

## **Negação de Serviço em servidores DHCP: Implementando um cenário de ataque e definindo estratégias de prevenção e defesa**

**Elionildo da Silva MENEZES (1); Igor Nogueira de OLIVEIRA (2)**

(1) Centro Federal de Educação Tecnológica da Paraíba (CEFET/PB), Avenida 1º de Maio, Nº 720, CEP 58015-430, João Pessoa – PB, (83) 32083062, e-mail: [elionildo@cefetpb.edu.br](mailto:elionildo@cefetpb.edu.br)

(2) CEFET/PB, e-mail: [acesso.igor@gmail.com](mailto:acesso.igor@gmail.com)

### **RESUMO**

O DHCP é um protocolo cliente/servidor da Arquitetura TCP/IP, responsável pela atribuição dinâmica de endereços IP para computadores de uma rede. Um servidor DHCP empresta endereços IP, por tempo determinado, para computadores (clientes DHCP) na rede em que ele atua. Inicialmente, o servidor DHCP é configurado com uma faixa de endereços IP. Em cada empréstimo, um endereço da faixa é utilizado e a quantidade de endereços disponíveis é decrementada. Ao esgotar os endereços disponíveis, o servidor não mais realizará empréstimos. Nesse contexto, uma aplicação maliciosa poderia requisitar todos os endereços disponibilizados pelo servidor DHCP, impedindo que computadores de usuários legítimos consigam obter endereços IP. O cenário descrito é denominado ataque de DoS (*Denial of Service* – Negação de Serviço). Este artigo pretende apresentar um cenário onde um servidor DHCP é alvo de ataque DoS e propor estratégias de prevenção e defesa contra esse ataque. O trabalho é uma pesquisa experimental e a metodologia utilizada contempla estudo do DHCP, implementação do cenário de testes, realização do ataque, análise das consequências e, discussão de estratégias de prevenção e defesa. Como contribuição deste trabalho, destaca-se a apresentação de estratégias para minimizar a vulnerabilidade de servidores DHCP, aumentando a disponibilidade desse serviço em uma rede.

**Palavras-chave:** DHCP, negação de serviço, ataque, defesa, prevenção

## 1. INTRODUÇÃO

Com a popularização da Internet, notadamente a partir de meados da década de 1990, motivado pela utilização da *World Wide Web* como principal aplicação, as redes de computadores tornaram-se um instrumento indispensável à comunicação entre pessoas espalhadas pelo mundo inteiro, sendo um dos fatores determinantes para a proliferação do uso de computadores pessoais em empresas e residências. Nesse cenário, surgiram duas questões relacionadas ao gerenciamento de endereços IP (*Internet Protocol*): a primeira estava relacionada à necessidade de configuração dos endereços IP nos *hosts* de forma mais simples, uma vez que o mecanismo tradicional consistia em uma configuração onde um ou mais indivíduos eram obrigados a configurar localmente e manualmente o endereço e outros parâmetros IP em cada *host* na rede; a segunda questão era a preocupação de como atender a uma demanda cada vez maior de *hosts* – o que inclui nos dias atuais roteadores, servidores de rede, estações de trabalho do tipo *desktops*, *notebooks* e outros dispositivos – que precisavam de endereços IP para comunicarem-se dentro da rede local e com outros dispositivos na Internet. A resposta para essas questões foi o desenvolvimento de um protocolo denominado DHCP (*Dynamic Host Configuration Protocol*), que é utilizado para emprestar, sob demanda e por um tempo determinado, endereços IP a *hosts* que precisam usar serviços de rede no âmbito da rede local ou na Internet.

Como acontece com outros protocolos de rede, a forma como o DHCP foi projetado, conforme descrito na seção seguinte, permite que usuários mal intencionados requisitem todos os endereços IP disponíveis para empréstimo. Com isso, *hosts* legítimos da rede não irão conseguir obter empréstimos de endereços IP e, dessa forma, ficarão impossibilitados de acessarem recursos de rede na sua rede ou na Internet. A situação apresentada aqui é denominada ataque de negação de serviço (DoS – *Denial of Service*).

Este artigo apresenta um cenário de ataque DoS a um servidor DHCP e propõe estratégias de prevenção e defesa contra este tipo de ataque. A seção 2 apresenta uma revisão bibliográfica de trabalhos relacionados com o tema em estudo. A seção 3 descreve o cenário de rede configurado para a realização do ataque bem como o próprio ataque e suas conseqüências. A seção 4 apresenta estratégias que podem ser usadas para proteger o servidor DHCP e minimizar os efeitos do ataque. Por fim, a seção 5 apresenta alguns comentários sobre o estudo realizado ao mesmo em que aponta para os passos futuros da pesquisa.

## 2. TRABALHOS RELACIONADOS

### 2.1. DHCP

O DHCP, descrito em DROMS (1997), é um protocolo cliente/servidor da Arquitetura TCP/IP (*Transmission Control Protocol/Internet Protocol*). Ele especifica um mecanismo para interação entre cliente e servidor DHCP durante o processo de negociação/renovação de um empréstimo de endereço (e outros parâmetros) IP e um mecanismo para configuração desses parâmetros no cliente.

Alguns dos conceitos relacionados ao contexto do serviço DHCP são (BLANK, 2002):

- Servidor DHCP – É um *host* executando o serviço de empréstimo de endereços IP a outros *hosts*. Ele é configurado por um administrador de rede com uma faixa de endereços que poderão ser emprestados. Doravante, será referenciado neste documento, apenas por servidor.
- Cliente DHCP – É todo *host* que requisita o empréstimo de um endereço IP ao servidor DHCP. Doravante, será referenciado neste documento, apenas por cliente.
- Escopo – Uma faixa de endereços IP que um servidor DHCP possui para emprestar aos clientes DHCP.

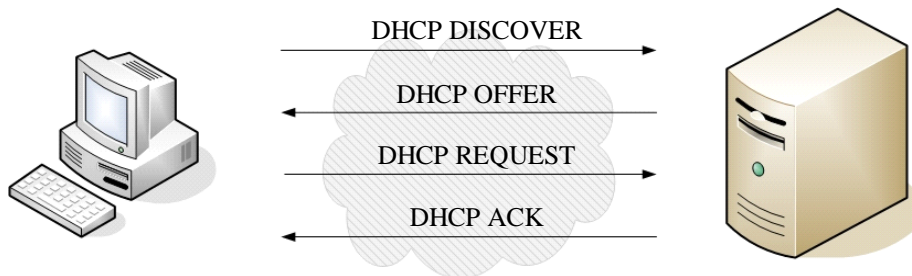
O DHCP suporta três tipos de configuração de endereços IP (COMER, 1995):

- Manual – O administrador da rede deve configurar localmente em cada *host* o endereço IP e demais parâmetros associados ao mesmo. Comumente utilizada para configurar servidores de rede e outros dispositivos de rede, como roteadores.
- Automática ou por reserva – O administrador da rede deve configurar o servidor de forma que a um determinado *host* sempre seja emprestado o mesmo endereço IP. Comumente utilizada para configurar estações de gerência da rede ou de usuários com necessidades específicas.
- Dinâmica – O administrador da rede deve configurar o servidor com uma faixa de endereços IP de tal forma que a qualquer *host* possa ser emprestado qualquer endereço IP disponível na faixa, por um período limitado. Comumente utilizada para configurar os *hosts* da rede pertencentes a usuários comuns.

Apenas nos dois últimos tipos de configuração existe realmente interação entre cliente e servidor. E, nesses casos, além do endereço IP emprestado, outros parâmetros de configuração podem ser, e comumente são, enviados ao cliente.

O mecanismo de empréstimo descrito a seguir é utilizado no restante deste artigo é aquele executado durante a configuração dinâmica de endereços IP.

A realização de um empréstimo IP é um processo que envolve quatro etapas, cada uma delas associada a uma mensagem específica, como mostrado na figura 1 e descrito a seguir (DROMS, 1997 e BLANK, 2002).



**Figura 1 - Mensagens trocadas entre cliente e servidor durante um empréstimo bem-sucedido**

- **DHCP DISCOVER** – Enviada quando o cliente é iniciado e precisa obter um empréstimo porque não possui um endereço IP ou porque precisa de um novo endereço. O pacote com a mensagem DHCP DISCOVER é enviado via *broadcast* para a rede e a meta é que ele chegue a algum servidor existente.
- **DHCP OFFER** – Ao receber a mensagem DHCP DISCOVER, o servidor consulta seu escopo em busca de um endereço disponível para emprestar ao cliente. Caso tal endereço exista, o servidor cria um pacote DHCP OFFER, contendo um endereço IP, máscara de rede, tempo de empréstimo, bem como outros parâmetros de configuração que o servidor está oferecendo. Esse pacote é enviado via *broadcast* para o cliente que fez a requisição. Caso o cliente receba mais de uma oferta, pelo fato de sua requisição ter chegado a mais de um servidor, ele escolherá a primeira.
- **DHCP REQUEST** – Quando o cliente recebe o pacote com a mensagem DHCP OFFER, ele envia um pacote DHCP REQUEST. Esse pacote diz ao servidor que sua oferta foi aceita. Ele é enviado via *broadcast* para a rede, pois o cliente ainda continua sem endereço IP válido e porque é preciso avisar todos os servidores sobre qual servidor teve sua oferta aceita. Com isso, aqueles servidores cujas ofertas não foram aceitas poderão liberar seus endereços para serem oferecidos quando da chegada de novas requisições.
- **DHCP ACK** – Ao receber a DHCP REQUEST, o servidor prepara um pacote para concretizar a realização do empréstimo. Esse pacote contém uma mensagem DHCP ACK. O servidor envia o pacote via *broadcast* para o cliente, seguindo as mesmas definições de endereçamento utilizadas para o envio da mensagem DHCP OFFER. Ao receber o pacote com a mensagem DHCP ACK, o cliente pode enfim, utilizar o endereço IP emprestado e os demais parâmetros de configuração, durante o tempo de empréstimo definido pelo servidor.

A figura 2 mostra os pacotes capturados com as mensagens trocadas entre cliente e servidor para empréstimo de um endereço IP via DHCP. É importante informar que, nessa negociação, o cliente obteve o endereço IP 192.168.10.10 além de outros parâmetros IP fornecidos no empréstimo realizado pelo servidor, cujo endereço IP é 192.168.10.254.

No. -	Time	Source	Destination	Protocol	Info
13	74.708007	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
14	74.709861	192.168.10.254	255.255.255.255	DHCP	DHCP Offer
15	74.726817	0.0.0.0	255.255.255.255	DHCP	DHCP Request
16	74.735224	192.168.10.254	255.255.255.255	DHCP	DHCP ACK

Figura 2 - Interação entre cliente e servidor para obtenção de um empréstimo DHCP

A cada empréstimo realizado, o endereço emprestado é removido do escopo. E, após emprestar todos os endereços, o servidor não poderá realizar mais nenhum empréstimo até que algum cliente libere seu endereço IP. Essa liberação pode ocorrer porque o cliente estava fora da rede ou desligado quando o tempo de empréstimo expirou ou porque o usuário executou um comando de liberação de empréstimo em seu cliente. É importante lembrar que o cliente que obtém um empréstimo de um endereço IP via DHCP, deve solicitar automaticamente a sua renovação, sob condições normais, ao final de 50% do tempo do empréstimo.

## 2.2. Ataque de negação de serviço

A meta de um ataque de negação de serviço, doravante referenciado apenas por DoS, é consumir todos os recursos de um *host* ou rede local ou remoto a fim de tornar um ou mais dos seus serviços indisponíveis para os usuários legítimos dos mesmos (MOORE, 2001 e MIRKOVIC, 2004).

A figura 3 mostra o cenário de um ataque de DoS. Nela, é possível notar que comumente o atacante invade um outro *host* e o utiliza para realizar o ataque ao sistema alvo.

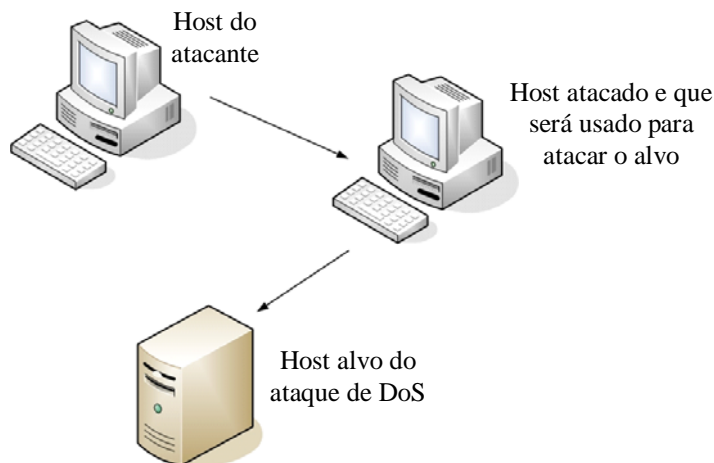


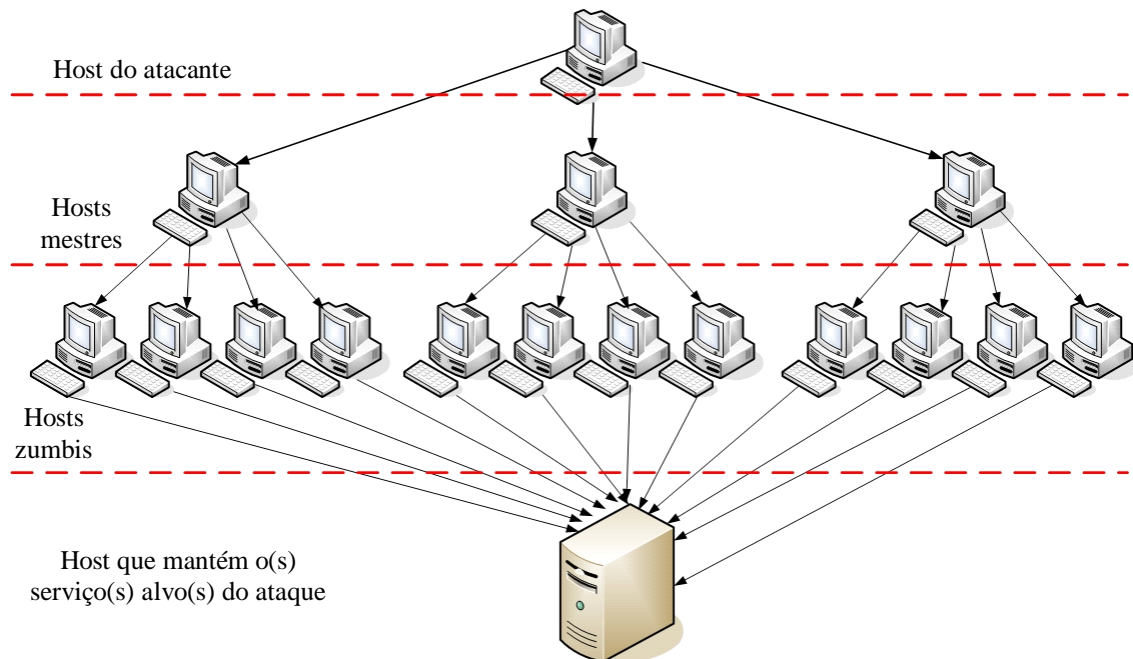
Figura 3 - Cenário de um ataque de DoS

As técnicas usadas em um ataque de DoS podem sobrecarregar uma rede a tal ponto que os verdadeiros usuários dela não consigam usá-la; derrubar uma conexão entre dois ou mais computadores; fazer tantas requisições a um *site* até que este não consiga mais ser acessado; negar acesso a um sistema ou a determinados usuários (ALECRIM, 2004).

Um dos fatores que dificultam a adoção de medidas para evitar ataques de DoS é o fato de não ser possível distinguir o tráfego gerado pelo atacante do tráfego gerado pelos usuários legítimos do serviço. Ou seja, os atacantes utilizam mensagens normalmente empregadas em comunicações normais. Assim, ações que

priorizem o tráfego legítimo em detrimento do tráfego de ataque são difíceis de serem tomadas (LAUFER, 2005).

Uma recente evolução dos ataques de DoS consiste na utilização, pelo atacante, de vários *hosts* como fonte para ataque a um determinado sistema. Essa nova estratégia é denominada ataque de negação de serviço distribuído (DDoS – *Distributed Denial of Service*). O ataque de DDoS é mais destrutivo que o DoS haja vista que nele o poder computacional dos vários *hosts*, denominados zumbis, é somado para tornar indisponível um único alvo. Além disso, é mais difícil detectar a origem real do ataque, pois este parte de várias fontes. A figura 4 mostra um cenário de ataque de DDoS.



**Figura 4 - Cenário de um ataque de DDoS (baseado na figura disponível em <http://www.infowester.com>)**

Na figura 4, pode-se observar que o atacante primeiro ataca os *hosts* denominados mestres e, em seguida, os utiliza para atacar os *hosts* denominados zumbis. A partir daí, os zumbis são configurados para, em um momento previamente configurado, atacarem o *host* alvo.

O estudo realizado neste artigo tratará apenas do ataque de DoS a um servidor DHCP, conforme descrito nas próximas seções.

### 3. ATAQUE DE NEGAÇÃO DE SERVIÇO AO SERVIDOR DHCP

#### 3.1. Cenário de rede

O cenário de rede utilizado para a realização e análise do ataque foi construído com três máquinas virtuais no programa VMWare<sup>1</sup>. Os sistemas operacionais instalados foram o Linux Debian Etch<sup>2</sup> como servidor DHCP, o Linux Debian Etch como cliente malicioso e o Microsoft Windows XP SP2 como cliente legítimo. A escolha do sistema Linux ocorreu devido ao uso de um *Shell Script* que foi desenvolvido para realizar o ataque. A utilização de um cliente Windows foi devido à grande popularidade na utilização desse sistema operacional como *desktop* de rede. As configurações das máquinas virtuais são descritas na tabela 1. A captura do tráfego de rede foi realizada com o Wireshark<sup>3</sup>

<sup>1</sup> O VMWARE pode ser encontrado para *download* em versão de avaliação no endereço <http://www.vmware.com>

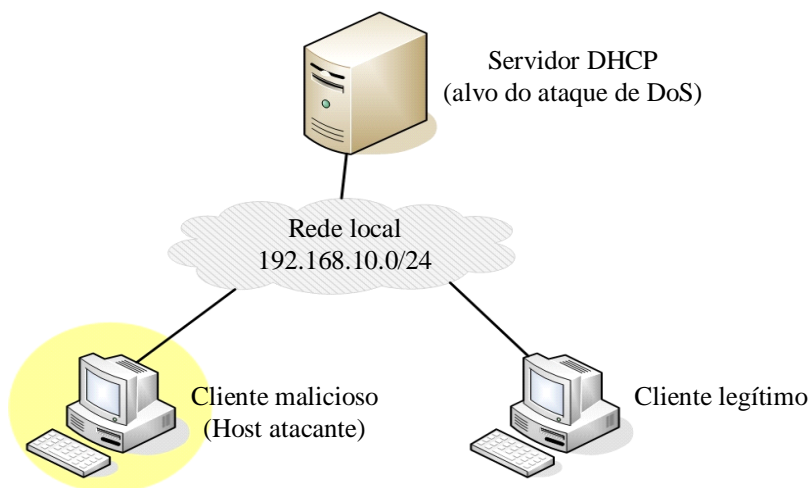
<sup>2</sup> O Linux Debian Etch corresponde à versão 4 deste sistema operacional. Ele pode ser obtido via *download* no endereço <http://www.debian.org.br>

<sup>3</sup> O Wireshark (antigo Ethereal) é um *sniffer*, isto é, um programa utilizado para capturar tráfego de rede. Ele pode ser obtido via *download* no endereço <http://www.wireshark.org>

**Tabela 1 - Configurações das máquinas virtuais**

Maquina	Processador	Memória	Disco rígido	Interface de rede
Servidor	Intel Pentium 4 1.8 GHz <sup>4</sup>	256 MB	3.0 GB	10Mbps
Cliente Malicioso	Intel Pentium 4 1.8 GHz	1024 MB	3.0 GB	10Mbps
Cliente Legítimo	Intel Pentium 4 1.8 GHz	256 MB	3.0 GB	10Mbps

A rede implementada no VMWARE obedece à topologia mostrada na figura 5.



**Figura 5 - Topologia da rede utilizada para testes de ataque**

### 3.2. Descrição dos ataques e análise das consequências

Durante os testes, foram realizados dois ataques ao servidor DHCP. Entretanto, esses ataques seguiram o mesmo princípio e foram realizados utilizando-se o mesmo *Shell Script*, cuja listagem do seu código é mostrada a seguir.

```
#!/bin/bash

# Endereço IP Atual.
echo "IP Atual:      "`/sbin/ifconfig $1 | grep inet | awk {'print $2'} | cut -d":" -f2`

# Endereço MAC Atual.
echo "MAC Atual:      "`/sbin/ifconfig $1 | grep HW | awk {'print $5'}`

# Gerando MAC aleatório.
hw=`dd if=/dev/urandom bs=1 count=6 2> /dev/null | od -t x1 | head -n 1 | cut -d' ' -f2-7 | awk {' print $1":"$2":"$3":"$4":"$5":"$6 ' } | cut -f1`
echo "MAC Aleatorio: "$hw

# Atribuindo MAC aleatório a interface de rede.
ifconfig $1 down
ifconfig $1 hw ether $hw

# Gerando requisição de configuração DHCP.
```

<sup>4</sup> A velocidade do processador depende da máquina onde o VMWare estiver sendo executado..



```
if [ -e /var/run/dhclient.pid ]; then
    rm /var/run/dhclient.pid
fi
dhclient $1

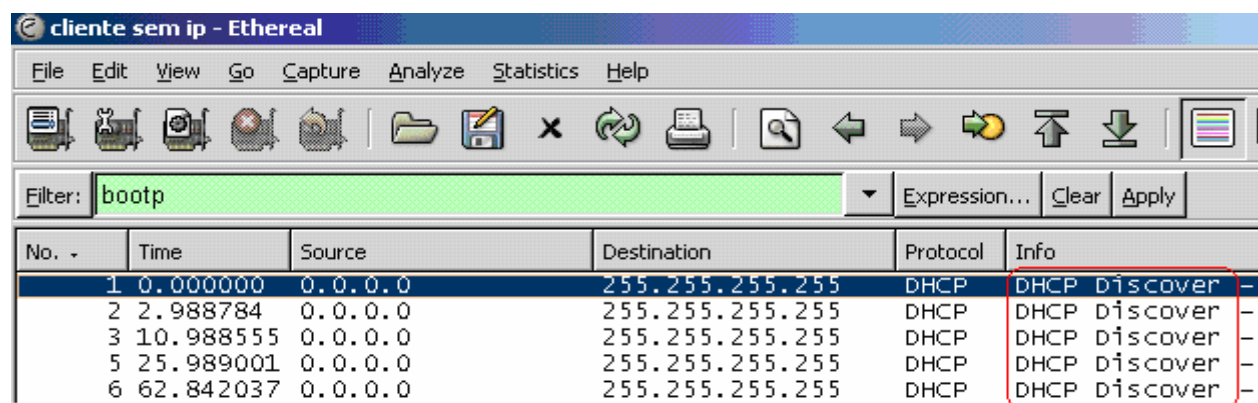
# Novo endereço IP
echo "IP novo:          "`/sbin/ifconfig $1 | grep inet | awk {'print $2'} | cut -
d":" -f2`
```

Os testes de ataque realizados consistiram na execução, no *host* malicioso, do *script* apresentado anteriormente. Basicamente esse *script* faz as seguintes tarefas: gera um endereço MAC<sup>5</sup> (*Media Access Control*) aleatório e, para esse endereço, solicita um empréstimo ao servidor DHCP. Ao ser executado dentro de uma repetição, o *script* consegue gerar endereços MAC e obter empréstimos até esgotar toda a faixa de endereços disponibilizados pelo servidor DHCP para alocação dinâmica, conseguindo, com isso, realizar o ataque de DoS. É importante observar que, como ocorre com outras modalidades de ataques DoS, é praticamente impossível descobrir o ataque ao servidor DHCP, pois na visão deste todas as solicitações vieram de *hosts* distintos.

A seguir são analisados os dois ataques realizados e seus impactos na rede:

- Primeiro ataque – Nesse cenário, o servidor DHCP foi configurado<sup>6</sup> com um tempo de empréstimo de 01 dia (86400 segundos) e uma faixa de IP's de 192.168.10.1 até 192.168.10.200. Em seguida, o processo servidor DHCP foi iniciado. Por fim, o *script* de ataque foi executado no cliente malicioso e, após algum tempo, esse cliente conseguiu obter por empréstimo todos os endereços da faixa disponibilizada pelo servidor DHCP. Com isso, o cliente legítimo não conseguiu o empréstimo do endereço IP que precisava para conectar-se à rede.

Análise da consequência do ataque: Com o tempo de empréstimo elevado, o efeito do ataque ao servidor é altamente danoso, pois cada empréstimo associado a um MAC forjado será válido por 1 dia, a menos que o servidor seja reiniciado pelo administrador da rede. Portanto, se esse ataque for realizado em uma organização durante um momento em que não haja alguém especializado para detectá-lo e reiniciar o processo servidor DHCP, os usuários de clientes legítimos terão 01 dia inteiro de trabalho sem acesso aos serviços da rede IP, o que inclui a rede da própria organização e o acesso à Internet. A figura 6 mostra as tentativas, sem sucesso, do cliente legítimo para obter um empréstimo junto ao servidor atacado.



The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "cliente sem ip - Ethereal". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons. A filter box contains the text "bootp". Below the filter is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, and Info. The first six packets are all DHCP Discover requests from source 0.0.0.0 to destination 255.255.255.255. The 'Info' column for these packets shows "DHCP Discover". The last four rows of the table are highlighted with a red box.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
2	2.988784	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
3	10.988555	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
5	25.989001	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
6	62.842037	0.0.0.0	255.255.255.255	DHCP	DHCP Discover

**Figura 6 – Tentativas do cliente para obter um empréstimo junto ao servidor DHCP**

A figura 7 mostra a tela do *prompt* de comandos do cliente legítimo em três momentos: (1) O cliente utilizava o endereço IP 192.168.10.10, obtido por empréstimo; (2) O usuário do cliente liberou o empréstimo do endereço; (3) O cliente não conseguiu obter um novo empréstimo, pois o servidor DHCP já havia sido atacado.

<sup>5</sup> O endereço MAC é também conhecido como endereço físico da placa de rede. Ele consiste em um valor de 6 bytes.

<sup>6</sup> O arquivo de configuração do servidor DHCP, no Linux Debian, é o `/etc/dhcp3/dhcp.conf`

```
C:\WINDOWS\system32\cmd.exe
Suífixo DNS específico de conexão . : redelinux.com.br
Endereço IP . . . . . : 192.168.10.10
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 192.168.10.253

C:\Documents and Settings\Administrador>ipconfig /release

Configuração de IP do Windows

Adaptador Ethernet Conexão local:

    Suífixo DNS específico de conexão . : redelinux.com.br
    Endereço IP . . . . . : 0.0.0.0
    Máscara de sub-rede . . . . . : 0.0.0.0
    Gateway padrão. . . . . :

C:\Documents and Settings\Administrador>ipconfig /renew

Configuração de IP do Windows

Erro ao renovar a interface Conexão local : não é possível contactar o servidor
DHCP. Expirado o tempo limite da solicitação
```

The screenshot shows a Windows command prompt window. The title bar reads 'C:\WINDOWS\system32\cmd.exe'. The command prompt shows the output of 'ipconfig' and 'ipconfig /release', followed by 'ipconfig /renew'. Three red boxes with numbers 1, 2, and 3 are overlaid on the image. Box 1 is around the first 'ipconfig' output. Box 2 is around the 'ipconfig /release' output. Box 3 is around the 'ipconfig /renew' output.

Figura 7 - Cliente legítimo. (1) Utilizando um endereço IP. (2) Liberando o empréstimo do endereço IP. (3) Sem conseguir obter um novo empréstimo de endereço IP

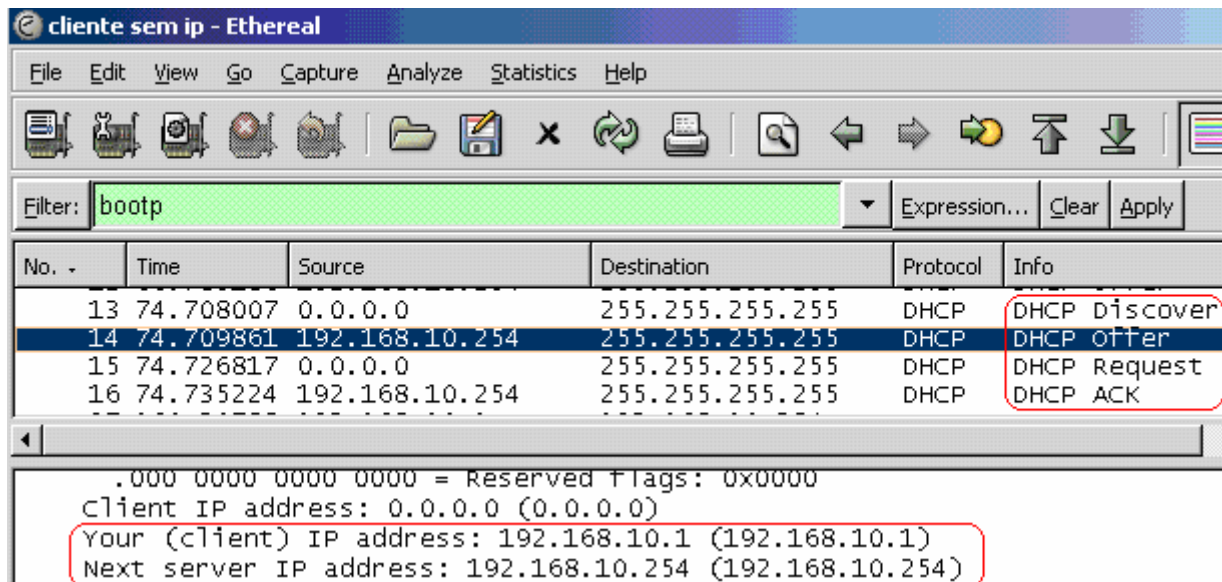
- Segundo ataque – Nesse cenário, o servidor DHCP foi configurado com um tempo de empréstimo de 10 minutos e uma faixa de IP's de 192.168.10.1 até 192.168.10.200. Em seguida, o processo servidor DHCP foi iniciado. Por fim, o *script* de ataque foi executado no cliente malicioso e, após algum tempo, esse cliente conseguiu obter por empréstimo todos os endereços da faixa disponibilizada pelo servidor DHCP. Com isso, o cliente legítimo não conseguiu o empréstimo do endereço IP que precisava para conectar-se à rede, assim como já havia acontecido no ataque anterior.

Análise da consequência do ataque: Graças ao tempo de empréstimo baixo, o efeito do ataque é um pouco menos nocivo ao servidor e principalmente ao cliente legítimo em comparação com o primeiro ataque, pois cada empréstimo associado a um MAC forjado será válido por, no máximo, 10 minutos. O grande problema é que, mesmo com esse tempo baixo, como o *script* estava executando indefinidamente, o cliente malicioso conseguia obter, na maioria das vezes, o empréstimo de cada endereço que havia sido liberado por falta de renovação, antes do cliente legítimo. Assim, mesmo com um tempo de empréstimo menor, o cliente legítimo nem sempre conseguiu um endereço IP.

A figura 8 mostra os pacotes trocados entre servidor DHCP e cliente legítimo quando este último, após várias tentativas mal-sucedidas, enfim conseguiu obter um novo empréstimo.

A figura 9 mostra a tela do *prompt* de comandos do cliente legítimo em três momentos. Nos dois primeiros, o cliente tenta obter um novo empréstimo e não consegue. No terceiro momento, o cliente legítimo vence a disputa com o cliente malicioso e consegue um novo empréstimo junto ao servidor DHCP, com o endereço IP indicado na figura anterior.





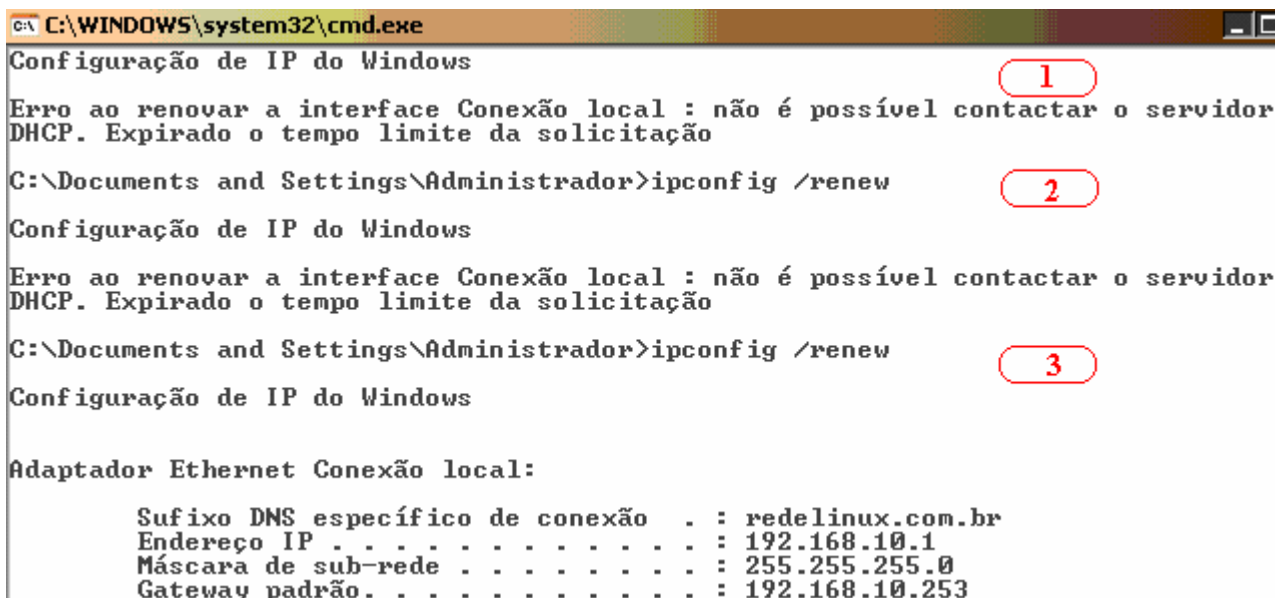
The image shows a Wireshark packet capture window titled "cliente sem ip - Ethereal". The filter is set to "bootp". The packet list shows four DHCP-related packets:

No.	Time	Source	Destination	Protocol	Info
13	74.708007	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
14	74.709861	192.168.10.254	255.255.255.255	DHCP	DHCP Offer
15	74.726817	0.0.0.0	255.255.255.255	DHCP	DHCP Request
16	74.735224	192.168.10.254	255.255.255.255	DHCP	DHCP ACK

The packet details pane for packet 16 shows the following information:

```
.0000 0000 0000 0000 = Reserved flags: 0x0000  
Client IP address: 0.0.0.0 (0.0.0.0)  
Your (client) IP address: 192.168.10.1 (192.168.10.1)  
Next server IP address: 192.168.10.254 (192.168.10.254)
```

Figura 8 - Cliente legítimo consegue o empréstimo do endereço 192.168.10.1



```
C:\WINDOWS\system32\cmd.exe  
Configuração de IP do Windows  
Erro ao renovar a interface Conexão local : não é possível contactar o servidor  
DHCP. Expirado o tempo limite da solicitação  
C:\Documents and Settings\Administrador>ipconfig /renew  
Configuração de IP do Windows  
Erro ao renovar a interface Conexão local : não é possível contactar o servidor  
DHCP. Expirado o tempo limite da solicitação  
C:\Documents and Settings\Administrador>ipconfig /renew  
Configuração de IP do Windows  
Adaptador Ethernet Conexão local:  
Sufixo DNS específico de conexão . : redelinux.com.br  
Endereço IP . . . . . : 192.168.10.1  
Máscara de sub-rede . . . . . : 255.255.255.0  
Gateway padrão. . . . . : 192.168.10.253
```

Figura 9 - Cliente legítimo. (1) e (2) Não consegue obter um empréstimo de endereço IP. (3) A requisição de empréstimo IP é atendida pelo servidor DHCP

É importante destacar que, como era esperado, após obter o empréstimo do endereço IP o cliente conseguiu renová-lo normalmente. Isso ocorre porque o cliente legítimo que obtém um endereço emprestado, sob condições normais, sempre tenta renovar o mesmo endereço antes que o tempo de empréstimo se esgote. Ou seja, o endereço emprestado ao cliente legítimo em momento algum fica disponível durante uma negociação de renovação de empréstimo.

#### 4. ESTRATÉGIAS DE PROTEÇÃO E DEFESA DO SERVIDOR

Após analisar os casos de ataques apresentados anteriormente, pode-se notar que praticamente não existe medida de defesa contra esses ataques. Entretanto, fica entendido pela análise da consequência do segundo ataque que uma possível medida de defesa é configurar o escopo do servidor DHCP com um tempo de empréstimo baixo. Embora tal estratégia gere mais tráfego na rede do que quando usado um tempo de empréstimo alto, ela mostrou que o ataque perde um pouco de sua força apesar de ainda continuar trazendo prejuízos aos clientes legítimos.

Como medida de proteção contra os ataques de DoS ao servidor DHCP, o administrador pode usar uma das abordagens seguintes: (1) Realizar a configuração manual de endereços, garantindo que apenas os clientes legítimos recebam endereços IP válidos. Essa abordagem impede a ocorrência do ataque de DoS, pois dispensa o uso do servidor DHCP. Entretanto, não é adequada para redes de médio e grande porte ou redes cujos clientes ficam espalhados pelo *campus* de uma organização, pois exige que o administrador da rede esteja localmente conectado a cada cliente para poder realizar a sua configuração. (2) Configurar o servidor DHCP para atuar no modo de empréstimo por reserva, conforme descrito na seção 2.1 deste artigo. Essa é uma abordagem menos desgastante para o administrador de rede, pois não é preciso que o mesmo esteja no local do cliente para configurá-lo. Todavia, ainda há certo grau de esforço, pois é preciso que cada cliente tenha uma entrada, mapeando o seu endereço MAC a um endereço IP, previamente configurada no servidor DHCP. Logo, pela análise das duas abordagens apresentadas, pode-se concluir que a segunda tende a ser mais usada como medida de proteção do servidor contra ataques de DoS.

## 5. CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Neste trabalho apresentamos o DHCP, um importante protocolo para configuração de endereços IP em *hosts*, e sua vulnerabilidade a ataque de negação de serviço (DoS). Para comprovar tal vulnerabilidade, implementamos uma ferramenta de ataque – baseada em *Shell Script* – capaz de obter toda a faixa de endereços IP disponíveis em um servidor DHCP. Realizamos ataques e analisamos seus impactos sob a perspectiva de um cliente de rede legítimo, em duas situações: primeira, com o servidor configurado para realizar empréstimos com tempo de vida alto e, segunda, com o servidor configurado para realizar empréstimos com tempo de vida baixo. Observamos que os danos ao cliente legítimo foram maiores na primeira situação.

Em relação às ações a serem realizadas, propomos que os escopos DHCP sejam criados levando em conta que os empréstimos deverão ocorrer com tempo de vida baixo, isso como forma de minimizar os impactos de um ataque. Adicionalmente, sugerimos que quando possível, os administradores configurem seus servidores DHCP para operarem no modo de empréstimo por reserva, fazendo com que apenas aqueles *hosts* clientes cujos endereços MAC estejam previamente cadastrados consigam obter o empréstimo de um endereço IP.

Como perspectivas de trabalhos futuros, pretendemos refinar a implementação do *script* de ataque a fim de melhorar o seu funcionamento e utilizá-lo em outros cenários de rede. Adicionalmente, analisaremos se o uso de servidores redundantes pode ser adotado como estratégia para minimizar os impactos de ataques de negação de serviço ao DHCP.

## REFERÊNCIAS

ALECRIM, E. **Ataques DoS (Denial of Service) e DDoS (Distributed DoS)**. Disponibilizado em 09/10/2004 no endereço <http://www.infowester.com/col091004.php>. Acessado em 10/08/2008.

BLANK, A. G. **TCP/IP JumpStart-Internet Protocol Basics**. 2nd. Edition: Sybex, 2002.

COMER, D. E. **Internetworking with TCP/IP**. Vol. I. 3rd. Edition: Prentice Hall, 1995.

DROMS, R. **Dynamic Host Configuration Protocol**. RFC (*Request For Comments*) 2131. March 1997.

LAUFER, R. P. **Rastreamento de Pacotes IP contra Ataques de Negação de Serviço**. Dissertação de Mestrado em Engenharia Elétrica. COPPE/UFRJ, 2005. Disponível em <http://www.gta.ufrj.br/ftp/gta/TechReports/Laufer05/Laufer05.pdf>. Acessado em 10/08/2008.

MIRKOVIC, J. et al. **Internet Denial of Service: Attack and Defense Mechanisms**. Prentice Hall PTR, 2004.

MOORE, D., VOELKER, G., SAVAGE, S. **Inferring Internet Denial-of-Service Activity**. p. 9-22. Proceedings of the 2001 USENIX Security Symposium, 2001.