UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO
CURSO DE ESPECIALIZAÇÃO EM TELEINFOMÁTICA E REDES DE COMPUTADORES

LUIS EDUARDO PEREIRA BUENO

SISTEMAS DE DETECÇÃO DE INTRUSÃO BASEADOS EM FLUXOS IP

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba
2011

LUIS EDUARDO PEREIRA BUENO

SISTEMAS DE DETECÇÃO DE INTRUSÃO BASEADOS EM FLUXOS IP

Monografia apresentada ao Programa de Pós-Graduação em Teleinformática e Redes de Computadores, como requisito para obtenção do grau de Especialista em Redes de Computadores e Teleinformática. Área de Concentração: Telemática.

Orientador: Prof. Msc. Lincoln Herbert Teixeira.

Curitiba

2011

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

Sistemas de Detecção de Intrusão Baseados em Fluxos IP

por

Luis Eduardo Pereira Bueno

Esta dissertação foi apresentada às 16 horas e 30 minutos do dia 15 de junho de 2011 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Msc. Lincoln Herbert Teixeira
(UTFPR)

Prof. Dr. Walter Godoy Júnior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do
Curso de Especialização em
Teleinformática e Redes de Computadores

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

Resumo

BUENO, Luis E P. Sistemas de Detecção de Intrusão Baseados em Fluxos. 2011. 22 f. Monografia (Especialização em Redes de Computadores e Teleinformática) – Programa de Pós-Graduação, Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

O crescimento das redes de telecomunicações tem cada vez mais gerado uma necessidade por maior banda. Ao mesmo tempo em que as redes crescem, a quantidade de ataques também aumenta às redes também cresce. As grandes redes precisam de soluções para detecção de ataques que operem em grandes velocidades e consiga proteger a rede satisfatoriamente. Sistemas de detecção de intrusão por fluxos IP são uma boa alternativa. Este trabalho apresenta o funcionamento de um IDS baseado em fluxos, suas vantagens e desvantagens em relação a IDS baseados na análise do payload de pacotes.

Palavras chave: IDS. NIDS. DoS. Detecção de intrusão. Fluxos IP.

Abstract

BUENO, Luis E P. Flow-Based Intrusion Detections Systems. 2011. 22 f. Monografia (Especialização em Redes de Computadores e Teleinformática) – Programa de Pós-Graduação, Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

The growth of the telecommunications networks is constantly requiring more bandwidth. As the networks become bigger, the number atacks grows. Big networks need solutions to detect atacks that are able work in high speeds. Flow-based intrusion detection systems are an alternative. This work presents how an flow-based IDS works, its advantages and disadvantages compared to a payload based IDS.

Keywords: IDS. NIDS. DoS. Intrusion detection. IP flow.

Lista de figuras

Lista de acrônimos

ACL	Acess Control List
DoS	Denial of Service
DdoS	Distributed Denial of Service
Gbps	Giganits per second
IDS	Intrusion Detection System
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention System
HIDS	Host Intrusion Detection System
NIDS	Network Intrusion Detection System
SCTP	Stream Control Transmission Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
TAP	Test Access Port
TCP	Transfer Control Protocol
UDP	User Datagram Protocol

Sumário

1. Introdução

Observa-se um constante crescimento dos serviços oferecidos na Internet e cada vez mais uma maior necessidade de banda. A interrupção destes serviços ou o roubo de dados de usuários pode gerar diversos problemas às vítimas, como processos por parte dos usuários, afetação da imagem da empresa e perda de renda durante o período de interrupção. Considerando os danos causados por ataques em redes, é importante detectá-los o mais rápido possível e tomar as ações necessárias para mitigação de qualquer ação que o invasor possa tomar. Muitos métodos foram desenvolvidos para prevenir ataques, como o uso de firewalls, criptografia e redes privadas virtuais (VPN)[1].

Normalmente a segurança contra ataques é feita por meio de firewalls, que nada mais são do que filtros que bloqueiam determinados pacotes de acordo com regras pré-configuradas. Porém se um atacante conseguir passar pelo firewall, irá passar completamente desapercebido até que suas ações dentro da rede tenham um grande impacto. Por isso é importante o investimento em sistemas de de detecção de ataques.

Para detecção de ataques são utilizados sistemas chamados *IDS* (*Intrusion Detection System*). Um IDS é um sistema que monitora redes ou *hosts* buscando sinais que indiquem uma possível ameaça à rede ou host. Os dados coletados por um IDS podem ser usados para mitigar um ataque no momento em que o mesmo ocorre. Podem ser usados também para uma análise posterior da segurança da rede e também como evidência legal de um ataque. Um IDS pode ser um software, um hardware ou uma combinação de ambos. Seu funcionamento básico consiste na coleta dos dados da rede, armazenamento e análise.

Um IDS pode ter dois focos distintos, redes ou hosts[2]:

Sistema de detecção de instrução baseado em hosts (Host-based intrusion detection system - HIDS)

Normalmente consiste em um software presente em um host que faz análise de *logs*, *system calls*, modificações em arquivos, pacotes que entram e saem do equipamento, etc e com base nestas informações alerta sobre possíveis ataques contra a máquina. Este tipo de IDS está fora do escopo deste trabalho.

Sistema de detecção de intrução baseado em redes (Network intrusion detection system - NIDS)

Normalmente consiste em um equipamento junto ao roteador de borda da rede. Monitora todo o tráfego passante e é transparente. O trabalho irá focar-se em NIDS que operam com fluxos IP, normalmente utilizados em redes de alta velocidade.

Os sistemas de detecção de intrusos podem ser ativos ou passivos[3]. Os sistemas passivos, normalmente chamados apenas de IDS, apenas detectam e reportam a ameaça e o operador deve tomar uma ação manualmente. Os sistemas reativos detectam a ameaça e podem tomar uma ação mitigatória. Sistemas ativos também são conhecidos por Sistemas de Prevenção de Ataques ou *IPS (Intrusion Prevention System*).

Ao detectar o ataque, um sistema passivo deve informá-lo a um operador para que sejam tomadas atitudes para mitigá-lo. Normalmente é enviada uma trap *SNMP* a um terceiro sistema, como *HP OpenView* ou *Tivolli*. Um IDS também pode enviar e-mails, *SMS* para informar a ameaça.

Um sistema de detecção de intrusão pode também tomar ações automaticamente com o objetivo de mitigar o ataque. Um IPS pode reconfigurar um firewall ou as ACLs de um roteador com o objetivo de bloquear a origem do ataque.

Um IDS pode detectar ataques realizando dois tipos diferentes de análises[1]:

Detecção baseada em payload

Neste método, o conteúdo dos pacotes (*payload*) é analisado em busca de padrões já identificados de ataques. Este tipo de análise envolve um grande processamento pois o pacote deve ser aberto e sua carga útil lida. É difícil de ser realizada de forma satisfatória em alta velocidade, como em redes que operam na ordem de vários Gbps

Detecção baseada em header

A análise apenas dos headers do pacote nada mais é do que a análise de fluxos. Não há necessidade de abrir a carga útil do pacote. Possui um desempenho melhor do que a análise baseada payload, sendo um boa alternativa para redes de alta velocidade. Outra motivação para utilização da análise por fluxo é a utilização de payloads criptografados, que não podem ser analisados.

2. Fluxos IP

2.1 Definição

Fluxos IP podem ser definidos como conjuntos de pacotes IP passando por um ponto de observação na rede em um certo intervalo de tempo com propriedades comuns[4]. Estas propriedades comuns podem ser endereço de origem e destino, portas, protocolo, entre outros. Para geração dos fluxos são analisadas informações do header da camada de rede e da camada de transporte. Com estas informações, é possível identificar padrões de comunicação entre hosts sendo possível identificar determinados tipos de ataques.

Além de monitoramento da rede para identificar ameaças, fluxos também podem ser usados para outros propósitos, como geração de estatísticas para planejamento futuro da rede, para usos de marketing, para monitoramento de aplicações específicas, billing, etc.

Um fluxo IP pode conter informações como

- timestamp
- endereço de origem
- endereço de destino
- flags TCP
- protocolo da camada superior
- Type of Service (TOS)
- interface SNMP

entre outras.

Como protocolo para exportar os dados dos fluxos IP, foi criado o Netflow, um protocolo da Cisco porém também suportado por outros fabricantes. As

especificações do Netflow definem o f*low exporter* e o f*low collector*. O flow exporter monitora os pacotes no ponto de observação, cria os fluxos e envia para o collector. O collector recebe os pacotes, extrai os dados do fluxo e os armazena para análise[5].

O Netflow geralmente envia as informações de fluxo utilizando UDP como transporte, porém também pode usar outros protocolos como SCTP na sua versão mais nova. O pacote enviado do exporter ao collector contem informações sobre a *template* utilizada e as informações do fluxo. A template nada mais é do que uma definição de em que formato os dados devem ser enviados ao exporter.

O Netflow chegou até a versão 9 e deu lugar ao *Internet Protocol Flow Information Export* (*IPFIX*). Este protocolo foi criado da necessidade de existir um padrão universal para troca de informações de fluxos. O IPFIX possui uma estrutura muito semelhante à do Netflow v9, com o mesmo conceito de templates e utiliza normalmente o SCTP como transporte[6,7].

2.2 Coleta

Para coleta dos pacotes e geração dos fluxos, os flow collectors são posicionados em pontos de obervação. A posição do ponto de observação depende do tipo de ameaças que devem ser detectadas. Para casos em que a ameaça pode vir de fluxos externos, o IDS deve ser posicionado nas saídas da rede, ou seja, onde a rede é conectada à Internet, conforme a figura 1.

Figura 1 - IDS posicionados nas bordas da rede para detecção de ameaça externa

Se o objetivo for detectar ameaças dentro da própria rede, um sensor deve ser posicionado em cada segmento da rede, ou apenas nos segmentos da rede mais sensíveis. A figura 2 mostra uma rede com dois segmentos, denominados 1 e 2[1].

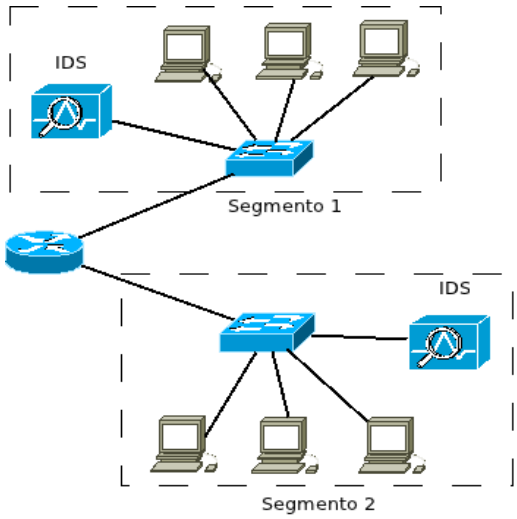

Figura 2 - IDS posicionados nos dois segmentos da rede.

2.3 Amostragem

Em links de alta velocidade, podem haver um tráfego de milhões de pacotes por segundo. Este alto tráfego coloca o flow exporter sob grande demanda. Para reduzir a demanda, são usadas técnicas de amostragem. É importante notar que apensar das técnicas de amostragem diminuírem a demanda sob o flow exporter, também tornam a detecção de ameaças mais difícil pois há menos informações para serem analisadas[4].

Podem ser usadas as técnicas de amostragem de pacotes ou de amostragem

de fluxos. Na amostragem de pacotes, os mesmos podem ser selecionados aleatoriamente de acordo com uma função de distribuição de probabilidade ou os pacotes podem ser selecionados a cada intervalo de tempo definido. Na técnica de amostragem de fluxos, os fluxos também são amostrados de acordo com uma função de distribuição de probabilidade. Deve-se estudar qual a melhor abordagem para cada tipo de rede.

2.3.1 Amostragem de pacotes

Técnicas de amostragem de pacotes podem ser divididas em sistemáticas e aleatórias. Na amostragem sistemática, um pacote é deterministicamente selecionado baseado em um intervalo de tempo ou por quantidade de pacotes[4]. Por exemplo, pode-se selecionar um pacote a cada *t* segundos ou um pacote a cada *n* pacotes. Na amostragem aleatória, a amostragem é feita de acordo com uma função de densidade de probabilidade. Neste método, tem-se a amostragem n-em-N e a amostragem probabilística:

- n-em-N: A cada N pacotes, n são selecionados.
- Amostragem probabilística: Um pacote é selecionado de acordo com a probabilidade p. A probabilidade p pode ser fixa ou dependente de outros fatores como, por exemplo, o tamanho do pacote.

A amostragem aleatória de pacotes é de fácil implementação, porém possui a pior performance entre as formas de amostragem. Introduz um grande número de falsos positivos em port scans[8].

2.3.2 Amostragem de fluxos

Ao invés da amostragem por pacotes, pode-se amostrar por fluxos. Um dos métodos utilizados é a amostragem aleatória de fluxos. Primeiramente os pacotes são classificados em seus respectivos fluxos. Em seguida, os fluxos são amostrados com probabilidade *p*. A amostragem aleatória de fluxos gera grande demanda de CPU e memória. Duas outras formas de amostragem de fluxos resolvem parcialmente este problema, o *sample and hold* e o *smart sampling*[8].

No método sample and hold (*S&H*), quando é recebido um novo pacote, se não for parte de nenhum fluxo já criado, o fluxo, de tamanho *x*, poderá ser criado com probabilidade *p(x)*. Ou seja, a amostragem é dependente do tamanho do fluxo. A probabilidade p pode ser calculada pela fórmula 1, na qual z é um limiar entre uma melhor precisão ou melhor uso de largura de banda.

$$p(x) = p_z(x) = \begin{cases} \frac{x}{z} & \text{se } x < z \\ 1 & \text{se } x \geq z \end{cases} \quad (1)$$

Ou seja, para um x grande (e consequentemente um fluxo grande), maior ou igual a z, o fluxo será coletado.

Outro método desenvolvido é o smart sampling. Para cada pacote é verificado se o mesmo pertence a um fluxo já criado. Se pertencer, é adicionado ao fluxo. Ou seja, um vez que o fluxo é criado, todos os pacotes pertencentes a ele serão colectados. Se o pacote não fizer parte de um fluxo, é aleatoriamente coletado e um fluxo é criado com probabilidade h_S. h_S é escolhido para que cada byte tenha probabilidade *h*. Logo, para um pacote com tamanho *s*, a probabilidade h_S é dada pela fórmula 2.

$$h_s = 1 - (1 - h)^s \approx h.s \quad (2)$$

Novamente, quando maior s, o tamanho do fluxo, mais facilmente o fluxo será coletado.

A amostragem aleatória de fluxos apresenta a melhor performance entre as formas de amostragem apresentadas, possuindo a menor distorção para anomalias de volume de tráfego e port scans. A desvantagem é a necessidade de uso excessivo de CPU e memória[8] Tanto em S&H como smart sampling exigem um demanda menor do sistema com relação a amostragem aleatória de fluxos, porém são voltados para fluxos grandes. Fluxos pequenos podem ser omitidos mas também podem ter grande impacto.

3. Equipamentos

Fluxos podem ser coletados de diferentes formas, do modo mais simples e barato até soluções proprietárias de alta performance. A escolha do forma de coleta deve ser feita de acordo com o tipo da rede, os requirimentos e o orçamento.

Os dados podem ser coletados por uma solução e analisados por outra. Há também as soluções que coletam e analisam os dados.

3.1 Hub

Hub é um dispositivo que trabalha na camada um do modelo OSI e, diferentemente de um switch, replica os *frames* recebidos em uma determinada porta para todas as outras portas. Para coletar utilizando um hub, basta conectar flow collector em uma das portas do hub e todos os dados que chegarem ao hub serão também direcionados para esta porta[9].

Uma grande desvantagem dos hubs é o fato de serem half-duplex, ou sejam somente um dispositivo conectado a ele pode comunicar-se por vez, gerando colisões e diminuindo o desempenho da rede. Utilizar um hub para conectar o flow collectar à rede pode ser uma opção barata para redes de baixa velocidade, mas para redes da ordem de Gbps o desempenho da rede cairia drasticamente, tornando-o inviável.

3.2 SPAN ports

SPAN significa *Switched Port Analyzer* and também pode ser chamado de espelhamento de porta. Consiste em uma porta de um *switch* configurada para espelhar o tráfego de outra porta. O flow exporter seria conectado à esta porta[9].

Quando o switch está sob grande carga, a SPAN port pode não ver todos os frames. O switch dá prioridade para passra o tráfego legítimo e, com o restante do processamento, duplica os frames para a SPAN port. Se todo o processamento for usado para o tráfego legítimo, os frames não serão duplicados na SPAN port. Em caso de redes de alta velocidade, os switches estariam sob grande carga frequentemente, causando falhas na análise dos fluxos.

3.3 TAP

Um *tap*, ou *test access port*, mostrado na figura 3, é um dispositivo colocado entre dois equipamentos de rede e consegue duplicar todo o tráfego para um terceiro equipamento. Normalmente uma porta é ligada ao roteador de borda e outra ao firewall. As outras duas portas replicam o tráfego, uma em um sentido e a outra no sentido oposto. O tráfego destas duas portas podem analisados separadamente ou combinados para análise[9].

Figura 3 - TAP

As TAPs tem vantagens sobre o uso de HUBs e SPAN ports. TAPs suportam tráfego full duplex, capturam todos os pacotes, não descartam pacotes mal formados (como switches) e não são um ponto a mais de falha na rede pois mesmo sem energia ainda conseguem passar pacotes. Algumas TAPs também podem funcionar como regeneradores de sinal.

3.4 Hardware especializado

Existem equipamentos especilizados na coleta e análise do tráfego. Dois exemplos são o IBM Proventia® Management SiteProtector™ e o Check Point IPS-1. O Check Point IPS-1 é um equipamento que pode operar em até 1Gbps com o modelo 9070[10].

Figura 4 - Check Point IPS-1 9070[10]

O IBM Proventia Network IPS GX5108 opera em até 1.2Gbps[11].

Figura 5 - IBM Proventia IPS GX5108[11]

Para redes de alta velocidade, as melhores alternativas são os TAPs e hardwares especializados, pois conseguem trabalhar com grande *throughput*. Hubs não são adequados para redes de alta velocidade pois operam em half duplex e SPAN ports podem não conseguir duplicar todos os pacotes para a porta de monitoração em situações de alta demanda.

4. Detecção de ataques

Detecções de ataques podem ser classificados de acordo com as categorias abaixo[4].

- Método de detecção – Pode ser baseado em uma definição de comportamento normal do sistema e é chamado de *behavior-based*. Se os dados combinam com uma definição de ataque, o sistema é chamado de *knowled-based*. O sistema também pode ser classificado em função da sua capacidade de automaticamente construir um modelo de comportamento normal do sistema ou se este modelo é programado por um desenvolvedor.
- Comportamento ao detectar ameaça – Um sistema pode gerar um alerta para ser analisado manualmente (sistema passivo) ou tomar uma ação contra o atacante (sistema ativo).
- Localização dos dados – Os dados analisados podem ser logs, pacotes ou alertas gerados por outros sistemas.
- Paradigma de detecção – O IDS pode detectar o status atual do sistema (seguro ou inseguro) ou detectar uma mudança de estado (de seguro para inseguro).
- Frequência – O sistema pode realizar análises em tempo real (análise contínua) ou após a ocorrência do evento (análise periódica).
- Local de processamento dos dados – O sistema pode ser centralizado ou distribuído.
- Local de coleta dos dados – Pode ser centralizada ou distribuída.
- Segurança – O IDS pode ser também alvo de ataques.
- Grau de interoperabilidade – O sistema pode trocar dados com outros

sistemas ou operar sozinho.

Existem diversos tipos de ataques, cada um com as suas particularidades. Abaixo são classificados os principais tipos de ataques[4].

- Buffer overflow – É ataque com objetivo de travar um sistema ou conseguir controle através do transbordamento de buffer em um determinado processo.
- DoS ou DDoS – Ataque de negação de serviço com objetivo de sobrecarregar um ou mais elementos da rede.
- Busca de informações – Ataque com objetivo de angariar informações sobre um sistema para usá-las depois em outro tipo de ataque. Abrange sniffing e port scans.
- Cavalos de tróia – Programa malicioso normalmente escondido em outro programa.
- Worms – Programa que se auto-propaga pela rede e possui uma disseminação muito rápida.
- Vírus – Parecidos com worms, porém não conseguem se auto-propagar; precisam de intervenção humana para ir de um host a outro. Possuem uma disseminação lenta.
- Botnets – Grupos de computadores infectados que podem ser controlados remotamente para realizar outros tipos de ataques. São utilizadas principalmente como infraestrutura para realizar qualquer tipo de ataque distribuído, como DDoS.

Devido à sua característica, a detecção por fluxos não consegue detectar todos os tipos de ataques. A seguir serão apresentados alguns ataques e suas formas de detecção em IDS baseados em fluxo.

4.1 Negação de serviço (DoS)

Ataque de negação de serviço podem ser divididos em ataques lógicos e ataques de flooding. Ataques lógicos podem ser evitados com atualizações de software e filtros de determinados tipos de pacotes.

Um exemplo de ataque lógico é o *Ping of Death*[7]. Este ataque é baseado no tamanho máximo de um pacote IP, definido em 65.353 bytes. Apesar de um pacote maior do que 64kB ser ilegal de acordo com o protocolo IP, é possível enviá-lo. A técnica consiste em fragmentar o pacote para enviá-lo e quando for remontado no destinatário poderá causar buffer overflow e travar o sistema. Um IDS ou mesmo um firewall poderiam detectar o ataque através da análise do header do pacote ICMP. Se o offset do fragmento mais o tamanho do pacote for maior que 64kB, caracteriza-se um ataque Ping of Death. Este é uma falha já corrigida na maioria dos sistemas atuais.

Ataques do tipo flooding geram uma variação sensível no número de fluxos na rede, sendo visível em um IDS baseado em fluxos. Também podem ter determinadas flags no cabeçalho TCP, sendo também visível em um fluxo.

Um exemplo de ataque de negação de serviço que é facilmente detectado por um IDS baseado em fluxos é o SYN FLOOD[13]. Como mostrado na figura 6, para iniciar uma conexão TCP entre os nós A e B, primeiramente A envia um pacote com o bit SYN ligado. Ao receber este pacote, o nó B reserva recursos no sistema para a conexão e retorna um pacote SYN+ACK. Finalmente, A envia um pacote ACK para confirmar a abertura da conexão e neste ponto, dados podem ser trocados entre A e B. Para

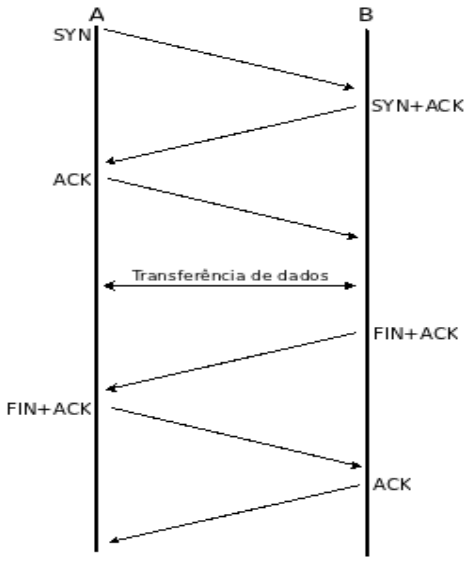

Figura 6 - Conexão TCP

finalizar a conexão, qualquer um dos nós pode enviar um pacote FIN e os recursos daquela conexão são usados.

Porém, se o nó A tiver a intenção de afetar o serviço do nó B, pode enviar diversos pacotes TCP com o flag SYN ligado, conforme a figura 7. Isto irá abrir muitas conexões no nó B e consequentemente muitos recursos serão consumidos afetando o desempenho do sistema. Como o ataque é baseado em flags no cabeçalho TCP, pode ser detectado em um fluxo.

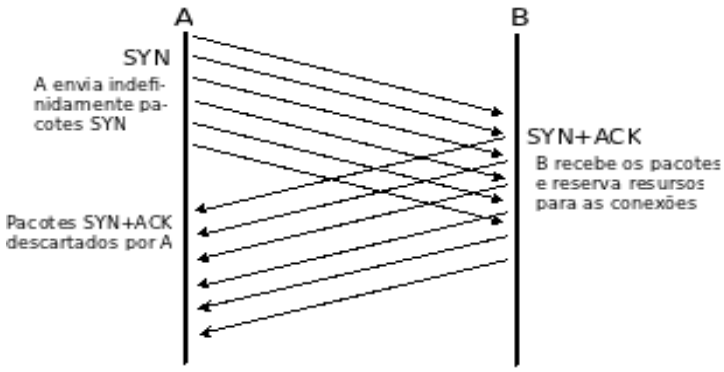

Figura 7 - Ataque por SYN FLOOD

4.2 Scans

Um scan podem ter três classificações:

- Vertical scan – Um host escaneando uma porta específica em vários hosts.
- Horizontal scan – Um host escaneando diversas portas em um único destino.
- Block scan – Uma combinação de vertical scan e horizontal scan.

Um scan normalmente gera diversos pequenos fluxos na rede, sendo possível identificar um ataque deste tipo pela análise dos fluxos[4].

Uma abordagem utilizada para identificar scans é monitoramento do número de conexões de saída da origem do host que executa o scan. Um host que está realizando um scan tem o número de conexões saintes sensívelmente aumentado. O IDS pode entender que este aumento como um ataque de scan[17].

Outra forma de detecção baseia-se no conceito de entropia. Quando um host está realizando um scan, é passível de mudança de entropia no seu tráfego. Considerando que um host está escaneando diversos outros hosts, com relação ao IP de origem a entropia diminui, pois existe apenas um endereço IP em vários fluxos. Já em relação aos IPs de destino, a entropia aumenta, pois diversos hosts são escaneados simultaneamente. Este padrão na entropia pode ser usado por um IDS para identificar um ataque de scan[18].

4.3 Worms

Worms operam em duas fases: a fase de identificação dos alvos, na qual o worm investiga a rede para determinar para onde propagar-se e a fase de transferência, quando o worm é transferido de um host infectado para outro vulnerável. Em IDS baseados em fluxo, é possível detectar apenas a primeira fase, a identificação dos alvos, já que é muito difícil detectar código malicioso sendo transferido sem analisar o payload na fase de transferência. Em muitos casos, a detecção da fase de identificação dos alvos é parecida com um ataque de scan[4].

Uma abordagem utilizada para detectar worms envolve separação dos tipos de tráfegos em três classes: “Traffic”, “Connector” e “Responder”. A classe Traffic envia muito mais tráfego do que recebe, típicamente worms que se propagam por e-

mails por exemplo. A classe Responder é identificada por conexões bidirecionais, ou seja, possui fluxos nas duas direções. Hosts que respondem a scans TCP ou iniciam conexões tem este padrão de tráfego. A classe Connector é caracterizada por muitas conexões saintes, típico de hosts que realizam scan em outros.

Um host pode fazer parte de mais de uma classe, gerando um total de 8 classes distintas: T (Traffic), R (Responder), C (Connector), T∩C, T∩R, R∩C, T∩C∩R e sem classe. Determinados padrões de classes presentes na rede podem indicar que existe um worm em atividade[21].

Algum worms também pode utilizar um outra forma de infecção chamada *hit-list*. O worm procura por hosts que supostamente estão sempre online para iniciar a proliferação. Isto aumenta a fase inicial de proliferação de um worm, que normalmente é lenta. Para detectar esta fase inicial do worm, o tipo de tráfego na rede é dividido pelo sistema de monitoramento (HTTP, FTP, SMTP ou Oracle). É considerado que o número de hosts utilizando um determinado protocolo é regular ao longo do tempo. Além disso, o padrão de comunicação entre os hosts tem as mesmas propriedades. Esta regularidade é alterada quando um hosts inicia a escanear a rede segundo um hit-list. Primeiramente hosts que normalmente nunca estão presentes no tráfego monitorado aparecem. Em seguida, um mesmo nó conecta com estes hosts. Desta forma, é possível determinar que o nó está tentando comunicar-se com servidores de uma hit-list para tentar disseminar o worm[20].

4.4 Botnets

Como uma botnet consiste de diversos hosts sendo controlados por um mestre, a abordagem normalmente utilizada resume-se em identificar e eliminar o mestre. Isto normalmente é feito pela análise de fluxos com determinados padrões

gerados pelo mestre. Diferentemente de ataques DoS e scan, as botnets não podem ser detectadas rapidamente. É necessária uma longa observação para seja possível identificar o controlador da botnet[4].

Apesar de existirem alguns resultados já apresentados na detecção de botnets, este tipo de estudo ainda está em desenvolvimento e não há um método eficiente para detecção de botnets. Provavelmente isto se deve a característica dinâmica das botnets.

5. Conclusão

Após o estudo de IDS baseados em fluxos IP, pode-se concluir que este é um método que interessante de ser utilizado em grandes redes de telecomunicações. Tomando por base redes de operadoras de telecomunicações, é normal que dezenas de Gbps de tráfego passem por um único link. É muito improvável que algum NIDS consiga operar neste tipo de rede e fazer a análise do payload dos pacote em tempo real sem deixar de analisar uma parte muito grande dos dados.

NIDS baseados em fluxo detectam muito bem ataques DDoS, pois basicamente este tipo de ataque gera um aumento sensível e anormal da banda utilizada. Considerando que o principal objetivo das operadoras é evitar que ataques gerem muito tráfego e congestionem a sua rede, estes sistemas mostram-se como uma boa alternativa.

Referências

1 UR, Rehman Rafeeq. **Intrusion Detection with Snort - Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and Acid**. 1ª ed. Prentice Hall, 2003.

2 Wikipedia. **Intrusion detection system**. Disponível em <http://en.wikipedia.org/wiki/Intrusion_detection_system>. Acesso em 22 abr. 2011.

3 LARRIEU, Cyrille**. Sistemas de Detecção de Intrusão**. Disponível em <http://pt.kioskea.net/contents/detection/ids.php3>. Acesso em 24 mai. 2011.

4 SPEROTTO, Anna; SCHAFFRATH, Gregor; SADRE, Ramin; MORAIU, Cristian; PRAS, Aiko; STILLER, Burkhard. **An Overview of IP Flow-Based Intrusion Detection**. Communications Surveys & Tutorials, IEEE, v. 12, abr. 2010. Disponível em: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=5455789>. Acesso em 17 jan. 2011.

5 Network Working Group. **RFC 3954, Cisco Systems NetFlow Services Export Version 9**.
Disponível em <http://www.ietf.org/rfc/rfc3954.txt>. Acesso em 22 abr. 2011.

6 Network Working Group. **RFC 5101, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information**.
Disponível em <http://tools.ietf.org/html/rfc5101>. Acesso em 22 abr. 2011.

7 Network Working Group. **RFC 5102, Information Model for IP Flow Information Export**.
Disponível em <http://tools.ietf.org/html/rfc5102>. Acesso em 22 abr. 2011.

8 MAI, Jianning; CHUAH, Chen-Nee; ASHWIN, Sridharan; YE, Tao; ZANG, Hui. Labs. **Is Sampled Data Sufficient for Anomaly Detection?** Internet Measurement Conference, out. 2006. Disponível em <http://conferences.sigcomm.org/imc/2006/papers/p17-mai.pdf>. Acesso em 12 mai. 2011.

9 BEJTLICH, Richard. **The Tao of Network Security Monitoring Beyond Intrusion**

Detection. 1ª ed. Addison Wesley, 2004.

10 Check Point. **Check Point IPS-1**. Disponível em <http://www.checkpoint.com/products/ips-1> Acesso em 21 mai. 2011.

11 IBM. **Proventia Server IPS**. Disponível em <http://www.ibm.com/br/services/sps/iss/ips/psips.phtml>. Acesso em 31 mai. 2011.

12 Insecure.org. **Ping of Death**. Disponível em <http://insecure.org/sploits/ping-o-death.html>. Acesso em 28 abr. 2011.

13 KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: Uma abordagem top-down**. 3ª ed. Addison Wesley, 2004.

14 MOORE, David. **Inferring Internet Denial-of-Service Activity**. The Cooperative Association for Internet Data Analysis, 2001. Disponível em <http://www.caida.org/publications/papers/2001/BackScatter>. Acesso em 28 abr. 2011.

15 YANG, Guang. **Introduction to TCP/IP Network Attacks**. Departament of Computer Science, Iowa State University. Disponível em <seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf>. Acesso em 19 mai. 2011.

16 KIM, M.-S.; KONG, H.-J.; HONG S.-C.; CHUNG, S.-H ; HONG, J. **A flow-based method for abnormal network traffic detection**. Departament of Computer Science and Engineering, Pohang University of Science and Technology. Disponível em <http://dpnm.postech.ac.kr/papers/NOMS/04/security-analysis/camera-ready/attack-analysis-v5-revision.pdf>. Acesso em 19 mai. 2011.

17 ZHAO Q.; XU, J.; KUMAR, A. **Detection of super sources and destinations in high-speed networks: Algorithms, analysis and evaluation**. Communications, IEEE, v. 24, 26 oct. Disponível em <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1705616>. Acesso em 12 abr. 2011.

18 WAGNER, A; PLATTNER, B. **Entropy based worm and anomaly detection in fast IP networks**. Communications Systems Laboratory, Swiss Federal Institute of Technolgy, Zurich. Disponível em <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.67.8921&rep=rep1&type=pdf>. Acesso em 12 abr. 2011.

20 COLLINS, M.; REITER, M.; **Hit-list worm detection and bot identification in large networks using protocol graphs**. Software Engineering Institute, Carnegie Melon Institute. Disponível em <www.cs.unc.edu/~reiter/papers/2007/RAID.pdf>. Acesso em 14 abr. 2011.

21 DÜBENDORFER, T.; PLATTNER B.; **Host behavior based early detection of work outbreaks in internet backbones**. Swiss Federal Institute of Technology, Zurich. Disponível <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.9477&rep=rep1&type=pdf>. Acesso em 24 mai. 2011.

22 CHEEMA, F. M.; AKRAM, A.; IQBAL Z. **Comparative Evaluation of Header vs. Payload based Network Anomaly Detectors**. World Congress of Engineering, jul. 2009. Disponível em <www.iaeng.org/publication/WCE2009/WCE2009_pp515-519.pdf>. Acesso em 31 mai. Jun.