplicar comandos em busca de vulnerabilidades em redes. Através de varreduras de portas dos sistemas alvos.

Palavra Chave: Ataques de negação de serviço. Rede de Computadores. Ataques DOS. Ataques.

INTRODUÇÃO

Tem-se uma rede de computadores quando há computadores independentes interconectados através de uma única tecnologia. Dois computadores estão interconectados quando é possível haver a troca de informações. A conexão pode ser feita utilizando-se fio de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélites de comunicações. As redes podem ser de diversos tamanhos, modelos e formas (TANENBAUM, 2003). Uma grande vantagem das redes de computadores é tornar mais fácil o compartilhamento de recursos. Esses recursos podem ser dados, impressoras e também a conexão de Internet de alta velocidade (CICCARELLI et al., 2009). É importante destacar que as redes possuem vários níveis ou camadas. Uma rede possui muitos sistemas sobrepostos, tais como o cabeamento estruturado, os esquemas de endereçamento ou as aplicações. As diversas camadas operam em conjunto, de forma a poderem enviar e receber dados (GOUVEIA; MAGALHÃES, 2013).

Com a melhoria dos equipamentos de redes e larguras de banda maiores, foi possível implementar ataques em redes afetando diversos serviços. Tais serviços hospedam sites públicos de empresas privadas e de usuários comuns.

METODOLOGIA

A pesquisa se configura como exploratória, buscando uma aproximação com o fenômeno, pelo levantamento de informações que levaraão mais o pesquisador a conhecer mais a seu respeito. E, para sua realização foram desenvolvidos os seguintes passos: pesquisa bibliográfica sobre ataques de negação de serviços, em especial, buscando construir um panorama atual da situação das tentativas de invasões.

RESULTADOS E DISCUSSÃO

Modelo de Referência OSI

O modelo OSI (Open System Interconnection) foi desenvolvido em 1984 pela ISO (International Standardization Organization). Seu propósito foi desenvolver um padrão aberto, que pudesse ser seguido por futuros protocolos de rede. Esse modelo possui sete camadas, também denominadas de níveis, que juntas formam uma pilha, onde cada camada na pilha recebe e provê informações para as camadas adjacentes (SCHMITT; PERES; LOUREIRO, 2013). As camadas do modelo OSI são: física, enlace, rede, transporte, sessão, apresentação e aplicação.

 ISSN 2357-836X

Firewall

Quando uma rede privada é conectada a uma rede pública, a possibilidade de invasão se torna maior. Para preservar a rede privada de acessos não-autorizados a partir de uma rede pública, emprega-se um firewall (CICCARELLI et al., 2009).

Os firewalls são, normalmente, uma combinação de hardware e software. O hardware pode ser um computador ou um equipamento dedicado que possui duas placas de rede. Uma placa de rede é conectada à rede pública e a outra é ligada à rede privada. O software gerencia a operação do firewall e protege a rede privada. Verifica cada pacote de entrada e saída e descarta os pacotes suspeitos. A função de um firewall é somente permitir passar os pacotes que estão dentro de certos requisitos de segurança (CICCARELLI et al., 2009).

Um firewall tem por função proteger informações entre uma rede privada e a Internet ou outras redes. Para ter um firewall eficiente, é necessário que ele seja configurado de forma correta, tenha bons recursos implementados e esteja corretamente posicionado na rede em questão (PEIXINHO; FONSECA; LIMA, 2013).

Ataques de Negação de Serviço

A largura de banda de uma rede é finita e o número de conexões que um servidor Web é capaz de manter com clientes é limitado. Todas as conexões com um servidor precisam de uma quantidade mínima de capacidade de rede para operar. Um ataque desenvolvido para fazer uma máquina ou software ficar indisponível e não apto a executar sua função básica é conhecido como ataque de negação de serviço (denial of service, DOS). Isso inclui qualquer situação que faça um servidor não operar de maneira correta, mas mais frequentemente se refere a tentativas intencionais de ultrapassar a largura de banda máxima disponível de um servidor (GOODRICH, 2013).

Como os atacantes em um ataque DOS não estão preocupados com o ganho de respostas de um alvo, o ato de burlar o endereço IP de origem é frequentemente empregado para obscurecer a identidade do atacante, assim como dificultar abrandar o ataque. Como alguns servidores são capazes de parar ataques DOS rejeitando todos os pacotes de certos endereços IP de uma “lista negra”, os atacantes podem criar um endereço IP de origem distinto para cada pacote enviado, impedindo que o alvo consiga reconhecer e bloquear o atacante. Portanto, a falsificação de endereços IP torna mais complicada a identificação da fonte de um ataque DOS (GOODRICH, 2013).

O ataque de inundação por ping é um tipo de ataque DOS. Em um ataque de inundação por ping (ping flood), uma máquina mais poderosa pode efetuar um ataque DOS numa máquina mais fraca. Para conduzir esse ataque, uma máquina poderosa transmite muitas requisições de eco para somente um servidor vítima. Se o atacante puder gerar mais requisições ping do que a vítima consegue processar, e a vítima tem uma largura de banda suficiente para receber essas requisições, então o servidor vítima se tornará sobrecarregado pelo tráfego e começa a rejeitar conexões legítimas (GOODRICH, 2013).

Outro tipo de ataque DOS é o ataque smurf que é uma técnica que tira vantagens de redes mal-configuradas. Muitas redes têm um endereço de difusão (broadcast) por onde o usuário consegue transmitir um pacote que é recebido por todos os endereços IP da rede. Ataques smurf exploram essa propriedade encaminhando pacotes ICMP com um endereço fonte configurado para o alvo e com um endereço destino configurado para o endereço de difusão da rede (GOODRICH, 2013).

Depois de encaminhados, todos os pacotes são recebidos por todas as máquinas na rede, que então encaminham um pacote ICMP de resposta para o endereço fonte do alvo. Como consequência ocorre um efeito de amplificação que multiplica o número de pacotes encaminhados pelo número de máquinas na rede (GOODRICH, 2013).

Para impedir ataques smurf, administradores devem configurar os hosts e os roteadores de suas redes para descartar requisições de difusão. Além disso, os roteadores precisam ser configurados para evitar enviar pacotes dirigidos a endereços de difusão, porque isso traz um risco de segurança no sentido de uma rede poder ser utilizada como amplificadora de inundação por ping (GOODRICH, 2013).

Outro tipo de ataque de negação de serviço é o ataque de inundação por SYN. No ataque de inundação por SYN, um atacante encaminha muitos pacotes SYN para o servidor, ignora as respostas SYN-ACK e nunca encaminha os pacotes ACK aguardados. Um atacante que começa esse ataque na prática provavelmente utilizará endereços fonte falsificados aleatoriamente nos pacotes SYN que ele encaminha, de maneira que as respostas SYN-ACK são encaminhadas para endereços IP aleatórios. Se um atacante encaminhar muitos pacotes SYN sem os correspondentes pacotes ACK, a memória do servidor ficará ocupada com os números de sequência que ele está guardando para estabelecer as sessões TCP com os pacotes ACK que está esperando. Esses pacotes ACK nunca chegarão, de

 ISSN 2357-836X

maneira que a memória desperdiçada bloqueará ao final as outras requisições legítimas de sessões TCP (GOODRICH, 2013).

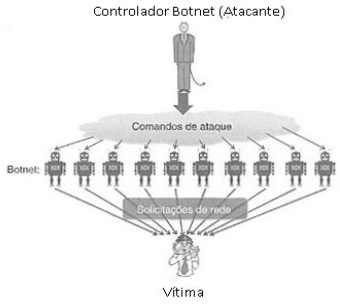
Atualmente muitos dos ataques DOS comuns são impraticáveis de realizar a partir de apenas uma máquina. A tecnologia de servidores modernos possibilita que sites Web atendam a uma grande quantidade de largura de banda – muito maior do que a largura de banda possível de apenas uma máquina. Entretanto, condições de negação de serviço ainda podem ser geradas utilizando mais de uma máquina atacante, no que é denominado de ataque de negação de serviço distribuída (distributed denial-of-service, DDOS) (Figura 1).

Nesse ataque, usuários mal-intencionados combinam a potência de várias máquinas para encaminhar o tráfego contra apenas um site numa tentativa de gerar condições de negação de serviço. Com frequência os atacantes realizam ataques DDOS utilizando botnets que são grandes redes de máquinas que foram colocadas em risco e são controláveis remotamente (GOODRICH, 2013).

Teoricamente não existe forma de afastar por completo a possibilidade de um ataque DDOS, porque a largura de banda que um servidor pode prover a seus usuários será sempre limitada. Contudo, podem ser tomadas medidas para amenizar os riscos de ataques DDOS. Por exemplo, muitos servidores incorporam mecanismos de proteção contra DOS que examinam o tráfego de entrada e eliminam pacotes de fontes que estejam consumindo muita largura de banda. Infelizmente, a falsificação de IP pode deixar mais difícil a prevenção de DDOS, obscurecendo a identidade dos atacantes e provendo informação que não tem consistência sobre a origem do tráfego da rede (GOODRICH, 2013).

Como resultado vimos que diversas redes estão sem proteção ou com mínimo aceitável para conter ataques de negação de serviço. Novas técnicas surgem a cada dia e novos mecanismos de proteção são implementados. As configurações padrões dos dispositivos de redes, não são a ideal, haja vista que detectamos divervos problemas de portas de serviço aberta e sem uso. Muitos dos sistemas estavam vulneráveis em diversos aspectos e outros estavam sujeitos a ataques de qualquer espécie.

Figura 1 - Rede botnet em ação.



Fonte – Goodrich (2013).

CONCLUSÕES

Existem diversos ataques de negação de serviço. Cada ataque tem sua particularidade e seus objetivos bem definidos. O número de ataques cresce rapidamente e novas técnicas são implementadas diariamente. Vários domínios de instituições públicas, privadas do Brasil e no mundo estão cada vez mais sendo alvos dos ataques de negação de serviço. Isso levou a adoção de mecanismos de proteção em computadores da rede.

Vimos que os ataques DoS, também denominados Ataques de Negação de Serviços , consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador. Para isso, são usadas técnicas que podem sobrecarregar a rede, fazendo que nenhum usuário consiga usá-la; derrubar uma conexão entre dois ou mais computadores; Os ataques do tipo DoS mais comum podem ser feitos devido a algumas características do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol), sendo possível ocorrer em qualquer computador que faça uso desses protocolos.

Uma das formas de ataque mais conhecidas é a SYN Flooding, onde um computador tenta estabelecer uma conexão com um servidor através de um sinal do TCP conhecido por SYN (Synchronize). Outra forma de ataque comum é o UPD Packet Storm, onde um computador faz solicitações constantes para que uma máquina remota envie pacotes de respostas ao solicitante, deixando o computador sobrecarregado a ponto de não conseguir responder mais acessos a seus serviços. Para detecção de ataques distribuídos de negação de serviço torna-se fundamental configurar

ISSN 2357-836X

os ativos da rede e instalação de softwares para monitoramento.

REFERÊNCIAS

CICCARELLI, Patrick et al. **Princípios de Redes.** Rio de Janeiro: LTC, 2009.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** Porto Alegre: Bookman, 2013.

GOUVEIA, José; MAGALHÃES, Alberto. **Redes de Computadores.** 10. ed. Lisboa: FCA, 2013.

PEIXINHO, Ivo de Carvalho; FONSECA, Francisco Marmo da; LIMA, Francisco Marcelo. **Segurança de Redes e Sistemas.** Rio de Janeiro: RNP/ESR, 2013.

SCHMITT, Marcelo Augusto Rauh; PERES, André; LOUREIRO, César Augusto Hass. **Redes de Computadores.** Porto Alegre: Bookman, 2013.

SOBELL, Mark G. **Um guia prático Linux de comandos, editores e programação de Shell.** Rio de Janeiro: Alta Books, 2009.

TANENBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: Elsevier, 2003.

 ISSN 2357-836X