UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM AMBIENTE EXPERIMENTAL PARA ANÁLISE DE ATAQUES DE NEGAÇÃO DE SERVIÇO

DANIEL ROSA CANÊDO

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR

DISSERTAÇÃO DE MESTRADO

PUBLICAÇÃO: 291/06

BRASÍLIA / DF: 12/2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM AMBIENTE EXPERIMENTAL PARA ANÁLISE DE ATAQUES DE NEGAÇÃO DE SERVIÇO

DANIEL ROSA CANÊDO

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Doutor, UnB
(ORIENTADOR)

ANDERSON CLAYTON ALVES NASCIMENTO,Ph.D., UnB
(EXAMINADOR INTERNO)

JOSÉ LUIZ DE FREITAS JÚNIOR, Doutor, UCG
(EXAMINADOR EXTERNO)

GEORGES AMVAME NZE , Doutor, UnB
(SUPLENTE)

DATA: BRASÍLIA/DF, 13 DE DEZEMBRO DE 2006.

FICHA CATALOGRÁFICA

CANÊDO, DANIEL ROSA. Um Ambiente Experimental para Análise de Ataques de Negação de Serviço [Distrito Federal] 2006. (xx), (85)p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2006).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Segurança da Informação 2. Negação de Serviço
3. DDoS

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

CANÊDO, DANIEL ROSA(2006). Um Ambiente Experimental para Análise de Ataques de Negação de Serviço. Dissertação de Mestrado, Publicação XXX/ANO, Departamento de Engenharia Elétrica, Universidade de Brasília , Brasília , DF, (85)p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Daniel Rosa Canêdo
TÍTULO DA DISSERTAÇÃO: Um Ambiente Experimental para Análise de Ataques de Negação de Serviço
GRAU/ANO: Mestre/2006.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte desta dissertação de mestrado pode ser reproduzida sem a autorização por escrito do autor.

Daniel Rosa Canêdo
Qd02 Cj A-5 Bloco D Apto 101
CEP 73015-105 – Sobradinho – DF - Brasil

A minha esposa, aos meus pais e a minha filha Lauana, que está para nascer.

AGRADECIMENTOS

Ao meu orientador Prof. Dr. Rafael Timóteo de Sousa Júnior, pelo constante apoio, incentivo, dedicação e amizade essencial para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.
Ao Prof. Anderson Nascimento, do Curso de Engenharia de Redes de Comunicação - Departamento de Engenharia Elétrica, verdadeiro co-orientador deste trabalho, que, apenas por razões de regulamentação, não pode ser registrado formalmente como tal.
Aos bolsistas do Laboratório de Engenharia de Redes de Comunicação – LabRedes da Universidade de Brasília, pelas conversas enriquecedoras, ajuda em diversos aspectos, colaboração e amizade.
A todos, os meus sinceros agradecimentos.

RESUMO

Realizou-se um estudo sobre o ataque de negação de serviço e negação de serviço distribuído, abordando definições a respeito destes ataques, e os procedimentos utilizados para sua execução. Criou-se e analisou-se um ambiente de execução deste ataque e definiu-se uma metodologia de ações a serem executadas por organizações para se defenderem e se prevenirem do ataque.

ABSTRACT

The work described in this dissertation has for objective to do a study about the attack denial of service and distributed denial of service, accomplishing definitions regarding these attacks, as well as the procedures used for your execution. This dissertation also has the objective of to create and to analyze an atmosphere of execution of this attack, defining a methodology of actions be executed by organizations to defend and to take precautions of the attack.

ÍNDICE

Capítulo **Página**

ÍNDICE DE TABELAS

Tabela **Página**

ÍNDICE DE FIGURAS

Figura **Página**

SIGLAS

ACK - *Acknowledgement*

CERT - *Community Emergency Response Team*

CSI/FBI - *Computer Security Institute/ Federal Bureau of Investigation*

DDoS - *Distributed Denial of Service*

DoS - *Denial of Service*

ICMP - *Internet Control Message Protocol*

IDS - *Intrusion Detection System*

IP - *Internet Protocol*

ISP - *Internet Service Provider*

RTT - *Round Trip Time*

SYN - *Synchronize*

TCB - *Transmission Control Block*

TCP - *Transmission Control Protocol*

UDP - *User Datagram Protocol*

1. INTRODUÇÃO

A Internet tornou-se um meio de comunicação e de interação mais utilizado pela população mundial, tendo se transformado em um recurso para o processamento e a troca de dados importantes e sigilosos, como por exemplo: senhas de cartões de crédito e de banco. Em função disso, a Internet passou a ser objeto de ações deliberadas que visam o comprometimento dos serviços da rede e danos às informações e aos usuários. Uma sub-classe especifica dessas ações prejudiciais consiste de ataque de Negação de Serviço - DoS (*Denial of Service*), assim denominados por que tem como objetivos provocar a inacessibilidade de um serviço provido por um recurso computacional ou por um elemento da estrutura de comunicação de rede.

Atualmente, as empresas dependem cada vez mais dos sistemas de informação e da Internet para fazer negócios, transações bancárias, treinamentos e outras atividades, não podendo se dar ao luxo de sofrer interrupções em suas operações. Um incidente de segurança pode impactar diretamente e negativamente as receitas de uma corporação, a confiança de sus clientes e o relacionamento com sua rede de parceiros e fornecedores.

Os incidentes de segurança da informação vêm aumentando consideravelmente e assumem as formas mais variadas, como por exemplo : infecção por vírus, acesso não autorizado, ataques *Denial of Service* contra redes e sistemas, fraudes internas e externas, uso não autorizado de redes sem fio, entre outros.

O ataque anônimo de negação de serviço é caracterizado pelo completo desconhecimento da sua verdadeira origem. Este ataque é realizado pelo envio de pacotes a uma taxa bem superior que a taxa que os roteadores possam processar para um determinado serviço, fazendo com que requisições legítimas do serviço não sejam atendidas. Os pacotes enviados para a vítima para concretizar o ataque podem ser organizados de forma distribuída, caso em que os pacotes são enviados de diferentes origens, aumentando consideravelmente o tráfego gerado para a vítima fazendo com que o serviço da vítima seja totalmente inutilizado. Nos dias atuais, o número de ataques gerados de forma distribuída a grandes sítios se torna cada vez mais alarmante e mais freqüente, existindo pragas digitais com o propósito especifico de gerar tal ataque.

Por outro lado, a atual infra-estrutura de comunicações da Internet tem como principal componente o roteador, o qual é responsável por designar rotas durante o tráfego de um pacote IP até este chegar ao seu destino [1][2][3][4]. Hoje as estruturas de roteadores ainda continuam vulneráveis a ataques anônimos de negação de serviço.

Verifica-se que a negação de serviço é um ataque cuja freqüência está crescendo desde o ano de 1999 quando se detectou os primeiros grandes ataques a sites de grande utilização, como CNN, eBay, ZDnet, Time Warner, Amazon e Yahoo [5]. Para as vítimas, os resultados destes ataques, em sua maioria, são financeiramente desastrosos, por isso há uma grande necessidade de se estudar e criar soluções para identificar sua ocorrência, bem como poder descobrir a verdadeira origem de determinado ataque. Vale notar que, dentro das limitações técnicas utilizadas, alguns autores [1][2][3][4] puderam observar mais de 4.000 ataques por semana. Pelo fato de os métodos empregados não conseguirem detectar todos os ataques que ocorrem na Internet, este valor é na verdade menor do que o número real de ataques. Os registros de ocorrência mostram que uma grande parte dos ataques é direcionada a vítimas brasileiras. De acordo com as pesquisas realizadas pelo CERT (*Community Emergency Response Team*), o domínio .br é o quarto domínio mais atacado por inundações, visando a negação de serviço. Em toda a Internet, somente os domínios .net, .com e .ro foram mais atacados que o domínio brasileiro. Uma informação do CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation*) [6] sobre crimes na área da computação afirma ainda que os ataques de negação de serviço estão entre os incidentes de segurança que mais causam prejuízo às instituições americanas.

É possível realizar o ataque de DoS e DDoS (*Distributed Denial of Service*) devido ao fato de se poder colocar pacotes na rede com endereços de origem forjados no datagrama usado no protocolo IP (*Internet Protocol*) [24]. Isto é possível, pois não existe uma entidade ou um mecanismo responsável pela verificação da autenticação de cada pacote vindo da fonte. A atual lógica do roteamento está baseada única e exclusivamente no endereço de destino, fazendo com que pacotes com endereços forjados alcancem o destino sem dificuldades. Desta forma um ataque pode forjar diversos endereços de origens tornando mais difícil a identificação da verdadeira origem do ataque.

Outra característica que permite a execução do ataque de negação de serviço e de sua forma distribuída é o fato de que nos roteadores não é armazenada para possíveis consultas futuras nenhuma informação relativa aos pacotes enviados. Em conseqüência disto, o

encaminhamento de pacotes não deixa pistas, tornando muito difícil descobrir qual rota seguiu até chegar no destino.

Essa situação motivou a escolha do tema para a presente dissertação e determinou uma abordagem de pesquisa, cujos objetivos são apresentados a seguir, assim como a organização adotada para a redação do texto.

1.1. OBJETIVOS

Este trabalho tem por objetivo fazer uma abordagem dos principais conceitos a respeito de segurança da informação no tocante aos ataques de negação de serviço e negação de serviço distribuído. Tanto para o ataque de negação de serviço simples quanto para o de forma distribuído o texto apresenta uma parte conceitual, a qual se dedica a explicar o contexto de realização dos ataques, seguida de uma descrição detalhada dos passos a serem seguidos para a execução de tais ataques.

Também será apresentada a descrição de duas ferramentas utilizadas para a execução de ataques de negação de serviço distribuído, denominadas de TRIN00 e STACHELDRAHT, que foram incluídos de forma controlada nos experimentos a serem realizados neste trabalho. Para verificar a ocorrência real de um ataque de negação de serviço distribuído deverão ser apresentados em detalhes os tráfegos de pacotes pertencentes a cada ataque.

Outro objetivo do desenvolvimento deste trabalho é realizar algumas análises tanto em relação a aspectos técnicos a serem aplicados em uma rede, quanto a aspectos gerenciais para minimizar a ocorrência de um ataque de negação de serviço ou de negação de serviço distribuído em um ambiente organizacional ou em uma determinada rede de computadores. Ou seja, um dos principais propósitos deste trabalho é apresentar algumas medidas a se tomar para que se tenha um ambiente computacional com um risco mínimo a ataques de negação de serviço.

Este trabalho vem a contribuir para a comunidade acadêmica e também a todos os profissionais da área de administração de segurança, quanto ao conhecimento claro da realização e das possíveis conseqüências dos ataques de negação de serviço, bem como, as principais ações para defesa destes ataques. Também contribuirá para a realização de pesquisas na criação de aplicações capazes de detectar, defender e identificar a verdadeira origem de um ataque de negação de serviço..

1.2. ORGANIZAÇÃO

Este trabalho se divide em cinco capítulos, sendo que o segundo trata-se da definição, estruturação e exemplificação de ataques de negação de serviço, apresentando as principais ferramentas publicadas para a execução de ataques de negação de serviço distribuído, bem como definições e estruturação relativas a tais ferramentas.

No capítulo 3 são apresentadas as principais técnicas utilizadas tanto para defender quanto para se prevenir de ataques de negação de serviço distribuído, levando em consideração as vulnerabilidades utilizadas pelos ataques, especificamente no que se refere aos protocolos TCP [25], UDP [26] e ICMP [27].

O capítulo 4 apresenta o ambiente realizado na simulação, relatando as instalações das ferramentas utilizadas, principais comandos e também apresentando o tráfego existente em cada um dos ataques. Também são apresentadas neste capítulo as análises da parte técnica do ambiente, assim como da parte de gerência de segurança e de medidas administrativas a serem adotadas em um ambiente computacional seguro.

O capitulo 5 se destina as conclusões decorrentes do trabalho e as sugestões de trabalhos futuros dele decorrentes.

2. NEGAÇÃO DE SERVIÇO E NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

O ataque de negação de serviço tem o objetivo de impedir que um usuário autorizado tenha acesso a serviços disponibilizados, por intermédio de uma rede, o que inclui serviços de processamento, armazenamento, comunicação e acesso a informações. Algumas maneiras de se realizar este tipo de ataque são:

- Inundar uma rede visando impedir que usuários legítimos façam uso dela;
- Impedir ou romper a conexão entre duas máquinas visando impedir o acesso a um serviço;
- Impedir o acesso de um determinado serviço ou site;
- Impedir ou negar um serviço a um sistema ou pessoa específica.

A seguir, tais formas de ataque são caracterizadas, a partir da apresentação de ataques reais descritos na literatura.

2.1. CARACTERÍSTICAS

Os ataques de DoS surgiram através da exploração de vulnerabilidades em implementações de serviços e de sistemas operacionais. Mais precisamente estes ataques atuam nas vulnerabilidades encontradas na pilha de protocolos TCP/IP, nos sistemas operacionais e nos programas servidores, facilitando que serviços de servidores de redes sejam negados a usuários autorizados.

Os principais ataques de negação de serviço são:

Ping-of-Death

Caracterizado por gerar um *buffer overflow* quando o *host* atacado recebe um pacote ICMP de tamanho superior a 65535 bytes, causando reinicialização ou desativação do sistema operacional do *host* atacado [7].

O protocolo IP permite o tamanho máximo de um pacote até 65536 octetos (1 octeto=8 bits), contendo um mínimo de 20 octetos para o IP *header* e 0 ou mais octetos para informação adicional. É conhecido que alguns sistemas reagem de uma forma imprevisível quando recebem pacotes de tamanho acima do estabelecido, vulnerabilidade esta que é explorada pelo ataque *ping-of-death*.

No *ping* normal do protocolo ICMP, um host envia à máquina destino um ICMP_ECHO-REQUEST e, se essa máquina estiver ativa, envia como resposta um ICMP_ECHO-RESPONSE. No *ping-of-death* os atacantes constroem datagramas ICMP_ECHO-REQUEST de tamanho acima do valor padrão de forma a enviar pacotes ping acima com mais de 65536 bytes.

SSPing

Este ataque DoS se caracteriza pelo envio de uma série de pacotes ICMP acima do tamanho permitido, mas altamente fragmentados [8].

Na execução deste ataque uma máquina tenta enviar grandes pacotes pela rede ou pela Internet, explorando a grande possibilidade de que os roteadores que processam os pacotes tentem fragmentá-los em blocos menores para serem corretamente encaminhados pela rede até ao destino. Caso a fragmentação ocorra, a máquina de destino recebe os fragmentos dos pacotes e faz a remontagem dos pacotes originais.

Como o atacante enviou pacotes ICMP acima do tamanho e altamente fragmentados através da rede, a vítima que recebe os pacotes vai tentar fazer a remontagem, guardando os fragmentos pela ordem até formar cada pacote. Pacotes altamente fragmentados exigem que a entidade IP mantenha a informação adicional para remontar corretamente o pacote. Se o software de controle de pilha do IP não for construído corretamente, ao tentar ordenar os diversos pacotes, sua execução pode resultar em *memory overflow*, fazendo com que a máquina vítima pare de responder. Normalmente o atacante precisa enviar alguns pacotes para paralisar a vítima.

Land Attack

Este tipo de ataque é realizado pelo envio de um pacote TCP SYN (primeira parte do *three-way handshake* do TCP) em que o endereço de destino e de origem são os mesmos, bem

como as portas de origem e destino [8]. A manipulação necessária para tanto é realizada pelo programa Land attack.

Em circunstâncias normais o endereço de origem será o da máquina que faz o pedido de conexão, bem como a porta será a do protocolo de aplicação utilizado. Já no Land attack, o atacante primeiro faz o spoofing do endereço IP e da porta da vítima para colocá-los no pacote de ataque.

Como o protocolo TCP é um protocolo orientado a conexão, sua operação começa por uma fase em que é feito o denominado *three-way handshake* para iniciar a comunicação. Quando uma conexão é iniciada, utiliza-se pacotes de SYN para sincronizar as duas máquinas. Os pacotes de SYN são iguais aos pacotes normais, só que têm ativo o bit SYN, que indica os primeiros pacotes para iniciar a comunicação.

A máquina da vítima do land attack recebe então o pacote de conexão e responde ao seu próprio endereço de origem com sua própria porta de origem, correndo o risco de auto-bloqueio por não saber o que fazer do pacote.

SYN Flooding

Caracterizado quando um *host* é atacado por intermédio de várias tentativas de estabelecer uma conexão para um serviço. Ao executar o *three-way handshake* o *host* responde normalmente, mas o atacante não dá continuidade ao processo. Caso o software TCP do *host* pare de aceitar novas conexões até obter uma resposta das que já estão tentando se conectar, esse *host* ficará bloqueado e não enviará resposta a outra tentativa normal de conexão que receberá um timeout após alguns minutos [8].

UDP packet storm

Este ataque se caracteriza pelo uso da porta UDP/echo, fazendo com que o *host* solicitado envie indefinidamente e em uma velocidade alta pacotes para a estação vítima.

Smurf

O ataque Smurf faz uso da existência de um endereço de broadcast de uma rede, que irá permitir que uma estação remota solicite uma resposta de todas as estações em uma determinada rede. O atacante irá forjar o endereço de uma estação e emitir um fluxo constante

de requisições utilizando o endereço de broadcast, em que um único pacote enviado pelo atacante pode facilmente ser multiplicado por 100 vezes ou mais [8].

IP Spoofing

IP Spoofing é uma técnica presente nos ataques de negação de serviço que tem o objetivo de forjar endereços IPs do remetente de um pacote IP. Esta é uma técnica muito utilizada em comunicações que exijam confiança, pois pode acarretar a aceitação de pacotes dentro de uma rede, tornando uma ferramenta extremamente útil dentro de um ataque Denial of Service [7] [28].

2.2. NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

O ataque DDoS, também conhecido como ataque de negação de serviço distribuído, que consiste da tentativa de paralizar um serviço através de computação distribuída. Para este novo enfoque do ataque de negação de serviço, os ataques não são mais focados no uso de um único *host* para iniciar um ataque e sim no uso de centenas ou milhares de *hosts* coordenadamente para realizar o ataque.

Os ataques de negação de serviço distribuído empregam técnicas semelhantes à computação distribuída ou sistemas distribuídos, de modo que os ataques são efetuados a partir de diversos computadores simultaneamente. Nesta forma de ataque, é feita uma sobrecarga ou inundação de pacotes com o objetivo de paralizar um serviço, *host* ou rede, fazendo com que dados sejam gerados numa quantidade superior à que o *host* ou a rede pode suportar, deixando serviços instáveis ou bloqueados.

Os primeiros ataques de negação de serviço distribuído documentados surgiram em agosto de 1999, sendo mais eficaz e definitivamente considerado um ataque poderoso na semana de 7 a 11 de Fevereiro de 2000, quando os sites do Yahoo, Ebay, Amazon e CNN ficaram inoperantes por algumas horas. Uma semana após serem documentados esses ataques, foram detectados ataques em brasileiros tais como: UOL, Globo On e IG [9].

Nos dias de hoje, segundo estatísticas realizadas pelo CERT/CC, diversos ataques de DoS e DDoS são registrados diariamente envolvendo novos vermes (um verme é um programa capaz de se reproduzir e utilizar canais de comunicação desprotegidos para passar

de uma máquina para outra em uma rede) e novas ferramentas de se implantar o ataque DDoS, estas ferramentas serão tratadas com maior detalhes posteriormente. Em alguns dos vermes utilizados nestes ataques são utilizados comandos e estruturas de controles que permitem ao atacante modificar de forma dinâmica o comportamento deste verme assim que ele infectar a vítima.

2.3. DESCRIÇÃO ATAQUE DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

Ataques DDoS corresponde a ataques de negação de algum serviço de forma distribuída para alguma determinada vítima. Antes de descrever em detalhes como ocorre este ataque é necessário determinar e definir os participantes e suas funções. Atualmente não existe uma padronização de nomenclatura para os personagens deste ataque, portanto será utilizada a nomenclatura adotada por pesquisadores. Deve-se salientar que ao longo deste trabalho será utilizado a seguinte notação para os personagens de um ataque DDoS [09][10]:

- Atacante: Integrante que efetivamente coordenará o ataque;
- Master ou Mestre: Integrante que recebe os parâmetros do atacante e comanda os agentes para a execução do ataque;
- Agente ou Zumbi: Integrante que concretizará o ataque DDoS contra uma ou mais vítimas, conforme especificação do atacante;
- Vítima: Integrante ou integrantes que serão alvos do ataque. Pode ser um *host* que será inundado por um volume enorme de pacotes, o que provavelmente irá causar um congestionamento da rede, provocando a paralisação de um ou mais serviços oferecidos pelo *host*;
- Cliente: Aplicação que reside no Master ou Mestre, e que terá a função de controlar os ataques, enviando comandos aos Daemons do Agente ou Zumbi;

- Daemons: Processos que estarão rodando no Agente ou Zumbi, e que serão responsáveis por receber e executar os comandos enviados pelo cliente.

O ataque de DDoS realiza-se em 3 fases distintas : A fase de intrusão em massa, a fase de instalação de software DDoS e fase de inicialização do ataque.

A fase de intrusão corresponde a execução de ferramentas ou aplicativos que têm o objetivo de comprometer máquinas clientes e obter acesso privilegiado de tal forma a permitir que o atacante tenha controle remoto total do *host* Cliente. Para esta fase executa-se os seguintes passos:

1 Realiza-se uma varredura ou *megascan* em redes de computadores consideradas por um atacante como interessantes, por exemplo, redes com conexão de banda larga ou com baixo grau de monitoramento;

2 Após realizar as varreduras, deve-se explorar as diversas vulnerabilidades encontradas com o propósito de se obter o acesso privilegiado nas máquinas scaneadas;

3 Elabora-se uma lista com todos os endereços IPs das máquinas que foram scaneadas para que o atacante possa criar a rede do ataque DDoS.

Após realizar a fase de intrusão em massa, deve-se executar a fase de Instalação de software DDoS, em que o atacante instala softwares DDoS nas máquinas pertencentes a rede de ataque DDoS criadas pelo atacante. Para a execução são realizados os seguintes passos :

1 Em primeiro lugar deve-se criar uma conta de usuário qualquer para que se possa obter as versões de todas as ferramentas de ataques DDoS;

2 No momento em que a máquina for acessada, os binários, ou módulos, das ferramentas de DDoS serão instalados para permitir que o atacante tenha total controle remoto das máquinas. Estas máquinas comprometidas desempenharão os papeis de Master ou

Mestre. A escolha destes integrantes é de critério do atacante, sendo que o ideal é que cada master não seja manuseado e monitorado constantemente, e que tenham uma quantidade satisfatória de agentes ligados ao master;

3 Depois de instaladas as ferramentas de DDoS em cada master será instalado e executado o módulo daemon DDoS nos agentes. Os agentes através da execução do daemon informam ao master sua presença e fica a espera de comandos oriundos do Master ao qual estão ligados. Neste momento o software DDoS que está presente no master registra uma lista de IPs referentes as máquinas agentes ativas;

4 A partir desta comunicação automatizada entre master e agente, pode-se organizar um ataque DDoS, ou seja, neste momento cria-se a rede de ataque DDoS.

A fase de Instalação do Software DDoS resulta nas definições de master e agentes em uma rede de ataque de negação de serviço distribuído e suas respectivas comunicações, através de software de DDos, que serão descritos mais detalhadamente a seguir. A terceira fase concentra-se na própria execução do ataque, em que o atacante controla os masters, e estes, por sua vez, têm a capacidade de controlar vários agentes, que consolidará o ataque à vítima através das diversas maneiras de inundação de pacotes. Enquanto o ataque não ocorre, os agentes ficam esperando instruções dos master para atacar um ou mais endereços IP por um período de tempo determinado. A figura 2.1 mostra a estrutura de um ataque DDoS.

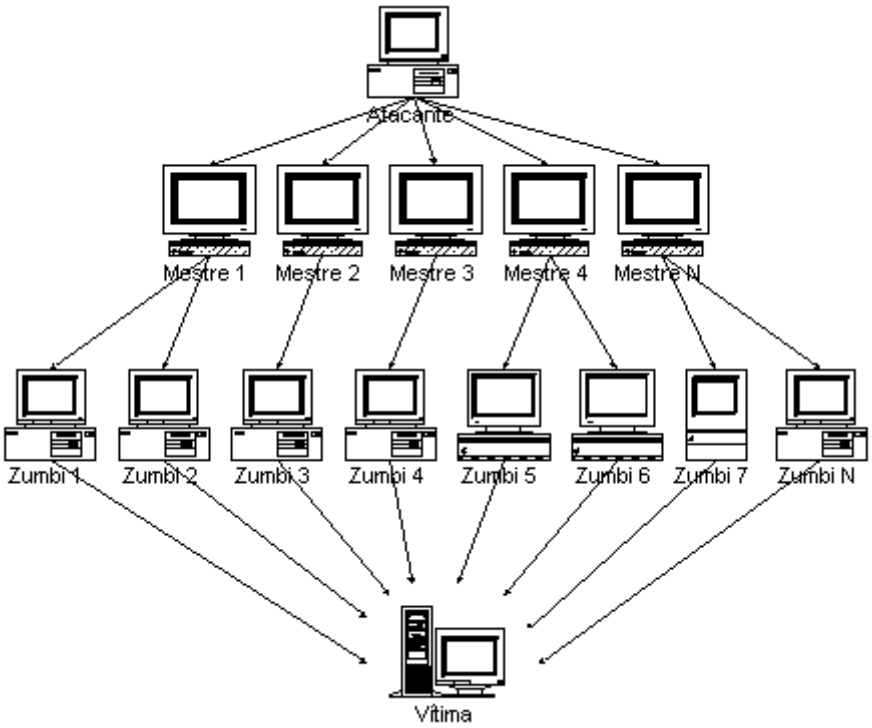

Figura 2.1 - Estrutura do Ataque DDoS.

Onde,

- Atacante: Representa o Atacante;
- Mestre: Representa os Masters;
- Zumbi: Representa os Agentes ou Zumbis;
- Vítima: Representa a Vítima do ataque.

2.4. FERRAMENTAS DE ATAQUE DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

Os ataques de negação de serviço não são novos e embora existam programadores que escrevam seus próprios códigos para estes ataques, já existem algumas ferramentas na Internet que são utilizadas para executarem tais ataques.

A primeira ferramenta encontrada que implementava um ataque de negação de serviço distribuído foi encontrada em 1998, vindo a partir deste momento a desenvolver diversas ferramentas cada vez mais sofisticadas e com interfaces mais amigáveis. Pode-se dizer que houve um grande crescimento de ataques deste tipo e que hoje é uma das grandes preocupações quanto a segurança da informação. Esta seção tem o objetivo de analisar o funcionamento das principais ferramentas utilizadas atualmente para realizar um ataque de DDoS, que são : TRIN00, TFN, STACHELDRAHT.

2.4.1. TRIN00

TRIN00 é uma das primeiras ferramentas que implementa ataques de negação de serviço distribuída de forma coordenada, em que tem por objetivo atacar uma vítima utilizando uma rede de ataque DDoS mostrada na figura 2.1[11][29].

A ferramenta TRIN00 tem como princípio básico realizar ataques do tipo UDP Flood coordenados por uma máquina atacante. O ataque UDP Flood consiste basicamente em inundar a vítima com pacotes UDP, pois estes pacotes não possuem nenhuma garantia de que a conexão foi realizada, ou seja, não há garantia que o pacote UDP foi realmente entregue na máquina da vítima. Por esta característica o atacante envia pacotes para todas as portas do host da vítima de forma randômica, ocasionando a inundação ou flooding da máquina vítima. No momento em que os pacotes UDP são recebidos pela vítima, esta máquina tenta determinar qual aplicação está a espera deste pacote na porta determinada. A vítima por sua vez, irá detectar que não existe nenhuma aplicação a espera de um pacote naquela porta e não enviará nenhuma mensagem ICMP para o destinatário informando que o pacote não encontrou o seu destino. Deve-se lembrar que nestes ataques os atacantes forjam os endereços de IP de origem de cada pacote, desta forma se houver uma grande quantidade de envios de

pacotes UDP para todas as portas de uma máquina poderá ocorrer que o sistema fique inativo podendo até ser reiniciado.

A partir desta descrição de ataques de UDP Flood, pode-se dizer que os ataques originados pela ferramenta TRIN00 têm o objetivo de interromper um serviço presente na máquina vítima, utilizando um flooding de pacotes UDP.

A rede de ataque TRIN00 é composta por um número pequeno de master ou mestres que tem o papel de comandar os agentes em um ataque, e um grande número de agentes que são as máquinas ou *hosts* que realmente irão realizar os ataques conforme especificação dos masters ligados a eles.

Todo ataque baseia-se no controle remoto, tanto de masters pela máquina atacante quanto de agentes pelos seus respectivos masters. O controle remoto do master é realizado utilizando uma conexão TCP na porta 27665, sendo que ao conectar, o atacante terá que fornecer uma senha normalmente "betaalmostdone", enquanto que o controle remoto dos agentes pelos respectivos masters é realizado através de conexões UDP na porta 27444 ou por conexão TCP na porta 1524. Neste controle é necessário o uso de uma senha padrão, "l44adsl", para executar os comandos nos agentes, sendo que apenas serão executados comandos que contêm a substring "l44". Neste ataque também ocorre a comunicação entre o agente e o master, pois os agentes devem informar aos masters que estão ativos e prontos esperando a execução de alguns comandos. Esta comunicação é realizada através de pacotes UDP na porta 31335, sendo que ao executar um daemon no agente este envia mensagens "*HELLO*" ao seu master respectivo, fazendo com que o master mantenha uma lista de IPs das máquinas agentes ativas.

Ao executar a ferramenta TRIN00 pode-se observar que no master encontra-se uma aplicação com o nome de master.c, enquanto que os daemons encontrados nas máquinas agentes podem receber uma variedade de nomes, dentre eles: ns, http, rpc.listen, trinix, etc.

De acordo com a análise do Projeto "TRIN00", há um cenário típico deste ataque que consiste em basicamente 4 etapas distintas que serão descritas a seguir.

Etapa 1: Esta fase tem o objetivo de descobrir um cenário ideal para a realização do ataque, em que deve conter um grande número de usuários conectados em uma rede utilizando uma largura de banda que permita a transferência de arquivo de forma rápida e sem

perda, ou seja, um cenário onde o atacante pode ser capaz de listar as vulnerabilidades por onde pode ocorrer o ataque.

Etapa 2: Nesta etapa faz-se uma varredura em redes que poderão vir a ser atacadas, para que identifiquem alvos de ataques. Estes alvos são identificados através das vulnerabilidades encontradas nos *hosts* das redes com relação a pilha TCP/IP, o que acarreta na possibilidade de obter acesso remoto dos integrantes da rede do ataque.

Etapa 3: Após obter os *hosts* que irão compor a rede do ataque DDoS, deve-se obter acesso remoto das máquinas mestres ou masters através da porta TCP 1524.

Etapa 4: Nesta etapa, tem-se o controle total das máquinas mestres e a iniciação dos controles das máquinas agentes, as quais realmente irão realizar o ataque. Nesta fase há uma comunicação entre master e agentes e vice-versa.

2.4.2. TFN -Trible Flood Network

Trible Flood Network é outra ferramenta que tem a capacidade de realizar diversos ataques de Negação de Serviço de forma coordenada com o objetivo de atacar uma ou mais vítimas pertencentes em uma rede de comunicação de dados. Para a realização de um ataque de negação de serviço é necessário primeiramente que se tenha a descrição da rede de ataque, a qual será composta por computadores master e computadores agentes conforme é descrito na figura 2.1[12].

A ferramenta TFN tem como principio básico realizar ataques de negação de serviço do tipo UDP Flood, SYN Flood, ICMP Flood e Smurf. A seguir, serão descritos de maneira detalhada estes ataques [14].

SYN Flood

O ataque de SYN Flood é baseado na conexão realizada pelo protocolo TCP, em que as entidades participantes executam o *three-way handshake* para efetuar a conexão entre duas máquinas. Esta conexão é mostrada em detalhes na figura 2.2[7].

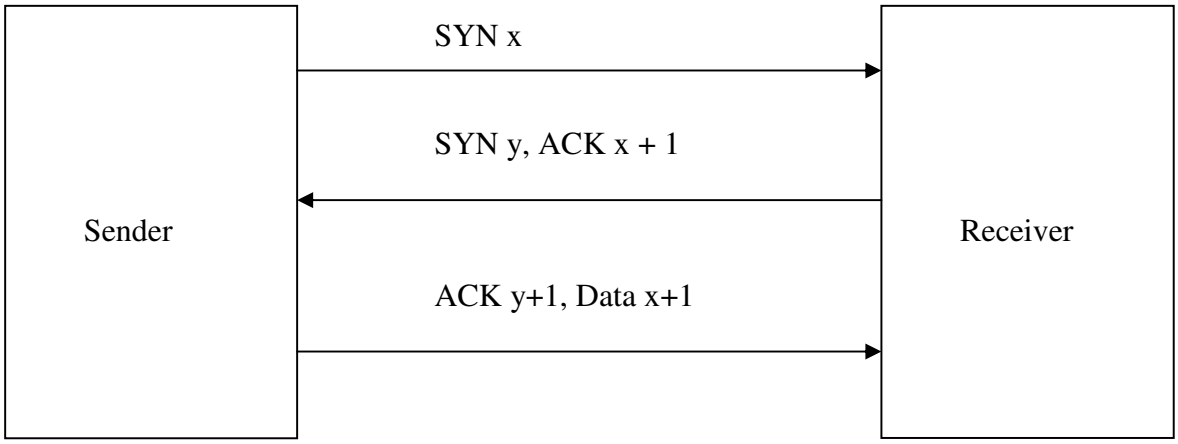

Figura 2.2 - Conexão do Protocolo TCP.

A conexão de duas máquinas ou *hosts* através do protocolo TCP se baseia na troca de três mensagens, em que o emissor envia uma mensagem ao receptor requerendo uma conexão, representada na figura por SYN x. A partir deste momento o emissor espera uma confirmação de recebimento da sua mensagem pelo receptor para que se possa estabelecer a conexão, que está representado na figura por SYN y, ACK x+1. Para estabelecer a conexão o emissor envia uma mensagem ao receptor com o objetivo de informar que recebeu a mensagem do receptor estabelecendo assim uma conexão entre as duas partes, sendo representada na figura por ACK y+1, Data x+1. Para estabelecer esta conexão algumas informações são armazenadas na memória, como por exemplo os valores dos números de seqüências utilizados durante a realização da conexão. Para esta alocação dá-se o nome de TCB (*Transmission Control Block*) que tem por objetivo armazenar todas as informações necessárias para que os sistemas operacionais sejam capazes de realizar tal conexão.

O ataque de SYN Flood tem como característica principal tentar realizar uma conexão TCP entre duas máquinas utilizando um IP forjado para o emissor, método conhecido como IP Spoffing. Desta maneira o host receptor irá alocar memória e recursos para armazenar as informações necessárias para tal conexão, mas como este não irá receber uma resposta de confirmação de sua mensagem (ACK y+1) então ficará em estado de repouso por algum tempo esperando a mensagem até que o seu TCB seja removido da memória. Isto faz com que haja um desperdício de recurso e tempo de processamento no host da vítima, o que irá favorecer no baixo rendimento do sistema operacional da vítima.

A ferramenta Trible Flood Network ao efetuar o ataque do tipo SYN Flood envia uma grande quantidade de pacotes com endereços IPs de origem forjados, fazendo com que na máquina da vítima ocorra um grande uso de memória e de CPU, tornando as aplicações que estejam executando nesta máquina, comprometidas. Isto por sua vez, pode acarretar até em reinicialização da máquina vítima. Como exemplo tem-se que em 2000 servidores do Yahoo e da Amazon sofreram este tipo de ataque [6].

ICMP Flood

O ataque do tipo ICMP Flood é caracterizado pelo uso de trocas de mensagens ICMP entre duas máquinas ou *hosts*. Este ataque se baseia fundamentalmente em saturar conexões, principalmente de Internet, através do envio continuo de mensagens de ICMP, utilizando o aplicativo ping. As mensagens trocadas entre as máquinas através de ping são um Echo Request por parte do emissor e um Echo Replay por parte do receptor.

Da mesma maneira que o ataque SYN Flood o ataque de ICMP Flood também armazena na memória as trocas de mensagens, o que irá prover um grande consumo de recursos e de processamento para responder a todas requisições de ping, fazendo com que a conexão fique comprometida podendo até provocar a reinicialização da máquina vítima [7].

SMURF

O ataque do tipo Smurf caracteriza-se pelo envio de mensagens ICMP para endereços de broadcast de redes de comunicação de dados vulneráveis [16]. O funcionamento deste ataque é bastante simples, porém possui resultados extremamente impressionantes.

O objetivo deste ataque não é de parar simplesmente uma máquina como os ataques do tipo UDP Flood, ICMP Flood, SYN Flood, mas sim de parar uma rede inteira. Este ataque funciona da seguinte maneira:

1 Em primeiro lugar o atacante realiza uma busca a fim de obter uma lista de endereços broadcast de redes vulneráveis;

2 Após obter os endereços de broadcast das redes vulneráveis, a máquina atacante envia pacotes ICMP com mensagens ICMP Echo_Request para o endereço de broadcast, sendo que o endereço de origem destes pacotes é identificado como o endereço da vítima;

3 As máquinas da rede que receber estes pacotes ICMP automaticamente irão enviar uma resposta ICMP Echo_Replay para a máquina da vítima e não para a máquina do agressor, devido ao método de IP Spoofing inserido pelo atacante. Desta forma dependendo do número de máquinas inseridas na rede pode haver uma falha de conexão nesta rede. A figura 2.3 mostra em detalhes a execução do ataque smurf.

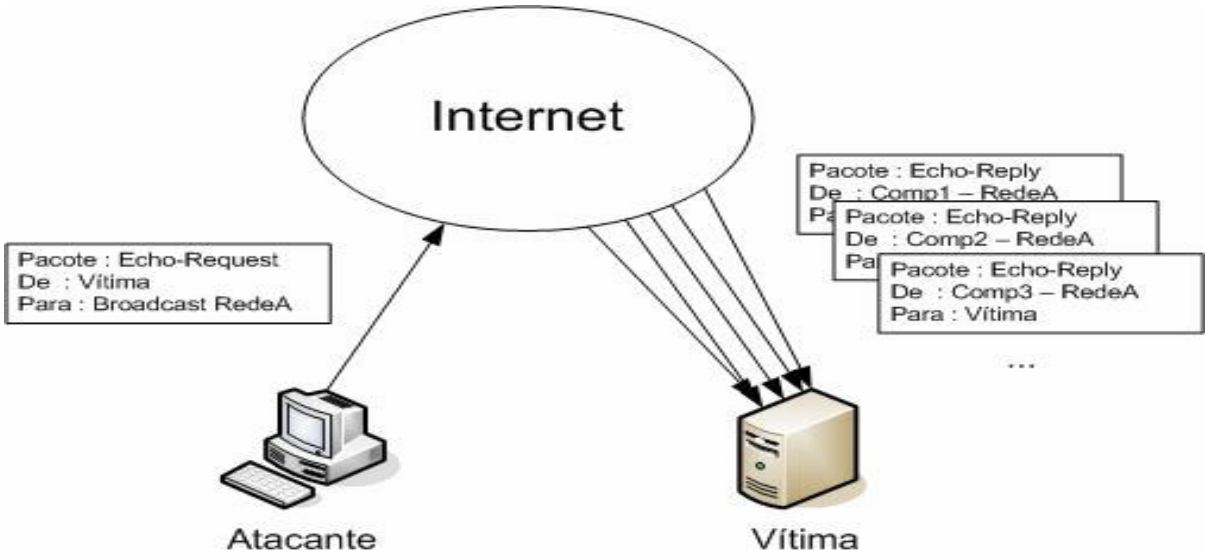

Figura 2.3 - Ataque SMURF.

A figura 2.3 mostra em detalhes a execução de um ataque do tipo smurf em uma única rede, em que o atacante envia mensagens ICMP Echo_Request para o endereço de broadcast da rede, fazendo com que todos os host da rede enviem uma mensagem ICMP Echo_Replay para o endereço de origem, identificados nos pacotes, que por sua vez é o endereço da vítima. A ferramenta Trible Flood Network tem a capacidade de efetuar este ataque de forma distribuída na Internet acarretando no baixo rendimento de servidores de Internet.

Após detalhar os tipos de ataques aplicados pela ferramenta TFN, percebe-se que a questão fundamental de sucesso da ferramenta e dos ataques gerados, é a capacidade de se aplicar o método de IP Spoofing, onde se pode forjar um endereço de origem e de destino dos pacotes transmitidos, o que irá dificultar ao máximo a descoberta do verdadeiro atacante.

Para a execução destes ataques de forma distribuída é necessário identificar quem serão os *hosts* masters e os *hosts* agentes, os quais irão de fato realizar o ataque. Da mesma maneira da ferramenta TRIN00 é necessário que haja um controle remoto dos masters e dos

agentes para que o ataque ocorra de forma distribuída. O controle remoto de uma máquina master em uma rede de ataque distribuída é realizado pelo próprio atacante através da execução de linhas de comandos que serão executadas pelo programa cliente que estará previamente instalado no master. Entre a máquina do atacante e a máquina master é necessário que exista uma conexão, a qual será realizada utilizando métodos de conexão, tais como : rsh, telnet, etc.

Após realizar a conexão o atacante não precisará de uma senha para executar os comandos do programa cliente, mas no entanto precisará de uma lista de endereços IPs das máquinas que possuem os daemons instalados, ou seja, precisa dos endereços IPs das máquinas designadas como agentes. Deve-se lembrar que antes de executar um ataque utilizando a ferramenta Trible Flood Network é necessário instalar os programas clientes e os daemons em suas respectivas máquinas para que se possa ter comunicação entre as máquinas da rede do ataque. A partir disso, tem-se que a comunicação entre o programa cliente e os daemons pertencentes a um ataque é realizada através de pacote ICMP_ECHOREPLAY, não existindo comunicação TCP e nem UDP entre as máquinas master e agente.

2.4.3. STACHELDRAHT

STACHELDRAHT também é uma das mais novas ferramentas utilizadas para executar um ataque de negação distribuída, tendo como alvo uma ou várias máquinas de uma rede de comunicação de dados [13]. Da mesma maneira que a ferramenta Trible File Network a ferramenta STACHELDRAHT tem a capacidade de gerar ataques de negação de serviço de forma coordenada, tais como : UDP Flood, TCP Flood, ICMP Flood e Smurf.

O funcionamento da ferramenta STACHELDRAHT se baseia na combinação das características básicas das ferramentas TRIN00 e Trible File Network no que se refere a comunicação das máquinas que compõe a rede de ataque de negação de serviço distribuída. No entanto a ferramenta STACHELDRAHT não utiliza somente as características de comunicação das ferramentas, mas também adiciona algumas particularidades como o uso de criptografia na comunicação realizada entre a máquina do atacante e as máquinas determinadas como masters, bem como também a atualização automática dos daemons que estão presentes nas máquinas determinadas como agentes em um ataque [13].

A idéia de se utilizar a criptografia na comunicação entre o atacante e as máquinas master surgiu exatamente pelo fato de ser uma fragilidade da ferramenta Trible File Network, a qual realizava tais comunicações de forma desprotegida, estando assim sujeitas a ataques de vulnerabilidades do protocolo TCP. Para solucionar este problema a ferramenta STACHELDRAHT utiliza de um utilitário chamado de telnet criptografado, o qual será responsável pela comunicação criptografada entre o atacante e os master de um ataque. Desta forma o controle remoto da máquina master pela máquina atacante é feita na ferramenta STACHELDRAHT através do utilitário telnet criptografado, o qual irá utilizar a porta 16660 do protocolo TCP para a conexão, que usará de criptografia simétrica para proteger as informações que trafegarão do atacante até o master.

Para a comunicação entre as máquinas master e as máquina agentes as quais realmente irão executar o ataque, são utilizados pacotes TCP na porta 65000 e mensagens de ICMP_ECHOREPLY.

O ataque de negação de serviço distribuído em que se utiliza a ferramenta STACHELDRAHT tem-se encontrado uma pequena quantidade de máquinas masters identificadas pelo atacante, e uma grande quantidade de máquinas agentes identificadas pelos atacantes, as quais estarão distribuídas entre as máquinas masters estabelecidas na topologia do ataque. É importante ressaltar que nas máquinas masters estará executando o programa cliente que por sua vez é comumente encontrado com o nome de *mserv*, enquanto que nas máquinas agentes, as quais irão de fato executar o ataque encontra-se em execução os daemons que são encontrado frequentemente sob o nome de *le*f ou *td*.

Na Tabela 2.1 mostra-se uma comparação das comunicações realizadas entre os personagens de uma rede de ataque de negação de serviço distribuída em relação as ferramentas TRIN00, Trible File Network, STACHELDRAHT.

Tabela 2.1 - Relação personagens X ferramentas DDoS.

Comunicação	**TRIN00**	**TFN**	**STACHELDRAHT**
Atacante → Master	1524/27665/TCP	ICMP_ECHOREPLAY	16660/TCP
Master → Agente	27444/UDP	ICMP_ECHOREPLAY	65000/TCP, ICMP_ECHOREPLAY
Agente → Master	31335/UDP	ICMP_ECHOREPLAY	65000/TCP, ICMP_ECHOREPLAY

Com as descrições e detalhamentos das principais ferramentas utilizadas hoje e que estão disponibilizadas na Internet, pode-se notar que um ataque de negação de serviço distribuído pode ser realizado facilmente e que traz para as redes e máquinas vítimas um grande transtorno. Também pode-se ressaltar, que hoje há um grande avanço nas técnicas de melhoramento destas ferramentas o que está despertando a atenção de pesquisadores na área de segurança da informação. Na próxima seção detalha-se sobre as principais técnicas de prevenção quando se tem a ocorrência de um ataque de negação de serviço.

3. TÉCNICAS DE DEFESA E PREVENÇÃO

Ataques de negação de serviço distribuído têm por característica principal negar o serviço de um host através de uma inundação de pacotes TCP, UDP e ICMP, em que o atacante utiliza da técnica de IP Spoofing o que possibilita que para cada pacote o endereço de origem seja forjado.

Nos ataques de negação de serviço distribuído há uma certa dificuldade no seu reconhecimento pelo fato de não possuir um tipo de pacote específico e sim uma variedade de pacotes misturados ao tráfego legítimo da rede, o que torna provavelmente estes pacotes ilegítimos não obtendo resposta, pois a máquina da vítima passa a ter uma baixa velocidade nas respostas de cada requisição, até começar a negar um serviço, ou seja, em um tráfego que sofre o ataque de negação de serviço distribuído possui pacotes que são verdadeiros e pacotes falsos.

Na seção anterior mostrou-se as principais ferramentas utilizadas para implementar ataques de negação de serviço distribuída, tais como TRIN00, TFN, STACHELDRAHT, que são altamente difundidas na Internet. Com a utilização destas ferramentas DDoS fica fácil fazer com que um tráfego ilegítimo em uma rede passa a fazer parte de um tráfego legítimo, utilizando a técnica de IP Spoofing. A utilização destas ferramentas possibilita a inundação de tráfego na rede que é controlada pelo atacante, tornando difícil e na maioria das vezes até impossível de se determinar quais pacotes são legítimos e quais são ilegítimos, além de fazer com que a vítima não tenha alguns serviços ativos, podendo fazer até com que máquinas se reiniciem. Mesmo que se consiga diferenciar pacotes legítimos de pacotes ilegítimos, teria uma dificuldade nos números, pois em ataques de negação de serviço distribuído de acordo com o CERT são utilizados em médias centenas, milhares de agentes a serviço do atacante que estão distribuídos ao longo de toda a Internet [17].

Com isso pode-se dizer que a grande dificuldade em se combater um ataque de negação de serviço distribuído está no uso da técnica de IP Spoofing, na similaridade entre pacotes legítimos e falsos e também levando em consideração a desempenho do sistema [15].

3.1. PRINCÍPIOS DE DEFESA

Em ataques de negação de serviço (DoS) e negação de serviço distribuído (DDoS) tem como fonte principal as vulnerabilidades de alguns protocolos tais como : IP, ICMP, TCP . Estas vulnerabilidades foram descritas com mais detalhes no Capítulo 2 deste trabalho.

Para se defender destes ataques é necessário conhecer com detalhes os princípios do ataque, bem como as vulnerabilidades que eles atingem, para que se possa analisar e elaborar as técnicas de defesa necessária. A seguir será descrita as principais vulnerabilidades e as respectivas técnicas de defesa para ataques de negação de serviço [7].

Defesas das vulnerabilidades do protocolo IP

Para a vulnerabilidade de fragmentação de um pacote, este pode ser dividido em vários blocos, sendo que a técnica de defesa se baseia na diminuição de tempo de armazenamento dos fragmentos. Através desta medida pode-se dizer que o ataque que utiliza o recurso de fragmentação do pacote IP não esteja totalmente impedido de acontecer, mas pode reduzir os danos.

Outra vulnerabilidade existente no protocolo IP é chamada IP Spoofing, que é uma inundação de pacotes para um determinado endereço IP. Para estas vulnerabilidades existem algumas técnicas que têm o objetivo de minimizar os seus efeitos, tais como:

- Filtro de Saída: Sempre que um pacote deseja sair de uma rede, os roteadores de borda devem checar se o endereço de origem destes pacotes são válidos na própria rede ou não, para que possa liberá-los. Este filtro somente irá permitir que pacotes com endereços IP definidos na própria rede trafeguem, caso algum endereço IP de origem de um determinado pacote seja de um endereço diferente do espaço de endereçamento designado pela rede, então este pacote será perdido, não alcançando o seu destino. Em outras palavras, esta técnica consegue proibir que máquinas de uma rede interna não realize spoofing de pacotes IPs, cujo endereço de origem não pertença ao range de IPs da rede interna;

- Filtro de Entrada: Sempre que um pacote IP tiver como destino um endereço IP de uma máquina pertencente a rede interna então os roteadores de bordas e internos devem checar se o endereço IP de origem dos pacotes pertence ao intervalo da

rede, caso pertença, o pacote será entregue ao seu destino, caso contrário o pacote é descartado da rede. Este filtro não permite que as máquinas de uma rede recebam pacotes que tenham origem fora da rede, ou seja, todo pacote antes de ser entregue tem que passar por um roteador de borda, que por sua vez entrega o pacote ao destino;

- Não permitir a transmissão de IP broadcast na rede, pois uma máquina pode requisitar inúmeras conexões de broadcast na rede interna;

- Em uma rede interna podem existir roteadores internos e não somente roteadores de bordas. Estes roteadores intermediários ou de borda também terão que realizar uma checagem nos pacotes que estão chegando a uma interface particular, descartando pacotes da rede que não tenham endereços de IP de origem compatíveis com uma determinada interface presentes nos roteadores intermediários.

Apesar de estas técnicas serem eficientes, isto não indica que a aplicação de algumas delas seja suficiente para prevenir um ataque de negação de serviço que utilize IP Spoofing, mas sim a aplicação de todas estas técnicas tendem a minimizar ao máximo a possibilidade da ocorrência desta vulnerabilidade, principalmente em ISP (Internet Service Provider).

Defesa da Vulnerabilidade do protocolo ICMP

A principal vulnerabilidade do protocolo ICMP na qual um ataque de negação de serviço faz uso, é o ataque chamado Smurf, o qual já foi detalhado anteriormente. Deve-se lembrar que o funcionamento deste ataque se fundamenta no envio de comandos pings para endereços de broadcast de uma determinada rede, em que também utiliza a técnica de IP Spoofing para alterar o endereço de origem de cada pacote enviado, colocando como endereço de origem o endereço da vítima.

Para minimizar ao máximo este ataque, deve-se desabilitar o endereço de broadcast de uma determinada rede interna e tentar prevenir o IP spoofing, utilizando as técnicas mencionadas anteriormente. Uma alternativa para prevenir um ataque de negação de serviço que utiliza um Smurf, poderia ser a inibição total de serviços de Ping, mas isto não pode ser feito pelo fato de afetar a funcionalidade de uma rede, pois as mensagens do protocolo ICMP são utilizadas para reportar um erro na rede, bem como outras informações de rede. Visto que

não se pode desabilitar o serviço de ping de uma rede, então uma alternativa é fazer com que os roteadores presentes nas redes façam, constantemente, uma atualização de suas tabelas de rotas, para realizar a autenticação de cada pacote e também a inserção de uma encriptação nas mensagens ICMP [7].

Defesa da Vulnerabilidade de TCP/IP

A vulnerabilidade envolvendo os protocolos TCP/IP é a presença de SYN Flood na rede, que nada mais é que um flooding de conexões TCP utilizando o processo de 3 way handshake, até que o receptor não consiga responder a pedidos de conexão de um emissor. A figura 2.2 ilustra em detalhes a conexão utilizando protocolo TCP.

De acordo com [7], os passos básicos para reduzir um ataque de negação de serviço que utiliza a vulnerabilidade SYN Flooding são:

- Ajustar os parâmetros do sistema da rede interna, para diminuir o tempo em que o bloco de controle das comunicações abertas na memória, ou seja, diminuir o tempo em que ficará na memória dados no processo *three-way handshake* durante a efetivação de uma conexão TCP. A partir disso, pode-se aumentar o comprimento de uma fila de reserva, a qual irá armazenar as conexões TCP que estarão abertas e ainda não finalizadas. É importante ressaltar que este tempo, deve ser menor até a ponto de que um *host* legítimo que possua um RTT maior, não possa efetuar uma conexão TCP. Além de aumentar a memória para armazenar um número maior de conexões abertas, é importante que fechem todas as portas que não estão sendo utilizadas, pois uma característica de ataques que utilizam desta vulnerabilidade, é fazer uso de portas que não estejam em uso em um sistema computacional;

- Implementar as técnicas para prevenir a vulnerabilidade de IP Spoofing, relacionadas anteriormente;

- Outra técnica utilizada para minimizar ao máximo um ataque do tipo SYN Flood é realizar uma melhoria quando se estabelece uma conexão TCP entre duas máquinas utilizando o processo *three-way handshake*. Em uma conexão normal, a máquina receptora pode armazenar o número de seqüência y para assegurar uma autorização de acesso ou senão quaisquer outros nodos podem enviar ACK com números randômicos e então estabelecer uma conexão não autorizada. Caso o

receptor possa gerar o valor de y antes da chegada da terceira mensagem, então não será permitido armazenar toda a informação de uma conexão, a qual ainda não foi finalizada. Um método utilizado para este cálculo é a utilização de um hash criptográfico da fonte, endereço de destino, portas, e até o valor de x, fazendo uso de uma chave secreta especifica. Com a possibilidade de poder criptografar informações referentes a abertura de uma conexão TCP, tem a possibilidade de proibir o SYN Flooding, fazendo com que somente conexões autorizadas sejam efetuadas e faz com que não sejam armazenadas informações de conexões não finalizadas.

3.2. PREVENÇÃO DE ATAQUES DE NEGAÇÃO DE SERVIÇO

Em se tratando de ataques, sejam eles de qual natureza for, sempre é viável se preocupar em sua prevenção, além também de sua remediação. Ataques de negação de serviço não se preocupará em maior ênfase com os dados, mas sim com os serviços que determinadas máquinas estão oferecendo em uma determinada rede de comunicação de dados.

Para ataques de negação de serviço (DoS) e também para ataques de negação de serviço distribuído (DDoS), a prevenção baseia em evitar que as máquinas designadas atacantes tenham a possibilidade de agirem, e também em aumentar as capacidades dos sistemas com o objetivo de resistir a grandes cargas de tráfego, para que um ataque falhe ao tentar inundar uma máquina vítima, o qual teria como foco principal impedir o acesso a serviços por usuários legítimos [15].

A partir disso, pode-se notar que uma solução definitiva para evitar por completo ataques DoS e DDoS seria obter sistemas e recursos de rede perfeitos, sem falhas. Mas como isto não passa de um ideal a ser alcançado, basta elevar a segurança destes sistemas, tomando medidas plausíveis tais como:

- Fazer com que haja uma melhor programação, elevando assim o nível de segurança nas diversas aplicações realizadas para trabalhar em redes de comunicação, bem como em aplicações de sistemas operacionais;

- Realizar um melhor desenvolvimento e projeto de software, bem como a elaboração de melhores testes para ajudar na escrita de códigos com um mínimo possível de falhas de segurança;

- Melhorar a segurança dos sistemas operacionais envolvidos, o que acarretará em um grande fator para reduzir as probabilidade de um atacante encontrar alguma vulnerabilidade e por fim poder explorá-la;

- Fazer uso de ferramentas automatizadas para verificarem falhas na aplicação, bem como fazer com que os desenvolvedores de softwares de redes e de sistemas operacionais façam uma melhor declaração a respeito da segurança do produto. Isto permitirá que consumidores de tais ferramentas possam escolher as mais seguras.

Em alguns casos de ataques de negação de serviço pode não ser possível prevenir, mas sim somente remediá-lo, pois os ataques que estão ocorrendo na Internet possuem vítimas já bem direcionadas e também devido ao fato de que o custo de prevenção é mais alto possibilitando um melhor e maior investimento na reação contra ataques, pois a reação terá algum custo somente na ocorrência de um ataque.

Ao se optar por um investimento em reação de um ataque de negação de serviço, isto não quer dizer que não haja uma preparação para tais atividades. De maneira diferente da prevenção, para que as definições das atividades de reação sejam executadas, é necessário que este ataque ocorra e seja detectado, para isto é interessante que um Sistema de Detecção de Intrusão esteja presente na rede atacada.

Para ataques DDoS e ataques DoS, pode-se utilizar recursos de prevenção e também de reação, mas em ambos tem objetivos aos quais pretendem atingir, ou seja, a defesa seja de qual forma for tem que ser efetiva, isto é, terá que funcionar. As técnicas de defesa devem ser capazes de identificar e tratar todo e qualquer tipo de ataque DDoS e DoS, os quais, os mais importantes foram descritos no capítulo anterior. Hoje na velocidade da comunicação da Internet, fica difícil fazer com que uma determinada técnica ou ferramenta consiga tratar todos os ataques de DoS e DDoS, pelo fato de que a cada instante novos ataques estejam surgindo com o objetivo de burlar defesas já existentes, o que propicia o grande requerimento de pesquisas e desenvolvimento a cada dia de novas ferramentas de segurança, principalmente para a Internet. O grande objetivo das defesas de ataques DoS e DDoS é fazer com que

serviços de uma máquina ou de uma rede de comunicação de dados estejam ativos para usuários legítimos.

Na próxima seção deste trabalho, apresentam-se mecanismos de defesas para ataques de negação de serviço, as quais terão o objetivo de minimizar ao máximo a ocorrência de um ataque, bem como a apresentação de uma política de segurança a ser tomada em redes de comunicação de dados em relação a ataques deste tipo.

3.3. MECANISMOS DE DEFESA

Quando um ataque de negação de serviço é efetuado, pode-se dizer que se tem duas vítimas distintas que são: os *hosts,* que representa a própria vítima; e também os *hosts* agentes, os quais por sua vez, são acessados de forma remota e sem o usuário legítimo perceber, estes executarão o ataque. Para obter um mecanismo de defesa, deve-se levar em conta a defesa da vítima e também dos agentes presentes em uma rede de ataque de negação de serviço, por sua vez, estes mecanismos de defesas não se distinguem para os dois tipos de vítimas.

Para ataque DoS e DDoS de uma forma geral, fica mais fácil e barato realizar uma remediação efetiva em menor tempo possível em uma rede e, se possível, durante a ocorrência do ataque, para que se tenha a possibilidade de obter a origem do ataque, pois após o ataque realizado ficará muito difícil chegar a sua origem devido ao fato da utilização de IP Spoofing. Um administrador de rede para realizar uma reação rápida e eficaz de um ataque de negação de serviço, deve por sua vez, entender com clareza como a rede está operando e também ter um grande conhecimento e uma certa experiência na utilização de ferramentas escolhidas para recolher e analisar os dados retirados da usa rede de comunicação de dados, pois serão através das ações em conjunto destas ferramentas que pode-se detectar o ataque e preparar a sua reação, isto pelo fato de que o fundamento de um ataque DoS e DDoS é inundar as redes de pacotes.

Sabe-se que para reagir a qualquer ataque é necessário que ele ocorra e que seja detectado. Portanto para ataques DoS e DDoS isto não é diferente. Para ataques DoS e DDoS este processo de detecção pode ser difícil pelo fato de que em determinados momentos estes não são percebíveis pelas ferramentas de detecção chamados de IDS (*Intrusion Detection*

System)[30]. Para realizar uma detecção de forma eficiente, deve-se configurar as ferramentas de detecção de forma a poder diagnosticar e caracterizar o problema, para que se possa reagir, bloqueando o tráfego falso e identificando a origem do tráfego falso(agentes). A seguir é listado algumas anomalias que permitem os IDS detectarem ataques DoS e DDoS[7][10] :

- Excesso de Tráfego: A utilização da largura de banda permitida na rede excede o máximo, fazendo com que ultrapasse o número de acessos esperados;

- Pacotes UDP e ICMP de tamanho acima do normal: Normalmente os pacotes UDP possuem um tamanho de dados dificilmente maiores que 10 bytes (payload), enquanto que as mensagens ICMP não ultrapassem a faixa de 64 e 128 bytes. Pacotes UDP ou mensagens ICMP que ultrapassem estes valores podem ser considerados suspeitos de conterem mensagens de controles destinadas aos agentes. Sabe-se que o conteúdo destes pacotes podem estar cifrados, mas com o endereço de destino verdadeiro, então pode-se localizar os agentes através dos fluxos de mensagens;

- Os tipos de pacotes devem ser analisados: Os dados de pacotes recebidos podem ser estritamente em formato binário e que tenham destino diferente as portas de ftp ou http, portanto devem ser descartados.

Atualmente não existe um mecanismo de defesa completo para prevenir e também remediar ataques de negação de serviço e negação de serviço distribuído, mas de acordo com pesquisadores e administradores de redes que já sofreram estes ataques, alguns métodos podem ser utilizados para minimizar os riscos de ocorrer estes ataques e também que podem ser utilizados para reagir a um ataque DoS e DDoS. Estes métodos são apresentados a seguir:

- Utilizar uma ferramenta de IDS, que tenham a capacidade de identificar e reconhecer ataques em uma rede;

- Aumentar o nível de segurança nas máquinas de uma determinada rede, instalando patches para tratar das vulnerabilidades conhecidas, com o objetivo de dificultar a formação de redes de ataques DDoS;

- Utilizando o backbone da rede, implementar um mecanismo de anti-spoofing para evitar o tráfego de pacotes com endereços forjados dentro da própria rede e também na Internet;

- Fazer com que ocorra a limitação de banda para determinado tráfego de pacotes através de seus roteadores, o que não permitirá o flood de pacotes na rede ou na máquina da vítima;

- Após detectar um ataque na sua rede deve-se desconectar o sistema da rede imediatamente;

- Estabelecer uma política de segurança a ser aplicada na rede;

- Estabelecer um plano de contingência quando ocorrer a detecção de um ataque DDoS ou DoS através do IDS;

- Impedir a instalação de ferramentas que realize o DDoS, sendo importante conhecer as deficiências do sistema operacional;

- Utilizar ferramentas de scanners na rede, para que possa analisar um tráfego suspeito de DoS e DDoS;

- Verificar log's;

- Desativar serviços que não sejam utilizados;

- Filtrar certos tipos de pacotes, que tenham IP forjados.

4. SIMULAÇÃO DO AMBIENTE DE ATAQUE DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO

Neste capítulo serão apresentados os diversos cenários realizados para realizar uma simulação real de um ataque de negação de serviço distribuído. Para esta simulação serão implementadas as ferramentas TRIN00 e STACHELDRAHT, a primeira é a primeira ferramenta de ataque DDoS observada e publicada na Internet, enquanto que a outra é uma das ferramentas mais avançadas atualmente para realizar um ataque DDoS. A descrição detalhada destas ferramentas foram apresentadas no capitulo 2 deste trabalho.

O objetivo desta simulação é realizar o ataque DDoS em um ambiente real, em que se deseja obter as informações dos componentes da rede de ataque antes e durante a realização do ataque, ou seja, o objetivo é capturar e analisar as informações das máquinas pertencentes ao ataque denominadas de atacante, mestres e vítima, bem como relatar as conseqüências do ataque na rede em que esteja realizando o experimento. Um outro objetivo desta simulação é fazer com que a vítima obtenha um software de IDS e verificar o comportamento da máquina vítima, bem como do software IDS no decorrer de um ataque, isto pelo fato do IDS ser um componente fundamental tanto para a reação quanto para a prevenção de um ataque DDoS.

Para que se possa obter as informações necessárias para analisar o ataque DDoS e também para verificar um método de reação, são definidos, em seguida, três cenários básicos.

4.1. CENÁRIO SEM A OCORRÊNCIA DO ATAQUE DDoS

Para este cenário o objetivo é verificar o tráfego da rede definida como rede de ataque de negação de serviço, sem a execução do ataque DDoS. A figura 4.1 ilustra este cenário.

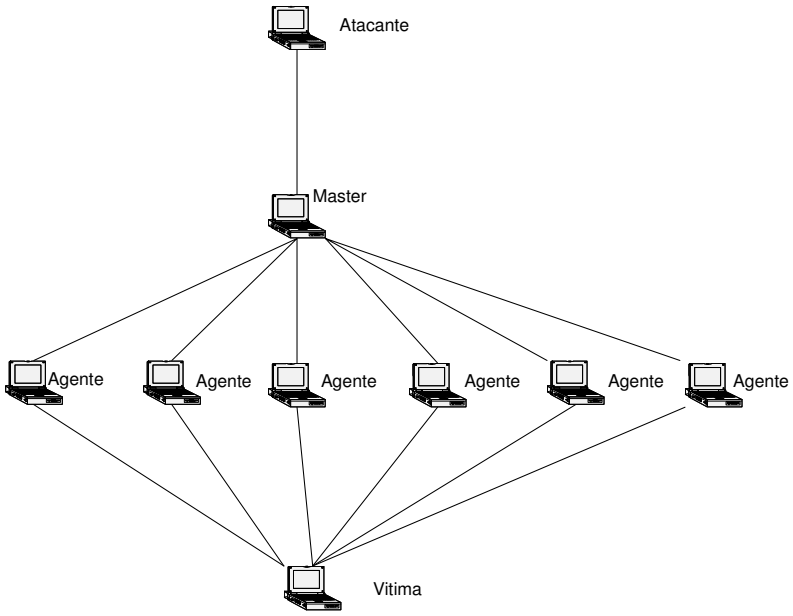

Figura 4.1 - Ambiente de Simulação.

4.2. CENÁRIO COM A OCORRÊNCIA DE ATAQUE DDoS

Para este cenário o objetivo é verificar o tráfego da rede definida como rede de ataque de negação de serviço, com a execução do ataque DDoS utilizando, a ferramenta TRIN00 e STACHELDRAHT. Neste cenário ilustrado pela figura 4.2, captura-se informações do master, dos agentes e da vítima. A rota de vermelho representa a rota de ataque do ataque DDoS.

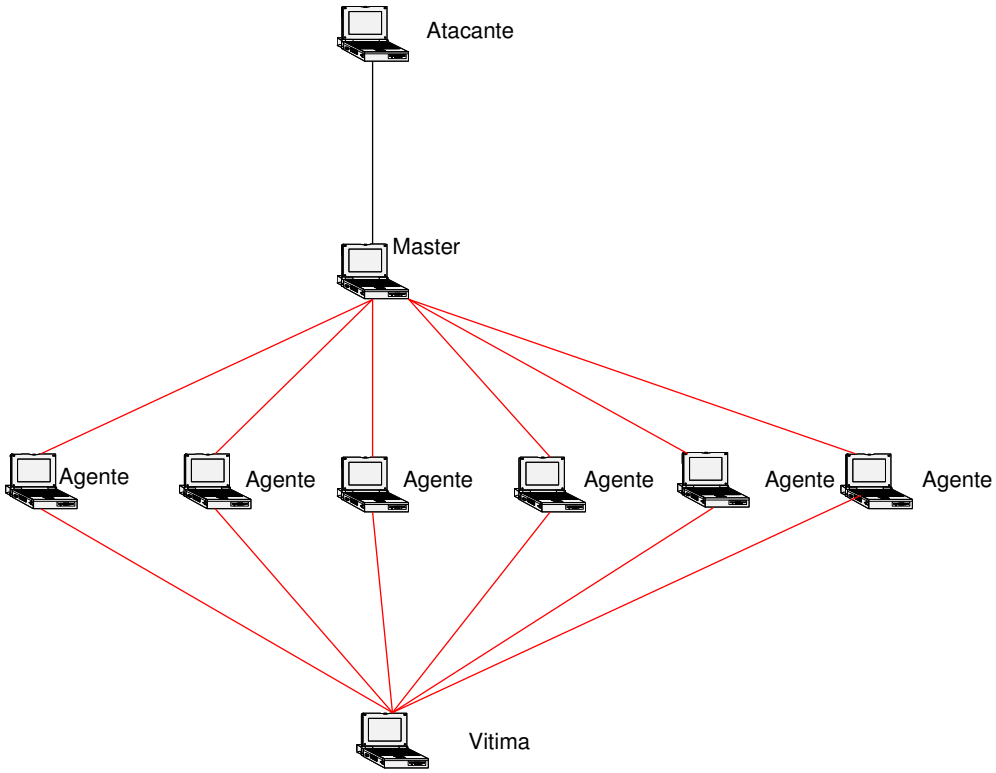

Figura 4.2 - Ambiente com Execução do Ataque.

4.3. CENÁRIO COM A PRESENÇA DE IDS

Para este cenário o objetivo é verificar o tráfego da rede definida como rede de ataque de negação de serviço, com a execução do ataque DDoS utilizando a ferramenta TRIN00 e STACHELDRAHT e com a presença de um software de IDS na máquina da vítima. Neste cenário, deve-se capturar informações do master, dos agentes e da vítima. A figura 4.3 ilustra este cenário.

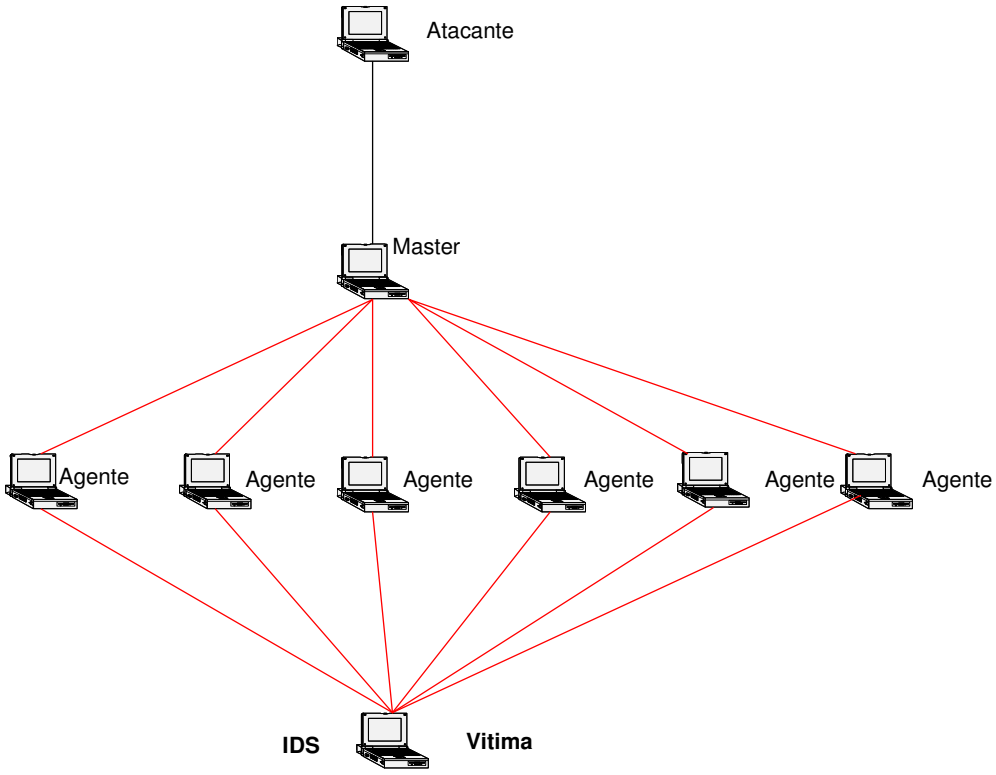

Figura 4.3 - Ambiente com IDS.

4.4. DESCRIÇÃO DA SIMULAÇÃO

Para a simulação das ferramentas de ataques DDoS TRIN00 e STACHELDRAHT, apresentam-se os passos para instalação das respectivas ferramentas nas maquinas atacantes, master, agentes também chamadas de zumbis e na máquina vítima. Para cada um dos componentes pertencentes a rede de ataque DDoS, descrevem-se os passos para que se possa inicializar o ataque. Após, a inicialização do ataque, será capturado o tráfego na rede nas máquinas pertencentes ao ataque. Para a realização tanto do ataque TRIN00 quanto STACHELDRAHT a simulação corresponde em fazer com que seis máquinas agentes estejam ligadas em um master e estas por sua vez, ataquem ao mesmo tempo uma máquina vítima.

4.5. ATAQUE TRIN00

Todos os ataques de negação de serviço distribuído estão publicados na Internet através da descrição de seus projetos [11][12][13]. Além dos projetos, também são publicados na Internet todos os códigos fontes pertencentes a determinadas ferramentas de ataque DDoS.

4.5.1. Instalação

Primeiramente para se instalar a ferramenta de DDoS TRIN00, deve-se fazer o download de seu pacote na Internet, tendo como fonte principal o site http://packetstormsecurity.org/ [32]. Neste pacote, têm-se dois módulos distintos chamados de master e daemon, que representa respectivamente os módulos da ferramenta a serem instalados nas máquinas mestres e nas máquinas agentes.

ATACANTE

Na máquina designada como atacante, deve-se ter instalado uma ferramenta capaz de realizar uma conexão remota com as máquinas mestras para que possa dar início ao ataque, a ferramenta utilizada no experimento é o Telnet, a qual é de fácil manuseio e que já se encontra nos sistemas operacionais das máquinas.

A partir desta ferramenta o atacante poderá se conectar a máquina master através da porta TCP/27665, que é a porta a ser aberta e utilizada na comunicação entre atacante e master. Para verificar esta comunicação, pode-se utilizar qualquer software analizador de pacotes de rede, como o Ethereal, Wireshark.

MASTER

Para a máquina designada como mestre na rede de ataque DDoS, deve-se instalar uma ferramenta capaz de capturar os tráfegos da rede para posterior análise. No master de um ataque DDoS será instalado o módulo master presente no pacote da ferramenta TRIN00, que fará com que esta máquina designada como master tenha a possibilidade de escutar os seus respectivos agentes, bem como transmitir uma tarefa para os agentes.

A instalação deste módulo será através da ferramenta make, a qual também já se encontra nos sistemas operacionais das máquinas envolvidas no ataque. Após a instalação é gerado um executável chamado de master, o qual será executado através do comando

./master. Para que o módulo master seja executado na máquina master é necessário a informação de uma senha, que é **g0rave**, como mostrado na figura 4.4.

```
debian1:/usr/src/master# ./master
?? gOrave
trinoo v1.07d2+f3+c [Sep 27 2006:19:39:37]
debian1:/usr/src/master# _
```

Figura 4.4 – Execução do Master – TRIN00.

No momento em que o módulo master é executado na máquina master, pode-se verificar o número do processo correspondente a ele, bem como as portas abertas para comunicação com os agentes e com a máquina designada como atacante, portas estas que são : 27665/tcp (porta que o atacante se conectará via telnet) e 31335/udp (porta que o daemon utilizará para comunicar com o master). A figura 4.5 e 4.6 mostra os snapshots destas ações.

```
debian1:/usr/src/master# ps awx | grep master
 2138 tty1     S      0:00 ./master
debian1:/usr/src/master# _
```

Figura 4.5 – Processo no Master – TRIN00.

```
debian1:/usr/src/master# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:27665           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:31335           0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  4      [ ]         DGRAM                    4038     /dev/log
unix  2      [ ]         DGRAM                    4371
unix  2      [ ]         DGRAM                    4050
debian1:/usr/src/master# _
```

Figura 4.6 – Portas Abertas no Master – TRIN00.

A partir deste momento a máquina master está pronta para receber o contato das máquinas agentes, em que os agentes irão informar que estão ativos e esperando uma ação, ou seja, estarão a espera de um comando do master para realizar o ataque.

AGENTE

Para as máquinas designadas como agentes de uma rede de ataque DDoS, também deve ser instalado uma ferramenta capaz de capturar os dados da rede, para que se possa verificar o tráfego da rede em direção a vítima. Nestas máquinas são instalados o módulo daemon presente no pacote da ferramenta TRIN00, que será responsável por habilitar a

comunicação dos agentes com os masters e também com a vítima, pois quem realizará de fato o ataque DDoS serão as máquinas agentes.

A instalação deste módulo também será através da ferramenta make, a qual já está presente na maioria dos sistemas operacionais. Após a sua instalação é gerado um executável chamado de ns, o qual deverá ser executado utilizando o comando ./ns. Antes de executar o módulo daemon é necessário editar o arquivo ns.c e informar o endereço IP das máquinas masters, presentes na rede de ataque DdoS, como mostrado na figura 4.7. Nesta figura mostra que a máquina com o endereço IP 172.16.198.128 é um agente dentro de uma rede de ataque DdoS.

```
/* #define PROCNAME "httpd" */
char *master[] = {
  "172.16.198.128",
  NULL
};
```

Figura 4.7 – Definição de Master no Daemon – TRIN00.

No momento em que o módulo daemon é executado, pode-se observar que é criado um processo designado para o daemon e também pode-se verificar a abertura das portas de comunicação com as máquinas masters, portas estas que são: 27444/udp (porta pela qual o master se comunicará com o agente) e 1024/udp (porta que o agente enviará os pacotes para o master). As figuras 4.8 e 4.9 mostram os snapshots destas ações.

```
debian2:/usr/src/daemon# ps awx | grep daemon
 2140 tty1     S      0:00 ./daemon
debian2:/usr/src/daemon#
```

Figura 4.8 – Processo no Daemon – TRIN00.

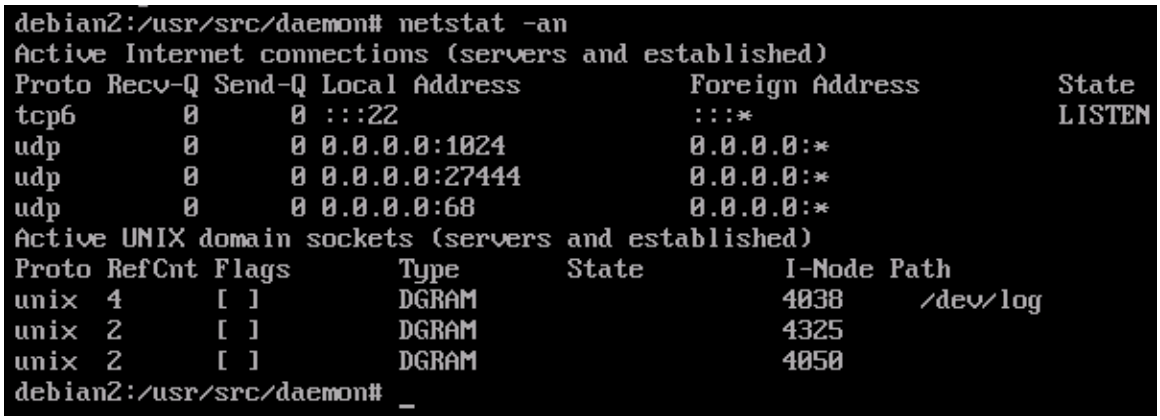

Figura 4.9 – Portas Abertas no Daemon – TRIN00.

Assim, o agente já está pronto, esperando que o master envie algum comando para que este proceda com o ataque a vítima.

VÍTIMA

Na máquina que será a vítima, deve-se instalar uma ferramenta capaz de captar o tráfego da rede para o segundo cenário, enquanto que para o terceiro cenário, deve-se instalar também um software IDS com o objetivo de detectar a presença de um ataque DDoS.

4.5.2. Ataque

Antes de descrever a realização do ataque, faz se necessário a apresentação das características das máquinas utilizadas para os cenários descritos anteriormente. Todas as máquinas que compõe a rede de ataque de negação de serviço distribuído são compostas de Sistema Operacional LINUX (distribuição Debian / Sarge) com instalação mínima, devido a melhor facilidade em se instalar as ferramentas necessárias e também pelo fato de se obter melhores resultados. A Tabela 4.1 descreve os endereços IPs de todas as máquinas do cenário.

Tabela 4.1 – Mapeamento de Endereço IP – TRIN00.

	Atacante	**Master**	**Agente**	**Vítima**
Nome do Host	linux0	linux1	Linux2 até Linux 8	Linux9
IP do Host	192.168.67.106	192.168.67.101	192.168.67.105. até 192.168.67.111	192.168.67.52

A realização da simulação do ataque de negação de serviço distribuído utilizando a ferramenta DDoS TRIN00 seguiu os passos :

1 Verificou-se a execução dos processos na máquina master(linux1) e nas máquinas agentes(linux2 até linux8), que são respectivamente ./master e ./daemon. Também verifica as portas que estes processos abrem nas máquinas que são respectivamente: 27665/tcp e 31335/udp em linux1 e as portas 27444/udp e 1024/tcp em linux2 até linux8.

2 Com o master e o agente no ar, deve-se conectar a partir da máquina do atacante (linux0) na máquina master que esta a rodar o processo ./master (linux1), através da porta 27665/tcp. Para isso utiliza-se a ferramenta Telnet, da seguinte forma:

```
# telnet 192.168.67. 27665
```

3 No momento em que consegue conectar a máquina atacante na máquina master é necessário inserir uma senha para executar o executável do módulo master que está instalado na máquina master. Por padrão esta senha é **betaalmostdone**. Caso esta senha esteja errada a conexão entre as duas máquinas será fechada, enquanto que se a senha estiver correta será aberta a conexão e aparecerá um prompt (trinoo>) para que se possa executar alguns comandos. A seguir será apresentado um snapshot com a senha errada e outro com a correta:

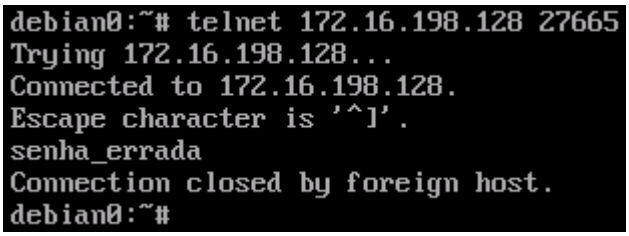

Figura 4.10 – Negação de Conexão - TRIN00.

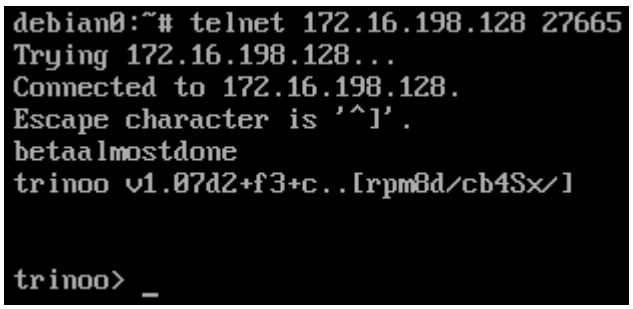

Figura 4.11 – Aceitação de Conexão - TRIN00.

4 Neste momento o cenário encontra-se pronto para a realização do ataque DDoS através da ferramenta TRIN00, pois as máquinas agentes estão prontas a receber uma ordem para atacar, onde deve-se lembrar que assim que o agente for ligado, este envia um pacote com *HELLO* para o master, fazendo com que este saiba que o agente está ativo.

5 Agora basta executar o ataque através dos comandos admitidos pelo módulo master, os quais são descritos a seguir [11]:

a) die – Shut down no processo do master.

b) quit – Log off do master (fechar a conexão).

c) mtimer N - Configura o tempo DoS para N segundos. Esse será o tempo que os agentes ficarão atacando a vítima. Pode ser entre 1 e 1999 segundos, o padrão é 300.

d) mdie password – Desabilita todos os Bcast *hosts* (agentes). O password padrão é **killme**. O comando "d1e 144adsl" é enviado para cada Bcast host.

e) mping – Envia o comando "png 144adsl" para cada Bcast host ativo. Todos os Bcast *hosts* responderá (PONG).

f) **info** – Mostra a versão e algumas informações da compilação.

g) **msize S** – Configura o tamanho dos pacotes a serem enviados durante o ataque DoS.

h) **nslookup host** – Faz uma pesquisa no servidor de nome pelo host.

i) **killdead** – Faz com que todos os Bcast *hosts* (agentes) enviem novamente o pacote com *HELLO* para que o master faça uma nova lista de Bcast *hosts* ativos.

j) **bcast** – Lista todos ativos Bcast *hosts* (agentes).

k) **mstop** – Para o ataque DoS que está sendo executado.

l) **dos IP** – ataque DoS no endereço IP especificado. O comando "aaa 144adsl IP" é enviado para cada Bcast host (agentes).

4.5.3. Tráfego

Será apresentado a seguir, as telas de capturas encontradas na execução do ataque DDoS utilizando a ferramenta TRIN00. Pode-se observar que no instante em que executa um comando de ataque, que nesta simulação é DOS 192.168.67.52, ocorre uma inundação de pacotes TCP nesta máquina. Deve-se salientar que nesta ferramenta, os endereços IPs de origens dos pacotes correspondem aos endereços de origem das máquinas agentes.

Captura de tráfego na máquina agente

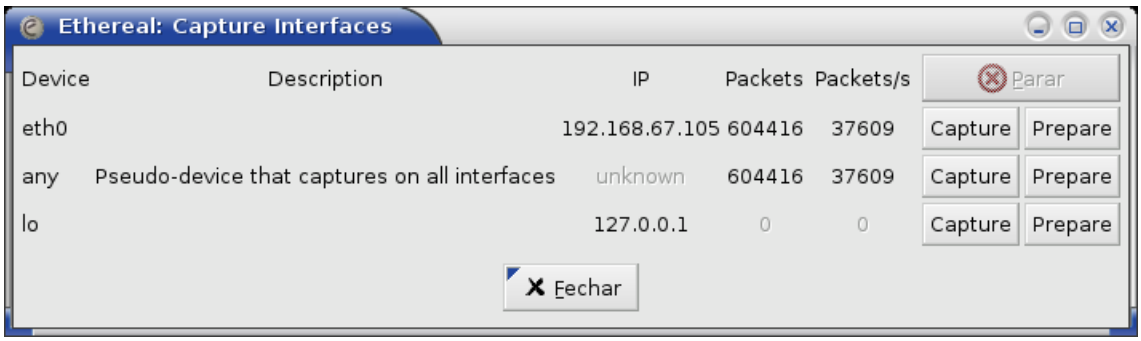

Figura 4.12 – Captura da Interface do Agente – TRIN00.

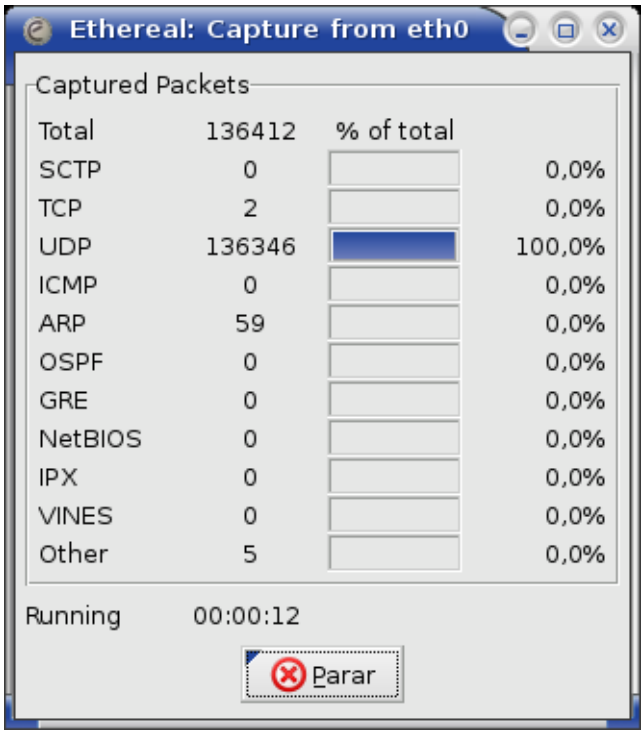

Figura 4.13 – Quantidade de Pacotes Recebidos no Agente – TRIN00.

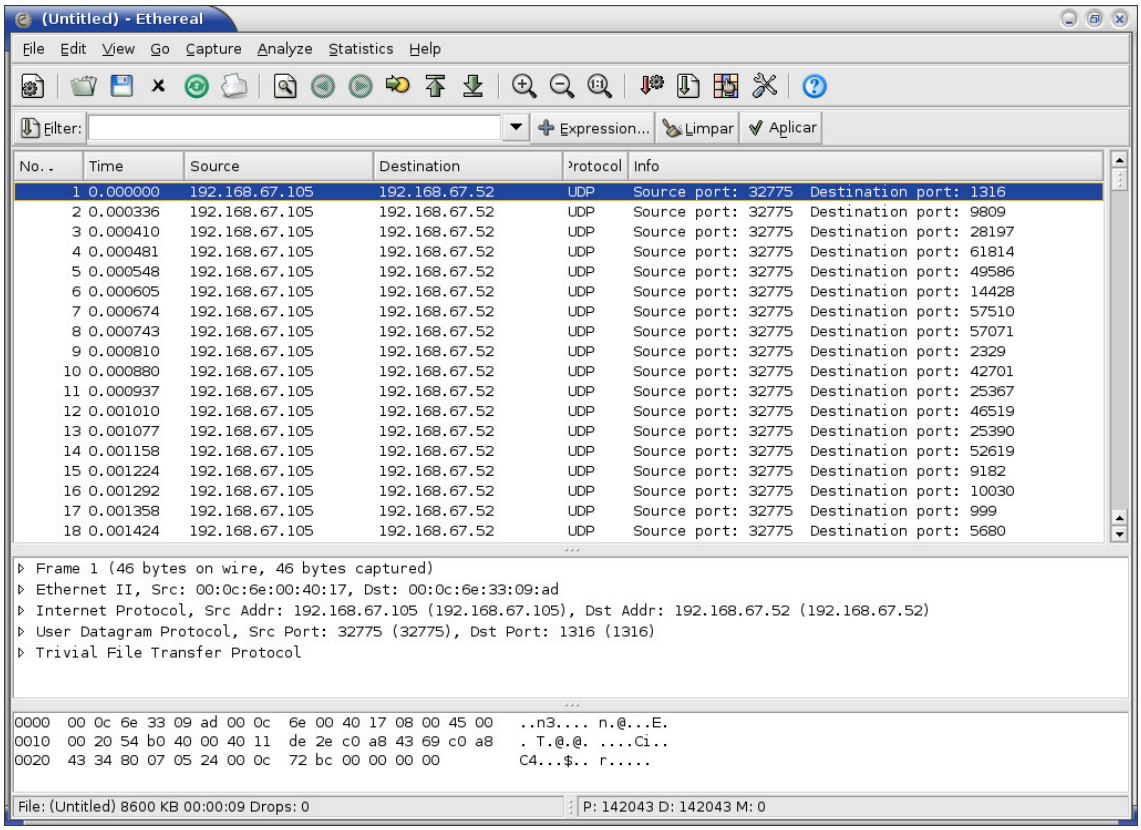

Figura 4.14 – Tráfego no Agente – TRIN00.

Captura de tráfego na máquina vítima

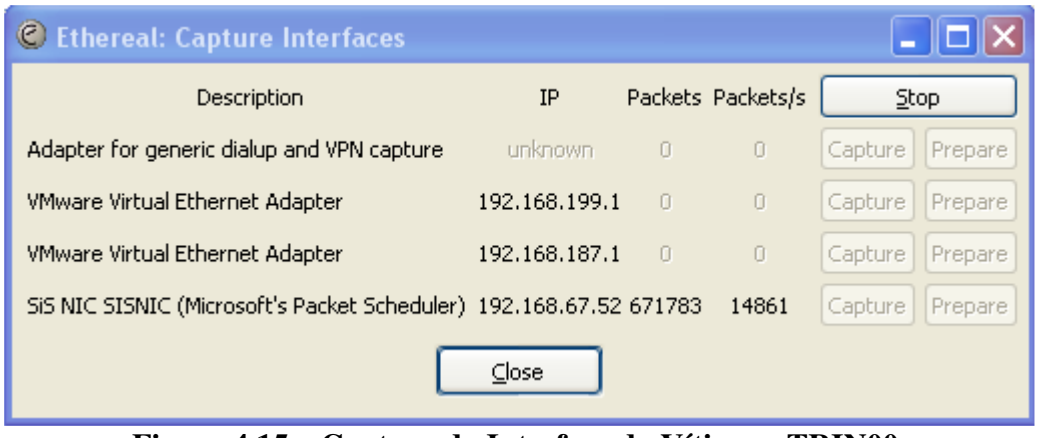

Figura 4.15 – Captura da Interface da Vítima – TRIN00.

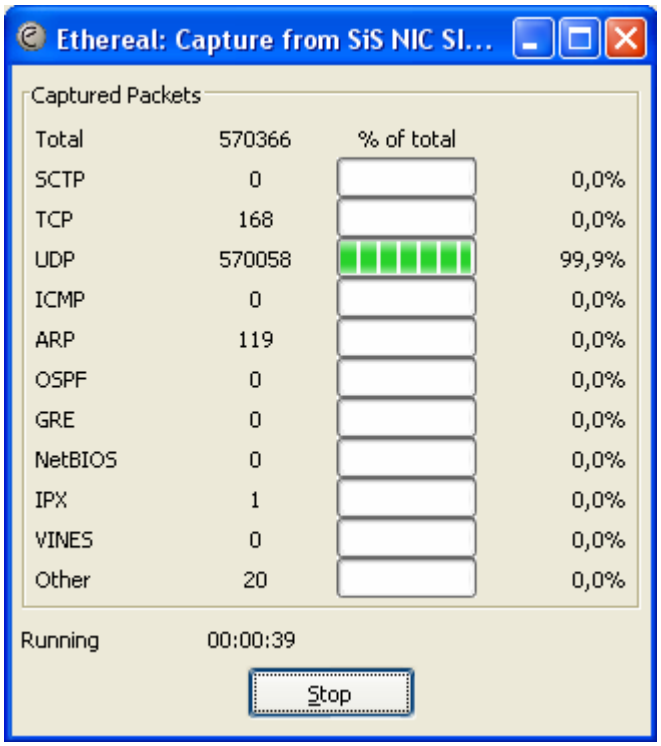

Figura 4.16 – Quantidade de Pacotes Recebidos na Vítima – TRIN00.

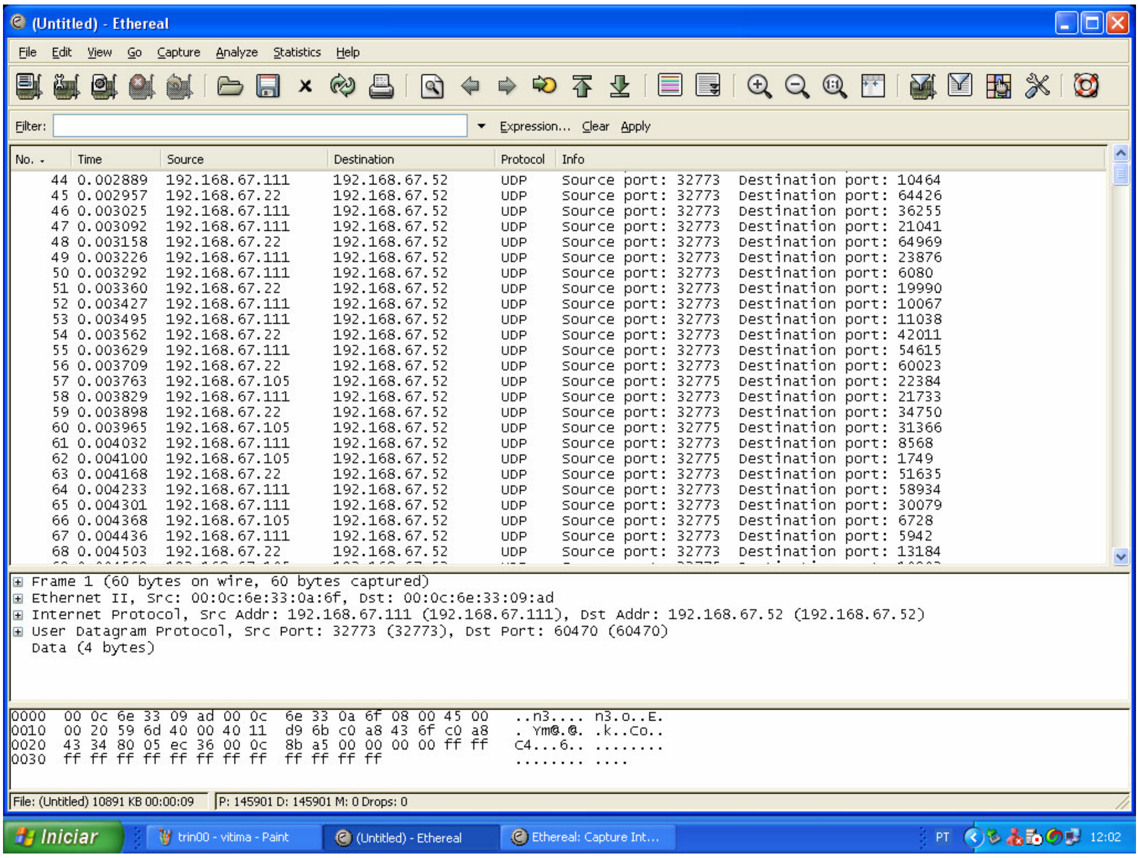

Figura 4.17 – Tráfego na Vítima – TRIN00.

Captura do Snort[31] e informações de arquivo LOG

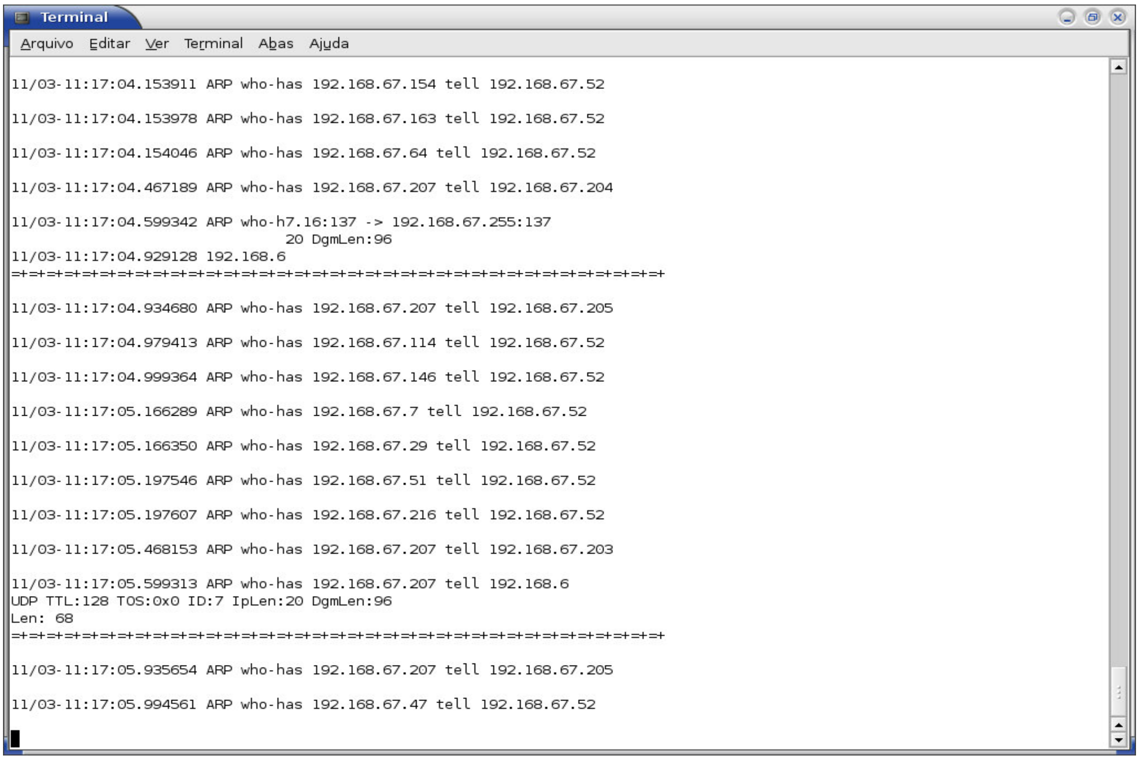

Figura 4. 18 – Captura do Snort – TRIN00.

Arquivo de Log do Snort

[**] [122:18:0] (portscan) UDP Decoy Portscan
[**]10/27-14:46:54.958640 192.168.67.205 -> 192.168.67.101
PROTO255 TTL:0 TOS:0xC0 ID:38216 IpLen:20 DgmLen:163
[**] [122:18:0] (portscan) UDP Decoy Portscan [**]
10/27-14:48:11.427443 192.168.67.56 -> 192.168.67.101
PROTO255 TTL:0 TOS:0xC0 ID:57250 IpLen:20 DgmLen:167
[**]

4.6. ATAQUE STACHELDRAHT

Uma outra ferramenta que possibilita a execução de um ataque de negação de serviço distribuído é o STACHELDRAHT, que também se encontra disponível no site http://packetstormsecurity.nl/. Para a ferramenta STACHELDRAHT, encontram-se publicados a sua descrição e o seu detalhamento, bem como os códigos fontes utilizados na sua implementação.

4.6.1. Instalação

Para realizar a instalação desta ferramenta é necessário realizar o download do pacote correspondente normalmente chamado de stachel, que pode ser encontrado na Internet no endereço http://packetstormsecurity.nl/ [13]. Da mesma forma que a ferramenta TRIN00, tem-se um módulo que será instalado nas máquinas designadas como atacantes, que são chamados de client, enquanto que as máquinas designadas como master são chamadas de handler e as máquinas agentes são chamadas de agent. Para os handler e os agentes são instalados os módulos client dentro de telnetc e td dentro de leaf.

ATACANTE

Na máquina designada como atacante deve-se ter instalado uma ferramenta capaz de realizar uma conexão remota com as máquinas mestras para que possa dar início ao ataque. A ferramenta STACHELDRAHT possibilita que uma máquina atacante controle uma ou várias máquinas handlers através do módulo client encriptado, o qual realiza esta comunicação utilizando a porta 16660/tcp.

A partir desta ferramenta, o atacante poderá conectar-se à máquina master ou handler na porta 16660/tcp, que é a porta a ser aberta e utilizada na comunicação entre atacante e master. Para verificar esta comunicação, pode-se utilizar qualquer software analisador de pacotes de rede, como o Ethereal, Wireshark

MASTER OU HANDLER

Para a máquina designada como mestre na rede de ataque DDoS, deve-se instalar uma ferramenta capaz de capturar os tráfegos da rede para posterior análise. No master de um ataque DDoS será instalado o módulo master presente no pacote da ferramenta STACHELDRAHT, que fará com que esta máquina tenha a possibilidade de escutar os seus respectivos agentes, bem como transmitir uma tarefa para os agentes.

A instalação deste módulo será através da ferramenta make, a qual já encontra-se nos sistemas operacionais das máquinas envolvidas no ataque. Após a instalação, é gerado um executável chamado de mserv, o qual será executado através do comando ./mserv, que será responsável pela comunicação entre o master e os agentes. Também no master é gerado um executável chamado de client, o qual irá se comunicar com o serv, para entrar na ferramenta STACHELDRAHT, que será executada utilizando o comando ./client. Para que o módulo master seja executado na máquina master, é necessário a informação de uma senha, que é **sicken**,como mostrado a seguir:

```
# ./client 192.168.0.1
[*] stacheldraht [*]
(c) in 1999 by ...
trying to connect...
connection established.
-----------------------------------
enter the passphrase : sicken
-----------------------------------
entering interactive session.
*****************************
welcome to stacheldraht
*****************************
```

type .help if you are lame

stacheldraht(status: a!1 d!0)>

No momento em que as aplicações mserv e client são executadas na máquina master, pode-se verificar os processos correspondentes a cada aplicação, bem como a porta aberta para comunicação com os agentes e com a máquina designada como atacante, porta esta que é : 65000/tcp. A figura 4.5 e 4.6 mostra as telas referentes à execução do mserv e do client na máquina master.

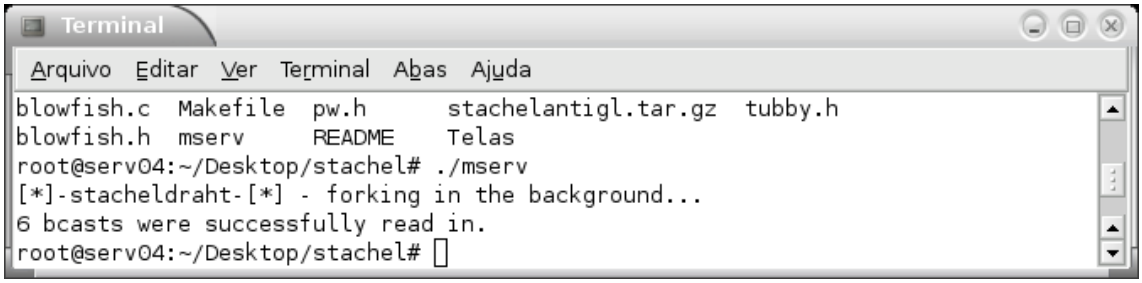

Figura 4.19 – Execução do Mserv – STACHELDRAHT.

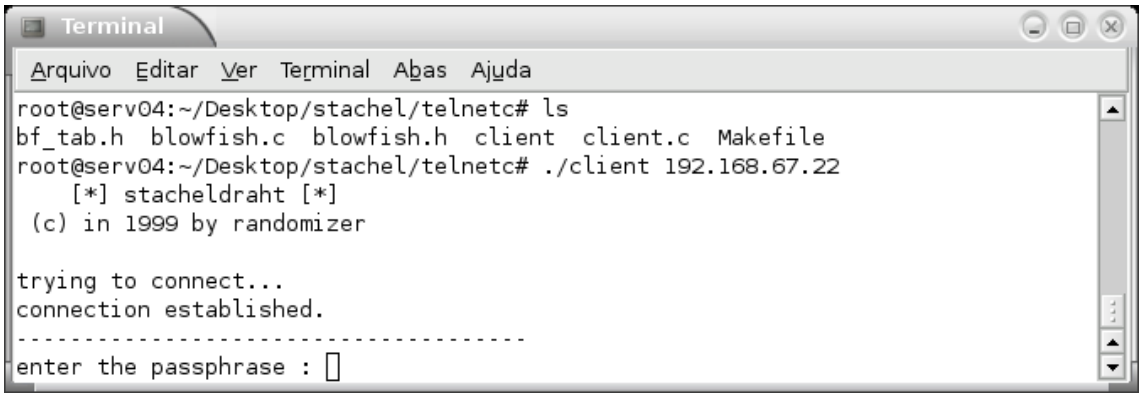

Figura 4.20 – Execução do Client – STACHELDRAHT.

A partir deste momento a máquina master está pronta para receber o contato das máquinas agentes, sendo que os agentes irão informar que estão ativos e esperando uma ação, ou seja, estarão a espera de um comando do master para realizar o ataque.

AGENTE

Para as máquinas designadas como agentes de uma rede de ataque DDoS, deve ser instalado uma ferramenta capaz de capturar os dados da rede, para que se possa verificar o tráfego da rede em direção a vítima. Nestas máquinas são instalados os módulos daemon presente no pacote da ferramenta STACHELDRAHT, chamado de módulo leaf, que será responsável por habilitar a comunicação dos agentes com os masters e com a vítima, pois quem realizará de fato o ataque DDoS serão as máquinas agentes.

A instalação deste módulo será através da ferramenta make, que já está presente na maioria dos sistemas operacionais. Após a sua instalação é gerado um executável chamado de td, que deverá ser executado utilizando o comando ./td.

No momento em que o módulo leaf é executado, pode-se observar que é criado um processo designado para o leaf e pode-se verificar a abertura da porta de comunicação com as máquinas masters, porta esta que é : 65000/tcp. A figura 4.21 mostra a execução da aplicação no master, a qual é necessário informar o endereço IP da máquina master.

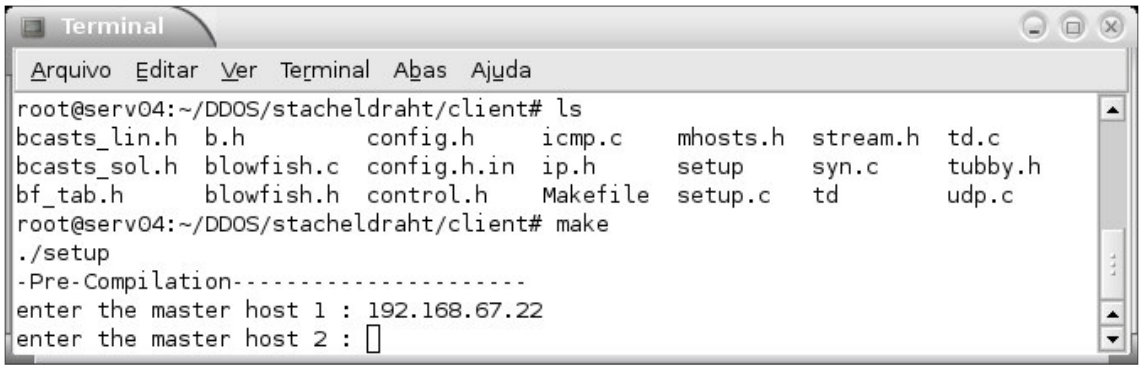

Figura 4.21 – Execução no Agente – STACHELDRAHT.

Assim, o agente já está pronto, esperando que o master envie algum comando para que este proceda com o ataque à vítima.

VÍTIMA

Na máquina que será a vítima, deve-se instalar uma ferramenta capaz de captar o tráfego da rede para o segundo cenário, enquanto que para o terceiro cenário, deve-se instalar um software IDS com o objetivo de detectar a presença de um ataque DDoS. Deve-se lembrar que a ferramenta STACHELDRAHT, bem como o TRIN00 utiliza, endereços IPs de origens forjados e diversas portas que não estão em uso.

4.6.2. Ataque

Antes de descrever a realização do ataque, faz se necessário a apresentação das características das máquinas utilizadas para os cenários descritos anteriormente. Todas as máquinas que compõe a rede de ataque de negação de serviço distribuído são compostas de Sistema Operacional LINUX (distribuição Debian / Sarge) com instalação mínima. A tabela 4.2 a seguir descreve os endereços IPs de todas as máquinas do cenário.

Tabela 4.2 – Mapeamento de Endereço IP – STACHELDRAHT.

	Atacante	**Master**	**Agente**	**Vítima**
Nome do Host	linux0	linux1	Linux2 até Linux 8	Linux9
IP do Host	192.168.67.106	192.168.67.106	192.168.67.105 até 192.168.67.111	192.168.67.52

A realização da simulação do ataque de negação de serviço distribuído utilizando a ferramenta DDoS STACHELDRAHT seguiu os passos :

1 Verifica-se a execução dos processos na máquina master (linux1) e nas máquinas agentes (linux2 até linux8), que são respectivamente ./mserv e ./client no master e ./td nos agentes. Também se verifica a porta que estes módulos abrem nas máquinas que são respectivamente: 16660/tcp e 65000/tcp em linux1 e as portas 65000/tcp em linux2 até linux8;

2 Com o master e o agente no ar, deve-se conectar a partir da máquina do atacante (linux0) na máquina master que está a rodar o processo ./master (linux1), através de uma ferramenta de conexão remota como, por exemplo, o Telnet;

3 No momento em que consegue conectar a máquina atacante na máquina master, é necessário inserir uma senha para executar o executável client do módulo master que esta instalado na máquina master. Por padrão, esta senha é **stick.** Caso esta senha esteja errada, a conexão entre as duas máquinas será fechada, enquanto que, se a senha estiver correta, será aberta a conexão e aparecerá um prompt stacheldraht(status: a!1 d!0)> para que se

possa executar alguns comandos. Os valores de a! e d! representam as quantidades de máquinas agentes ligadas a esta máquina master;

4 Neste momento o cenário encontra-se pronto para a realização do ataque DDoS através da ferramenta STACHELDRAHT, pois as máquinas agentes estão prontas para receber uma ordem para atacar, onde deve-se lembrar que assim que o agente for ligado, este envia um pacote com *HELLO* para o master, fazendo com que este saiba que o agente está ativo;

5 Agora basta executar o ataque através dos comandos admitidos pelo módulo master, os quais são descritos abaixo[13]:

a) distro user server :

Ensina o agente para instalar e gerar uma cópia nova de si mesmo, usando o rcp no servidor de sistema, utilizando o usuário de conta (por exemplo, " rcp ttymon " de user@server:linux.bin)

b) help

Listagem de comandos suportados pela ferramenta Stacheldraht

c) .killall

Eliminação de agents ativos.

d) .madd ip1[:ip2[:ipN]]

Adiciona endereços IPs como máquinas vítimas.

e) .mdie

Envia dados de requisições para todos os agentes.

f) .mdos

Inicia um ataque DoS.

g) .micmp ip1[:ip2[:ipN]]

Inicia um ataque de ICMP Flooding para os endereços IPs especificados

h) .mlist

Listagem dos endereços IPs que estão sofrendo o ataque no momento.

i) .mping

Realiza um ping para todos os agents, afim de verificar se estão ativos.

j) .msadd

Adiciona um novo master na lista de master ativos.

k) .msort

Mostra a porcentagem de agents ativos e inativos.Isto é feito através do envio de pings para os agentes.

l) .mstop ip1[:ip2[:ipN]]

Parar o ataque DDoS a uma determinada vítima, especificada pelo seu endereço IP.

m) .mstop all

Parar o ataque DDoS a todas as vítimas.

n) .msrem

Retira um master da lista de ativos

o) .msyn ip1[:ip2[:ipN]]

Inicia um ataque SYN flood para uma vítima especificada pelo endereço IP.

p) .mtimer seconds

Indica o tempo de duração do ataque DDoS em segundos.

q) .mudp ip1[:ip2[:ipN]]

Inicia um ataque UDP flood para uma vítima especificada pelo endereço IP. Representa uma emulação do ataque DDoS Trin00.

r) .setisize

Indica o tamanho de pacotes ICMP a serem enviados para a vítima

s) .setusize

Indica o tamanho de pacotes UDP a serem enviados para a vítima

t) .showalive

Mostra todos os agentes ativos.

u) .showdead

Mostra todos os agentes inativos.

v) .sprange lowport-highport

Define o intervalo de portas para o SYN Flooding(padrão : 0 a 140).

4.6.3. Tráfego

Será apresentado a seguir as telas de capturas encontradas na execução do ataque DDoS utilizando a ferramenta STACHELDRAHT. Pode-se observar que no instante em que executa um comando de ataque, que nesta simulação é .msyn 192.168.67.52, ocorre uma inundação de pacotes TCP nesta máquina. Deve-se salientar que os endereços IPs de origens dos pacotes não correspondem aos endereços de origem das máquinas agentes.

Captura de tráfego no agente

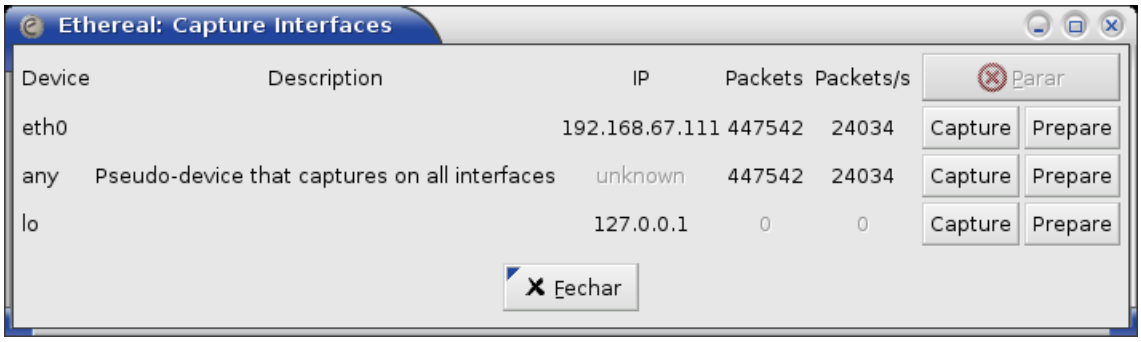

Figura 4.22 – Captura Interface do Agente – STACHELDRAHT.

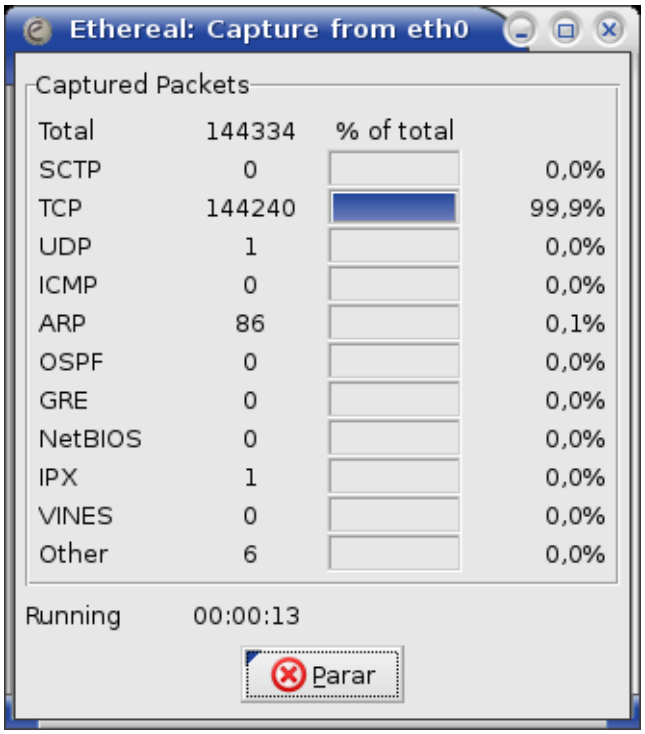

Figura 4.23 – Quantidade de Pacotes Capturados no Agente – STACHELDRAHT.

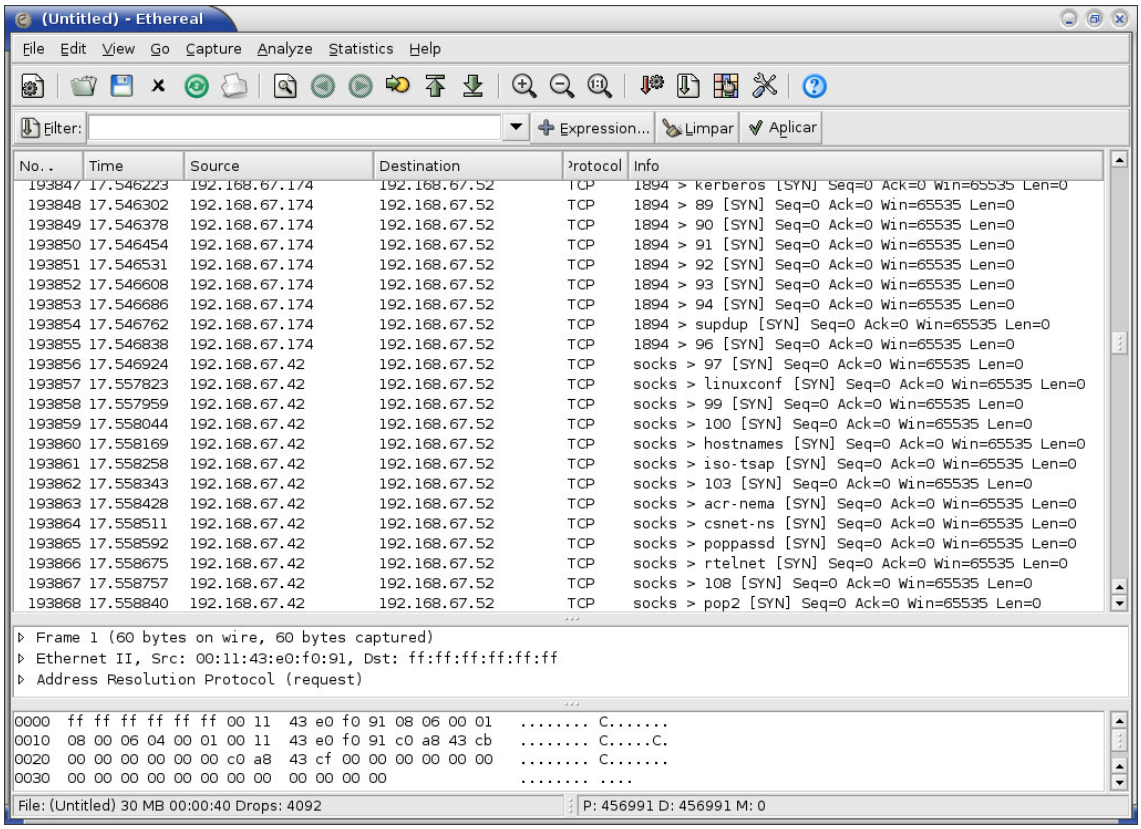

Figura 4.24 – Tráfego no Agente – STACHELDRAHT.

Captura de tráfego na vítima

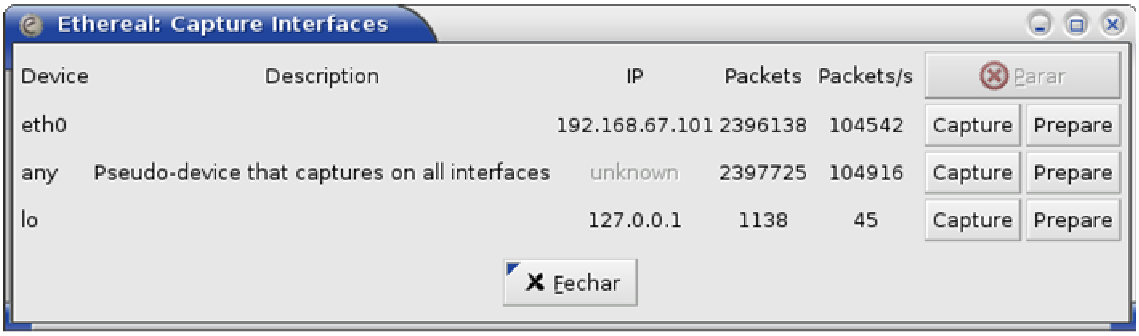

Figura 4.25 – Captura Interface da Vítima – STACHELDRAHT.

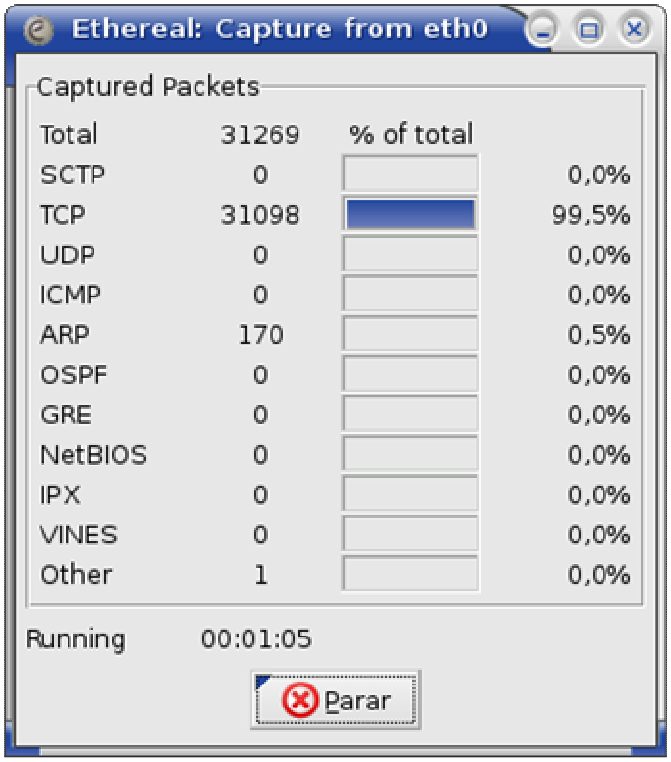

Figura 4.26 – Quantidade de Pacotes Capturados na Vítima – STACHELDRAHT.

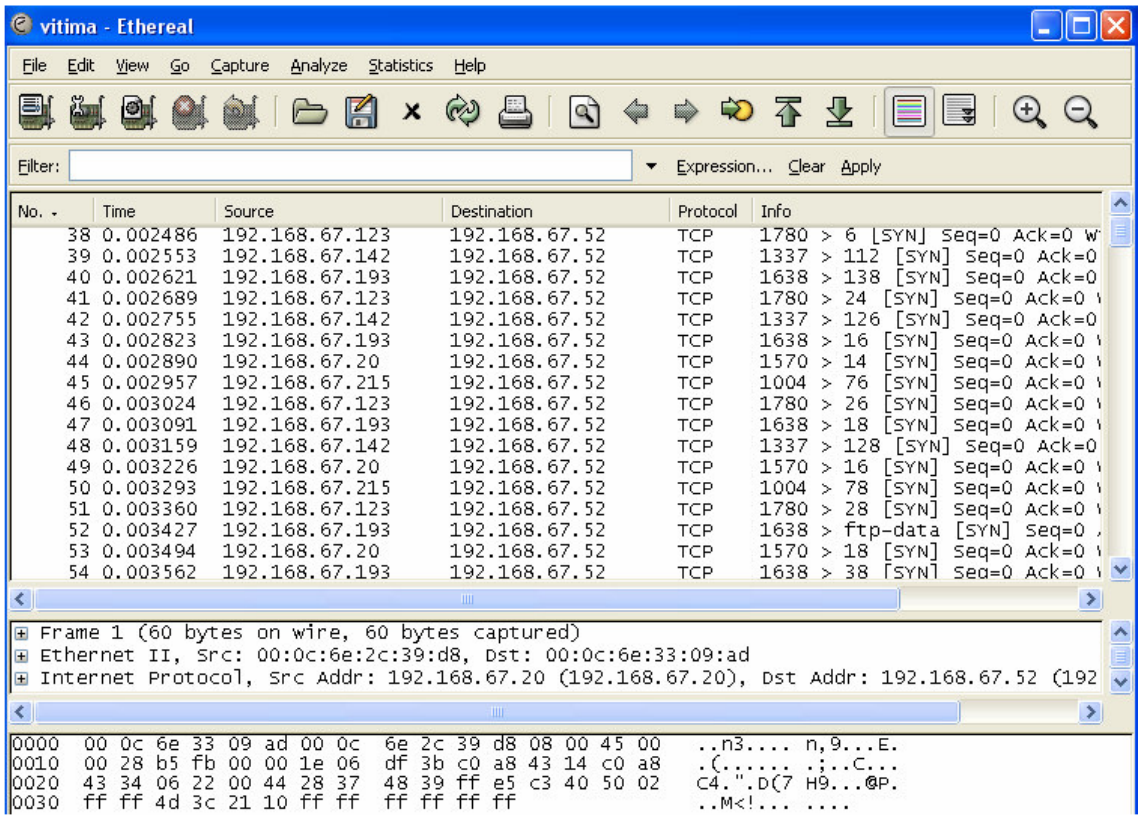

Figura 4.27 – Tráfego na Vítima – STACHELDRAHT.

Captura do Snort e informações de arquivo LOG

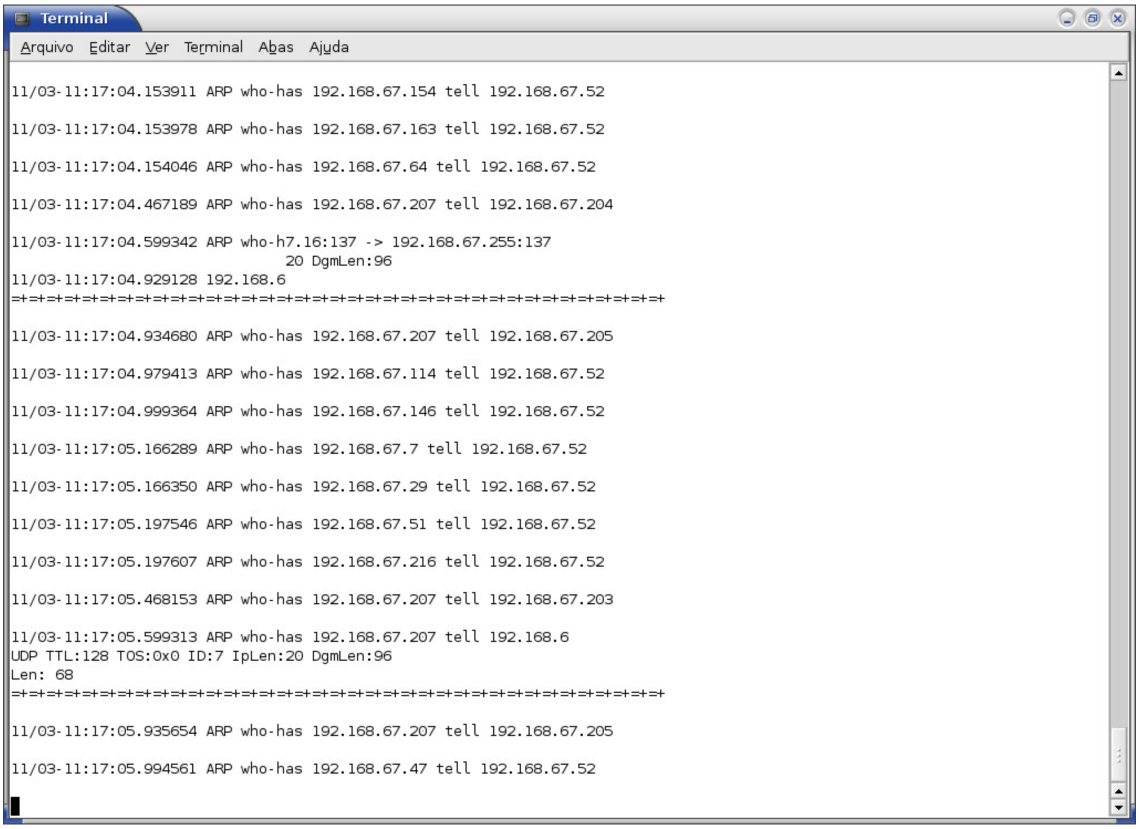

Figura 4.28 – Captura do Snort – STACHELDRAHT.

Arquivo de Log do Snort

[**] [1:241:10] DDOS shaft synflood [**][Classification: Attempted Denial of Service] [Priority: 2]

10/27-15:15:51.545033(tempo de ataque) 192.168.67.124:1617 -> 192.168.67.52:58339 TCP TTL:30 TOS:0x0 ID:14043 IpLen:20 DgmLen:40

********S* Seq: 0x28374839 Ack: 0x97212F05 Win: 0xFFFF TcpLen: 20**

4.7. ANÁLISE

Com a obtenção de todo tráfego de rede em cada um dos componentes pertencentes a uma rede de ataque DDoS, originado pela execução do ataque, pode-se perceber a eficiência deste tipo de ataque. Para o experimento deste trabalho, utilizou-se de duas ferramentas de ataque DDoS: TRIN00 e STACHELDRAHT e ficou evidente que a ferramenta mais eficiente e que pode oferecer maior dificuldade na sua percepção é a ferramenta STACHELDRAHT pelo fato de usar a técnica de criptografia nas comunicações entre master e agentes e também entre agente e a vítima, alem disto esta ferramenta possibilita a ocorrência de um ataque utilizando o TCP_Syn, que em se tratando de negação de serviço é o mais eficiente.

Nos ataques DDoS TRIN00 e STACHELDRAHT é possível perceber que os recursos da máquina da vítima ficam inoperantes após um determinado tempo de execução do ataque, mais precisamente após 10 minutos de execução. Os recursos o qual se tentou executar foram basicamente acesso a Internet, visualização de e-mail e execução de conexão a máquinas da mesma rede, sendo que para todos eles a máquina da vítima tornou-se inoperante.

Um outro ponto positivo neste experimento é que após obter um acesso remoto das máquinas pertencentes a rede de ataque fica bastante simples executar um ataque DDoS, ou seja, após montar a rede de ataque DDoS basta instalar os plugins contido no pacote da ferramenta utilizada em cada componente utilizado no ataque, para depois executá-lo. Para o experimento tanto da ferramenta TRIN00 quanto da STACHELDRAHT a preparação para o ataque utilizou-se em média 20 minutos, sendo que neste tempo realizou-se o download do pacote na Internet e as devidas instalações necessárias para realização dos ataques. Após executar diversas vezes este experimento nos cenários apresentados pode-se afirmar que em poucos minutos um atacante pode efetuar um ataque de negação de serviço e também de negação de serviço distribuído, sendo que a única dificuldade seria a obtenção de controle total das máquinas pelo atacante. A seguir encontra-se uma análise mais detalhada do ataque utilizando TRIN00 e STACHELDRAHT.

TRIN00

A análise destes ataques é fundamentada somente no tráfego obtido durante o ataque, pois como visto anteriormente a percepção deste ataque está no aumento da taxa de tráfego em um host da rede ou também no aumento de tráfego para uma rede, o que permite que algumas requisições não sejam atendidas, como por exemplo, o acesso a uma página de Internet. Nesta simulação, capturou-se tráfego dos *hosts* designados como master, agente e principalmente da vítima, informações estas que estão na seção anterior deste trabalho.

Para o master, pode-se notar que após todos os agentes configurados e executando devidamente seus plugins, estes enviam uma mensagem de ICMP HELLO para o master, enquanto que o agente irá enviar uma seqüência de requisições UDP para a vítima, utilizando endereços IPs diferentes dos deles e de portas que estão abertas na máquina da vítima. A ferramenta escolhe um endereço IP da rede que não pertence a rede de ataque DDoS criada pelo atacante, por isto encontra-se no tráfego requisições de UDP com IPs diferentes, o que representa a técnica de IP Spoofing.

STACHELDRAHT

A análise deste ataque também é fundamentada no tráfego obtido durante a execução do ataque, pois como apresentado anteriormente, a percepção deste dá-se ao aumento da taxa de tráfego em um host da rede ou no aumento de tráfego para uma determinada rede, o que permite que algumas requisições não sejam atendidas como, por exemplo, o acesso a uma página de Internet. Neste experimento capturou-se tráfego dos *hosts* designados como master, agente e principalmente da vítima, informações estas que estão na seção anterior deste trabalho.

Para o ataque utilizando a ferramenta STACHELDRAHT, o tráfego na máquina master ou handler representa a confirmação dos agentes que enviam uma mensagem ICMP do tipo HELLO informando que estão ativos, enquanto que nos agentes, pode-se perceber uma grande quantidade de requerimentos de conexão para a máquina da vítima. Por fim na máquina da vítima, encontra-se uma grande taxa de requerimentos oriundas de máquinas com IP diferente, o que representa a técnica de IP Spoofing. Deve-se levar em consideração que na ferramenta STACHELDRAHT, o atacante pode escolher qual tipo de ataque DoS a ser executado dos agentes para a vítima, ou seja, o flooding existente na máquina da vítima poderá ser de ICMP, UDP ou TCP. Para o experimento, utilizou-se o ataque TCP Syn. Este

flooding é visualizado na vítima quando se tem pacotes TCP seqüenciais com IP de origem distintos e com os campos de ACK e SEQ nulos.

Para concluir a análise dos experimentos destes ataques serão apresentadas a seguir algumas ações a serem tomadas pelos responsáveis de segurança de uma rede ou até de uma organização, dentre estas aplicações encontra-se a elaboração e o consentimento de todos da importância de se aplicar uma política de segurança em um ambiente de tecnologia da informação, pelo fato de estar auxiliando a todos em obter bons usos de seus equipamentos e também dos recursos que se encontram disponíveis em uma determinada rede ou empresa. Além de se aplicar as diversas técnicas de prevenção e de contenção mostradas no capitulo 3 deste trabalho, recomenda-se tomar as seguintes ações[17][18] :

1 Sensibilizar a alta direção para o assunto segurança;

2 Realizar análises profundas e constantes de todos os equipamentos de uma rede ou de uma organização;

3 Corrigir as vulnerabilidades encontradas nestes equipamentos, tais como: Implantar um anti - spoofing [20] na rede, fechar as portas não utilizadas das máquinas e instalar um IDS na rede;

4 Atualizar constantemente todos os sistemas operacionais das máquinas da rede;

5 Criar uma política eficaz de senhas para administradores e usuários com acessos privilegiados;

6 Aplicar regras e filtros anti - spoofing na rede;

7 Proibir que informações confidenciais trafeguem em claro na rede, ou seja, deve-se aplicar protocolos ou ferramentas que implementem a criptografia sobre os dados trafegados na rede;

8 Habilitar e analisar constantemente os logs do sistema;

9 Analisar constantemente todo o tráfego da rede, em que se deve verificar principalmente a taxa de tráfego da rede;

10 Manter atualizado as novas vulnerabilidades;

11 Desabilitar serviços não utilizados na rede;

12 Estabelecer uma política de segurança [19];

13 Capacitar os responsáveis pela administração dos sistemas;

14 Educar usuários para o uso seguro dos recursos de rede;

15 Criar processos de pesquisa e busca de características das eventuais tentativas de ataque;

16 Monitorar, avaliar, corrigir e realimentar o processo de segurança constantemente.

Com análise destes experimentos, pode-se afirmar que a execução de um ataque DDoS é factível de se acontecer em qualquer rede e principalmente na Internet, desde que se tenha controle total de alguns *host.* Para que isto não aconteça deve-se aplicar algumas técnicas de prevenção como, por exemplo, aplicar um filtro de anti-spoofing, bem como a utilização de um IDS capaz de detectar tráfegos estranhos na rede, como o Snort, por exemplo. Para que se tenha um ambiente seguro é viável a aplicação das diversas ações apresentadas anteriormente, bem como a aplicação de uma política de segurança, isto pelo fato de que a segurança de cada integrante da rede depende de todos.

5. CONCLUSÃO

Ataques de negação de serviço e também de negação de serviço distribuído têm causado grandes prejuízos nos últimos anos. Estes ataques visam deixar os serviços oferecidos por uma determinada vítima inacessíveis para usuários legítimos. No caso de vítimas que dependem da Internet para a viabilidade de seus negócios, os ataques de negação de serviço podem ser a causa de danos financeiros incontestáveis. A motivação para estes ataques vai desde o prestígio e a fama dentro da comunidade virtual a outras razões mais sérias, como motivos financeiros e políticos.

Diversos ataques de negação de serviço são conduzidos a partir de pacotes com endereço de origem forjados, através da técnica de IP Spoofing com o objetivo de dificultar a identificação do atacante. Como o roteamento de pacotes IP é baseado exclusivamente no endereço de destino e nenhum teste é realizado para verificar a autenticidade da origem, pacotes com endereços de origem forjados são enviados sem problemas até o seu destino. Além disso, os roteadores não armazenam nenhuma informação sobre os pacotes encaminhados, o que impossibilita a determinação da rota tomada por um pacote depois do seu recebimento. Atacantes aproveitam-se destas características para executarem um ataque do tipo DDoS sem precisar se identificar.

Este trabalho objetivou-se em estudar e desenvolver um ambiente experimental de ocorrência de um ataque DDoS, bem como fazer as análises necessárias quanto ao tráfego presente na rede e nos componentes de uma rede de ataque DDoS, tais como : Atacante, Master, Agente e a própria Vítima. Como resultado desta análise são apresentadas algumas ações importantes a serem tomadas pelo administrador de uma rede e de uma organização, tais como implantar uma política de segurança séria e um plano de contingência baseando-se nas técnicas de prevenção apresentadas neste trabalho.

Após a simulação destes ataques utilizando as ferramentas TRIN00 e a ferramenta STCHELDRAHT, pode se observar que os ataques de negação de serviço e negação de serviço distribuído são muito eficientes e rápidos para atingir o seu objetivo, que é negar o serviço de uma máquina ou rede para usuários legítimos, utilizando vulnerabilidades encontradas nas próprias máquinas e em seus sistemas operacionais. A partir disto, conclui-se que um ambiente de rede que tem o objetivo de minimizar os riscos de um ataque de negação de serviço e principalmente de um ataque de negação de serviço distribuído deve

periodicamente estar monitorando o tráfego de rede através da aplicação de um anti - spoofing e de um IDS, bem como também estar constantemente se atualizando quanto as novas vulnerabilidades encontradas em sistemas operacionais, softwares e até nas próprias máquinas, como por exemplo, desativar as portas de comunicação que não se encontram em uso pelo sistema. Com isso, nota-se que não existe uma única solução eficiente capaz de minimizar por completo um ataque de negação de serviço, mas sim a aplicação de diversas técnicas, que podem incluir gerência de redes, monitoramento de tráfego, configuração ideal de máquinas de uma rede e técnicas definidas em uma política de segurança para determinada organização ou até uma determinada rede.

Após a execução deste trabalho, bem como, as devidas análises obtidas dele, pode-se listar algumas propostas de trabalhos futuros com a função de complementar algumas indagações apresentadas neste trabalho, apresentados a seguir:

1 Elaborar em detalhes uma política de segurança e um plano de contingência, levando em consideração os resultados e as análises encontradas neste trabalho.

2 Construir um ambiente para simulação real de ataques de negação de serviço e ataques de negação de serviço distribuído, utilizando uma rede sem fio, bem como, fazer uso de um filtro anti - spoofing e de um IDS.

3 Analisar e criar simulações em ambientes reais de ataque de negação de serviço, em que terá como objetivo apresentar soluções confiáveis a respeito do *traceback* da detecção de um ataque de negação de serviço, tais como o Filtro de Bloom [21][23] e utilizando uma marcação de pacotes IP[22]. Desta forma, pode-se obter um ambiente ideal onde se tem a oportunidade de rastrear o verdadeiro atacante de um ataque de negação de serviço.

4 Implementação de um detector de ataque em uma rede, abordando métricas de Qualidade de Serviço e de Gerência de Redes, que serão fundamentais na prevenção e defesa de ataques de DoS e DDoS.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CERT. *CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack*, fevereiro de 1996. Acessado em 15/04/2006 em http://www.cert.org/advisories/CA-1996-01.html.

[2] CERT. *CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks*, setembro de 1996. Acessado em 15/04/2006 em http://www.cert.org/advisories/CA-1996-21.html.

[3] CERT. *CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks*, janeiro de 1998. Acessado em 15/04/2006 em http://www.cert.org/advisories/CA-1998-01.html.

[4] CERT. *CERT Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks*, novembro de 2000. Acessado em 15/04/2006 em http://www.cert.org/advisories/CA-2000-21.html.

[5] Bertholdo, L. M., Andreoli, A. V., e Tarouco, L. 2005 Compreendendo Ataques *Denial of Services*, 2005.

[6] GORDON, L. A., LOEB, M. P., LUCYSHYN, W., E RICHARDSON, R. *2005 CSI/FBI Computer Crime and Security Survey*, 2005.

[7] Kumar, S. P.,Sanghi, D. 2005 Techniques to Mitigate and Prevent DoS/DDoS Attacks, 2005

[8] Segurança de rede – *Network Security*. Acessado em 15/08/2006 em http://paginas.fe.up.pt/~mgi98020/pgr/DoS.htm.

[9] RNP. Tudo que Você Precisa Saber Sobre os Ataques DDoS. Acessado em 07/04/2006 em http://www.rnp.br/newsgen/0003/ddos.html

[10] Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P. INTERNET DENIAL OF SERVICE Attack and Defense Mechanisms. Prentice Hall, 2005.

[11] *Dittrich, D. The DoS Project's 'trinoo' distributed denial of service attack. Acessado em 07/04/2006 em* http://staff.washington.edu/dittrich/misc/trinoo.analysis

[12] *Dittrich, D. The DoS Project's 'Trible Flood Network' distributed denial of service attack. Acessado em 07/04/2006 em* http://staff.washington.edu/dittrich/misc/tfn.analysis

[13] *Dittrich, D. The DoS Project's 'stacheldraht' distributed denial of service attack. Acessado em 07/04/2006 em* http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

[14] Advanced Networking Management Lab (ANML) Distributed Denial of Service Attacks(DDoS) Resources. Acessado em

07/08/2006 em http://anml.iu.edu/ddos/types.html
[15] Pivotto, C. V. C., Pimenta, L. C. S., Denial of Service – Negação de Serviço. Acessado em 11/09/2006 em http://www.gta.ufrj.br/grad/06_1/dos
[16] C. A. Huegen, "The latest in denial of service attacks : 'Smurfing' description and information to minimize effects," Feb.2000. Acessado em 07/08/2006 em http://users.quadrunner.com/chuegen/smurf.cgi
[17] CERT. *CERT Coordination Center, "Results of the distributed systems intruder tools workshop", Novembro 1999.* Acessado em 15/04/2006 em http://www.cert.org/reports/dsit_workshop.pdf.

[18] Correa, N. DDoS, Tudo o que você precisa saber antes de receber esta visita. Acessado em 11/09/2006 em http://www.modulo.com.br
[19] Dias, C. Segurança e Auditoria da Segurança da Informação. Axcel Books, 2000.
[20] Ferguson, P., Senie, D. "RFC 2267 : Network ingress filtering : defeating denial of service attacks which employ IP source address spoofing", Janeiro 1998. Acessado em 15/10/2006 em http://info.internet.isi.edu/innotes/rfc/files/rfc2267.txt
[21] Laufer, R. P., Velloso, P. B., Duarte, O. C. M. B., Um Novo Sistema de Rastreamento de Pacotes IP contra Ataques de Negação de Serviço, 2005.
[22] Dean, D., Franklin, M., STUBBLEFIELD, A. "An Algebraic Approach to IP Traceback", Maio de 2002.

[23] Laufer, R. P., Velloso, P. B., Duarte, O. C. M. B., Defeating DoS Attacks with IP Traceback, Abril de 2005.
[24] Boulevard, W. RFC 791 : Internet Protocol, Setembro de 1981. Acessado em 15/10/2006 em http://www.ietf.org/rfc/rfc0791.txt.
[25] Boulevard, W. RFC 793 : Transmiss Control Protocol, Setembro de 1981. Acessado em 15/10/2006 em http://www.faqs.org/rfcs/rfc793.html.
[26] Postel, J. RFC 768 : User Datagram Protocol, Agosto de 1980. Acessado em 15/10/2006 em http://www.freesoft.org/CIE/RFC/768/index.htm
[27] Postel, J. RFC 792 : Internet Control Message Protocol, Setembro de 1981. Acessado em 15/10/2006 em http://www.freesoft.org/CIE/RFC/792/
[28] Sharma, K. IP Spoofing, Dezembro de 2001. Acessado em 17/10/2006 em http://www.gazetadolinux.com/pr/lg/issue63/sharma.html
[29] Internet Security Systems. Iss Security Alert, 2000. Acessado em 17/10/2006 em http://www.internetsecuritysystems.com/about/press_center/releases/pr_14687.html
[30] Wikipedia. Intrusion Detection System, Outubro 2006. Acessado em 20/10/2006 em http:// http://en.wikipedia.org/wiki/Intrusion-detection_system

[31] Wikipedia. Snort, Outubro 2006. Acessado em 20/10/2006 em http://en.wikipedia.org/wiki/Snort_software

[32] Packet Storm. Outubro 2006. Acessado em 20/10/2006 em http://packetstormsecurity.org/