UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO SOFTWARE LIVRE APLICADO A TELEMÁTICA

DANIEL GUGELMIN

ALTERNATIVAS AO PROTOCOLO ICMP PARA DIAGNÓSTICO DE ESTADOS DE *HOSTS* E VERIFICAÇÃO DE ROTAS UTILIZANDO SOFTWARE LIVRE

MONOGRAFIA

CURITIBA
2012

DANIEL GUGELMIN

ALTERNATIVAS AO PROTOCOLO ICMP PARA DIAGNÓSTICO DE ESTADOS DE *HOSTS* E VERIFICAÇÃO DE ROTAS UTILIZANDO SOFTWARE LIVRE

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Software Livre Aplicado a Telemática, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Msc. Lincoln Herbert Teixeira

CURITIBA
2012

RESUMO

GUGELMIN, Daniel. **ALTERNATIVAS AO PROTOCOLO ICMP PARA DIAGNÓSTICO DE ESTADOS DE *HOSTS* E VERIFICAÇÃO DE ROTAS UTILIZANDO SOFTWARE LIVRE**. 2012. 35 f. Monografia (Especialização em Software Livre Aplicado a Telemática) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

O propósito desta monografia é de pesquisar a razão pela qual é comum e desejável se bloquear o protocolo ICMP e encontrar alternativas em Software Livre para realizar as principais tarefas desse protocolo como o ping e o traceroute, fazendo testes em uma rede experimental e em uma rede em produção para se verificar se é realmente possível executar tais operações com a mesma eficiência se utilizando das ferramentas alternativas.

Palavras-chave: ICMP. TCP Syn. Ping. Traceroute. Software Livre.

ABSTRACT

GUGELMIN, Daniel. **ALTERNATIVES TO THE ICMP PROTOCOL FOR DIAGNOSIS OF STATES OF HOSTS AND VERIFICATION OF ROUTES USING FREE SOFTWARE.** 2012. 35 p. Monograph (Specialization in Free Software Applied to Telematics) - Post Graduation Program in Technology, Federal Technological University of Paraná. Curitiba, 2012.

The purpose of this monograph is to search the reason why it is common and desirable to block the ICMP protocol and to find alternatives using Free Software to perform the main activities of this protocol, such as the ping and the traceroute, executing tests in both an experimental and a prodution network to verify if it is really possible to run such operations as efficiently using the alternative tools.

Keywords: ICMP. TCP Syn. Ping. Traceroute. Free Software.

LISTA DE FIGURAS

LISTAGEM DE SAÍDAS DO TERMINAL

SUMÁRIO

1 INTRODUÇÃO

O protocolo de rede ICMP (*Internet Control Message Protocol)* permite a comunicação entre roteadores e hosts, para que identifiquem e relatem o estado de funcionamento de uma rede.

As ferramentas mais conhecidas que utilizam esse protocolo são o *ping,* que envia mensagens para um determinado *host* com o intuito de testar a sua conectividade, e o *traceroute* que mostra as rotas percorridas por um pacote até chegar ao seu destino. (SIQUEIRA, 2009)

Contudo com a proliferação dos ataques de negação de serviço (DDos) e muitas outras explorações de vulnerabilidades nos servidores conectados na rede, as mensagens do protocolo ICMP representam uma grande oportunidade para realizar ataques dessa natureza, e por causa disso é uma prática cada vez mais comum desabilitá-lo tornando assim o servidor mais seguro, porém necessitando de meios alternativos para verificação do estado de funcionamento na rede. (DEFRAWY, 2006)

1.1 OBJETIVO

Encontrar uma técnica ou ferramenta alternativa e segura, utilizando software livre, para verificar o estado de um *host* em uma rede e analisar a rota até ele em situações aonde o protocolo ICMP deve estar desativado por questões de segurança.

1.2 JUSTIFICATIVA

O protocolo ICMP nos proporciona funcionalidades imprescindíveis para a administração de servidores e sistemas, porém nos deixa vulneráveis a ataques de negação de serviços (DDos), e portanto se faz necessário o bloqueio do protocolo e também uma solução alternativa para não prejudicar a eficiência e confiabilidade dos sistemas.

1.3 ESTRUTURA DA MONOGRAFIA

A monografia começa com uma revisão bibliográfica sobre o protocolo ICMP e suas funcionalidades mais utilizadas (Item 2.1). A revisão segue levantando como os ataques de negação de serviço exploram o protocolo ICMP para derrubar os sistemas e a importância de bloquear esse protocolo para tornar os sistemas mais seguros (Item 2.2). Por fim são pesquisadas alternativas em Software Livre que permitam realizar as principais tarefas do ICMP de uma maneira segura e eficiente (Item 2.3).

A parte seguinte da pesquisa consiste em um trabalho prático experimental começando pela montagem uma rede simples e realização das tarefas de verificação de estado utilizando as mensagens ICMP e coletando os resultados. Em sequência o protocolo ICMP é bloqueado e feito testes para comprovar que as operações utilizando o ICMP não podem ser realizadas. Então são aplicadas as soluções alternativas encontradas analisando se elas conseguem realizar as tarefas de verificação de status (ex.: ping) e analise da rota até ele (ex.: traceroute) com a mesma eficiência que utilizando o protocolo ICMP (Item 3.1). Assim que os testes com a rede experimental terminam as soluções são aplicadas em um ambiente real de produção para que a sua utilização prática seja analisada (Item 3.2).

Após a coleta de todos os dados da parte experimental é feito um relatório constando quais as aplicações em Software Livre podem ser utilizadas de maneira alternativa ao protocolo ICMP para realizar as verificações de estados e traçar as rotas até os *hosts* e quais as suas eficiências nessa tarefa (Item 3.3).

2 REFERENCIAL TEÓRICO

Nessa seção são apresentados detalhes introdutórios do protocolo ICMP, informações sobre como os ataques de negação de serviço o exploram para obter sucesso e ao final são apresentadas algumas alternativas em Software Livre para permitir o uso das funcionalidades do ICMP de uma maneira muito mais segura.

2.1 PROTOCOLO ICMP

O protocolo ICMP, do inglês Internet Control Message Protocol, é pertencente à suíte de protocolos TCP/IP e tem como um objetivo geral fornecer relatórios de erros e estados para o requisitante.

O protocolo IP em si já possui um mecanismo de detecção de erros em que através de um *checksum* de cabeçalho de cada datagrama que é criado pelo host de origem e verificado pelo host de destino se ocorrer alguma divergência o datagrama é simplesmente descartado sem qualquer processamento adicional.

Contudo para se detectar erros não específicos só a pacotes individuais mas também na rede como um todo, gerando informações de controle, o protocolo ICMP tem um papel fundamental para detectar falhas em roteadores ou em um host específico por exemplo. Mas apesar da funcionalidade específica dentro do conjunto TCP/IP, o protocolo IP e o ICMP são co-dependentes sendo que o IP usa o ICMP quando envia uma mensagem de erro e o ICMP usa o IP para transportar as suas mensagens (COMER, 2006).

Na figura 1 se pode observar como uma mensagem ICMP é encapsulada em um datagrama IP:

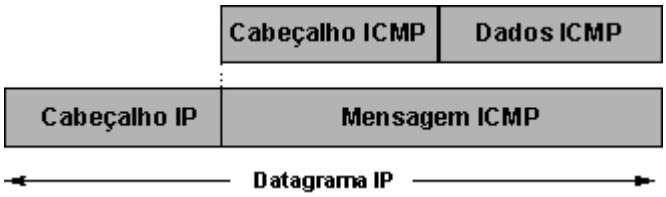

Figura 1 - Mensagem ICMP em um datagrama IP

Fonte: Adptado de **Redes, Guia Prático 2ª Ed** (MORIMOTO,2011)

Caso ocorra alguma situação prevista pelo ICMP, uma mensagem sobre a situação é preparada e entregue à camada IP, que a adiciona no seu cabeçalho e a envia para o emissor do datagrama com o qual a ocorrência aconteceu.

Vale ressaltar que o ICMP apenas indica o erro ou o estado do host ou da rede em questão e não oferece nenhum mecanismo para a correção do erro, ficando essa operação sob a responsabilidade da camada de aplicação .

A figura 2 representa o formato geral de uma mensagem ICMP:

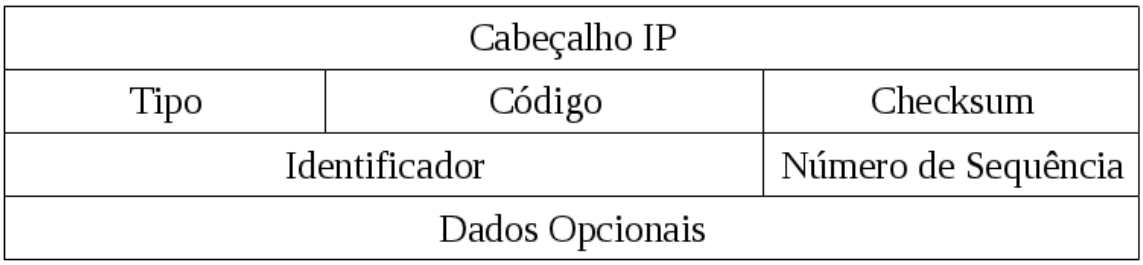

Figura 2 - Representação de uma mensagem ICMP

Fonte: Autoria própria baseada nas descrições de: **Redes de computadores e internet.** (COMER, 2006)

A mensagem ICMP é identificada pelo campo **Tipo** enquanto o campo **Código** é usado na especificação dos parâmetros da mensagem e finalmente o campo **checksum** corresponde a um código verificador calculado a partir da mensagem completa.

Para resumir:

“O Internet Control Message Protocol inclui mensagens sobre erros e mensagens informativas. O ICMP está integrado ao IP: O ICMP encapsula mensagens em IP para transmissão e o IP usa o ICMP para relatar problemas.” (COMER, Douglas E., 2006, p 280)

O ICMP possui uma lista significativa de mensagens que são classificadas em dois tipos: de erro e de consulta. A lista atualizada de todas as mensagens definidas no padrão está disponível no site oficial do órgão responsável pela coordenação da raiz DNS, do endereçamento IP e outros recursos dos protocolos de internet, o IANA (Internet Assigned Numbers Authority), no seguinte endereço: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml

Na figura 3 se pode observar a lista completa das mensagens ICMP:

Tipo	Nome
0	Echo Reply
1	Não utilizado
2	Não utilizado
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Não utilizado
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reservado (por Segurança)
20-29	Reservado (por Experimento de Força)
30	Tracerout
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41	Mensagens ICMP utilizadas por protocolos experimentais como o Seamoby
42-252	Reservado para uso futuro
253	RFC3692-style Experiment 1
254	RFC3692-style Experiment 2
255	Reservado para uso futuro

Figura 3: Lista de mensagens do protocolo ICMP

Fonte: Autoria própria baseada em http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml (Acesso em: 07 nov. 2012)

Embora a lista de mensagens seja bem extensa o trabalho se concentra nas mensagens *0 – Echo Reply* e *8 – Echo Request,* referentes ao comando ping, e à *30 – Traceroute* correspondendo à mensagem utilizada no comando traceroute.

2.1.1 Ping

O princípio do funcionamento das implementações do comando ping consiste em enviar de um host de origem uma mensagem do tipo *8 – Echo Request* para um determinado host de destino. Uma vez que o host de destino recebe a mensagem ele usa os mesmos dados da requisição para os campos identificador, número de sequência e dados opcionais e alterando principalmente o tipo da mensagem para *0 – Echo Reply* e a envia novamente para o destino, funcionando como uma confirmação de recebimento (MORIMOTO, 2011).

Na cultura popular existe uma analogia dessa operação com o jogo de “Ping-pong”, aonde a bola é lançada para o adversário (ping) e após recebê-la o adversário a devolve para o sacador (pong).

Dentro do campo “dados opcionais” da mensagem ICMP do ping geralmente é armazenado o tempo em que a mensagem foi enviada e o tempo de destino possibilitando assim se calcular o valor aproximado para a mensagem ir e voltar ao seu destino, sendo esse tempo conhecido como RTT (*Round Trip Time*). O valor do RTT é aproximado e pode não representar a real velocidade do tráfego porque como o ICMP possui uma prioridade baixa relativamente aos outros protocolos de transporte, se a rede estiver muito congestionada o tempo da mensagem será inferior do que um pacote real de transmissão realmente levaria. Por isso na maioria das implementações ao final da execução do comando são mostrados 3 tempos, o mínimo, médio e o máximo, sendo que quanto maior a diferença entre eles mais existem probabilidades de congestionamento ou problemas na rede. Existe também o tamanho do pacote (geralmente são utilizados pacotes pequenos para que o processo seja mais ágil) e o campo TTL e que funciona como um prazo de validade de cada pacote: a cada roteador que o pacote passar o valor do TTL é decrementado em uma unidade. O valor máximo do TTL é de 255 e quando o valor chegar a zero o pacote é descartado (COMER, 2006).

Na listagem 1 se pode observar a execução da implementação do ping no Linux:

```
# ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=53 time=67.5 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=53 time=70.8 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=53 time=64.2 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=53 time=63.8 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=53 time=66.4 ms
64 bytes from 8.8.8.8: icmp_req=6 ttl=53 time=71.9 ms
64 bytes from 8.8.8.8: icmp_req=7 ttl=53 time=67.2 ms
64 bytes from 8.8.8.8: icmp_req=8 ttl=53 time=64.4 ms
64 bytes from 8.8.8.8: icmp_req=9 ttl=53 time=64.8 ms
64 bytes from 8.8.8.8: icmp_req=10 ttl=53 time=63.3 ms
64 bytes from 8.8.8.8: icmp_req=11 ttl=53 time=63.2 ms
64 bytes from 8.8.8.8: icmp_req=12 ttl=53 time=61.5 ms
64 bytes from 8.8.8.8: icmp_req=13 ttl=53 time=61.8 ms
64 bytes from 8.8.8.8: icmp_req=14 ttl=53 time=62.9 ms
64 bytes from 8.8.8.8: icmp_req=15 ttl=53 time=67.3 ms
^C
--- 8.8.8.8 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14021ms
rtt min/avg/max/mdev = 61.558/65.454/71.909/2.976 ms
```

Listagem 1 - Exemplo dos resultados gerados pelo ping convencional

Observa-se que 15 pacotes ICMP com 64 bytes foram enviados para o *host* 8.8.8.8.

O número de roteadores que o pacote passou foram 11 (TTL Inicial 64-53 TTL Final) roteadores. Pela estatísticas percebe-se que 15 pacotes foram enviados e nenhum foi perdido e que o tempo mínimo foi de 61,558ms, médio 65,454 e máximo de 71,909.

2.1.1 Traceroute

O conceito do *traceroute* visa permitir ao usuário conhecer o caminho percorrido pelos seus pacotes até o destino. Para isso ele se utiliza do campo TTL que representa o tempo de vida do pacote. Como para cada roteador pelo qual o pacote passa o valor do TTL é decrementado em uma unidade e quando o valor for igual a zero o roteador descarta o datagrama e envia uma mensagem ICMP do tipo *11 – Tempo excedido*, a implementação envia diversos datagramas em ordem sequencial para um determinado destino começando com um TTL igual a 1 e espera

pela resposta. Quando o primeiro pacote chega ao primeiro roteador ele decrementa o valor do TTL (passando de 1 para 0) e renomeia a mensagem de tempo excedido e como a mensagem ICMP viaja em um datagrama IP o traceroute pode extrair o endereço IP de origem e anunciar o endereço do primeiro roteador do caminho até o destino original. Em seguida é enviado um segundo datagrama com o TTL com o valor 2. O primeiro roteador decrementa esse valor para 1 e ao chegar no segundo roteador o valor é novamente decrementado chegando novamente em 0 fazendo com o que o segundo roteador também envie um datagrama com a mensagem de tempo excedido e o programa do traceroute consegue capturar o ip do segundo roteador. Continuando ele envia o datagrama com o TTL em 3 e todo o processo se repete até que o que o endereço de destino retorne o datagrama significando que o destino foi alcançado que e todos os endereços pelo qual os pacotes passaram foram relatados (MORIMOTO, 2011). Na listagem 2 se tem um exemplo de funcionamento da implementação do Linux do traceroute:

```
# traceroute -n -w 2 -q 2 -m 30 8.8.4.4:

traceroute to 8.8.4.4 (8.8.4.4), 30 hops max, 52 byte packets
 1  192.168.0.254  1.106 ms  1.083 ms
 2  139.97.9.38  12.177 ms  12.484 ms
 3  139.97.9.37  38.253 ms  11.881 ms
 4  139.97.6.250  11.863 ms  11.574 ms
 5  213.192.191.53  12.129 ms  12.160 ms
 6  213.192.184.45  18.793 ms  19.304 ms
 7  74.125.50.145  19.332 ms  18.791 ms
 8  209.85.250.192  19.104 ms  18.361 ms
 9  209.85.248.132  47.524 ms  47.942 ms
10  216.239.48.53  47.272 ms  46.593 ms
11  * *
12  8.8.4.4  47.425 ms  46.619 ms
```

Listagem 2 - Exemplo dos resultados gerados pelo traceroute tradicional

2.2 ATAQUES DE NEGAÇÃO DE SERVIÇO ATRAVÉS DO ICMP

Junto com a simplicidade e todas as excelentes funcionalidades do protocolo ICMP vem junto também um grande risco e falta de segurança em suas operações fazendo com que ele possa ser utilizado de diversas formas como ferramenta para ataques maliciosos contra redes e servidores.

Pela facilidade de acesso ao uso do protocolo ICMP é muito confortável para o atacante realizar um ataque de negação de serviço ou a interceptação de mensagens. Dentre os muitos possíveis tipos de ataques seguem abaixo alguns exemplos (KAUSHIK, 2010):

- ICMP PING flood attack: Esse é um ataque clássico aonde um host é alvejado com uma quantidade infinitamente maior do que ele é capaz de processar de mensagens ICMP do tipo *08-Echo Reques*t, causando congestionamento na rota e também sobrecarga no host.

- Multiplicação de pacotes (ou ICMP Smurf): Um atacante envia mensagens 8-Echo Request falsas para endereços broadcast de redes vulneráveis. Todos os hosts dessas redes passam a enviar mensagens *0-Echo Reply* para a vítima, consumindo bastante banda de conexão podendo provocar uma negação de serviço pelo excesso de tráfego.

- ICMP DoS Attack (Denial of Service): O invasor pode forjar tanto a mensagem *11-Tempo excedido* quanto *03-Destino não alcançável* enviando para o host de origem ou destino (ou os dois ao mesmo tempo) resultando que a conexão seja terminada imediatamente. Já a mensagem *05-Redirect* também pode ser forjada fazendo com que os pacotes que teriam um *host* como destino possam ser redirecionadas para um host do invasor, roubando assim informações.

- **Varredura ICMP:** Essa técnica não é um ataque direto à rede mas definitivamente é uma ameaça de segurança. Fazendo uma varredura utilizando as mensagens do protocolo o invasor pode obter informações sobre hosts ativos e então à partir dessas informações realizar ataques aos hosts encontrados. A técnica tem seu funcionamento simples e tem como objetivo usar a funcionalidade do comando ping (*Echo request* + *Echo Reply*) disparando essas mensagens para todos os hosts de uma determinada rede e recebendo a confirmação dos *hosts* que estão ativos.

Para mitigar o risco dos ataques através do protocolo ICMP é uma prática cada vez mais comum restringir o seu uso bloqueando parcialmente ou totalmente o uso das ferramentas como *ping* e *traceroute* tornando as redes e os hosts mais seguros porém sem as funcionalidades interessantes que as mensagens ICMP podem oferecer.

2.3 ALTERNATIVAS EM SOFTWARE LIVRE AO ICMP

Desfrutar de um sistema o mais seguro possível e que ao mesmo tempo forneça as funcionalidades como o ping e o traceroute é algo desejável em um ambiente tão hostil das redes públicas globais de hoje em dia. Uma das soluções mais eficientes de hoje é de utilizar os pacotes SYN do protocolo TCP ao invés das mensagens ICMP. O princípio é extremamente simples e ao se enviar o pacote SYN para uma determinada porta o host de destino pode responder com um SYN|ACK (significando que está aberto para conexões) ou um RST (significando que está fechado para conexões). A grande vantagem desse método é que essa é uma operação elementar do protocolo TCP e que não necessariamente abre uma conexão entre os hosts até esse ponto. Em seguida é abordado como as ferramentas como nmap, hping3 e tcptraceroute exploram esse conceito e como elas podem representar uma alternativa interessante e mais segura ao uso das mensagens ICMP.

2.3.1 Nmap

O Nmap ou “*Network Mapper”* é uma ferramenta de código aberto para exploração de rede e auditoria de segurança e foi criada para possibilitar a varredura de redes amplas, embora também funcione muito bem contra *hosts* individuais. E é justamente a sua possibilidade de escanear *hosts* específicos que é explorada nessa seção porque é essa funcionalidade que permite substituir o uso do tradicional *“ping”* implementado utilizando o protocolo ICMP. (Disponível em <http://nmap.org/>, acesso em: 07 nov. 2012)

O comportamento padrão do nmap para a operação de verificação de estado de um host (*ping*) é de enviar tanto uma mensagem ICMP (*8 – Echo Request*) quanto um TCP SYN. Esse comportamento pode ser alterado se utilizando o comando *nmap* ***-PS*** *<endereço ip ou nome do host>.* O comando anterior utiliza somente o TCP SYN para realizar a operação do ping e os resultados são bem completos pois além de retornar se o host consultado está ativo ou não ele

também retorna quais as portas e tipos de serviços estão disponíveis. Na listagem 3 segue a saída obtida com o comando:

```
    #nmap -PS www.google.com.br

    Starting Nmap 5.21 ( http://nmap.org ) at 2012-11-21 00:53 BRST

    Nmap scan report for www.google.com.br (177.99.189.232)

    Host is up (0.0085s latency).

    Hostname www.google.com.br resolves to 16 IPs. Only scanned
177.99.189.232

    rDNS record for 177.99.189.232: googlecom232.static.host.gvt.net.br

    Not shown: 997 filtered ports

    PORT    STATE SERVICE
    80/tcp  open  http
    443/tcp open  https
    554/tcp open  rtsp

    Nmap done: 1 IP address (1 host up) scanned in 4.57 seconds
```

Listagem 3 - Exemplo dos resultados gerados pelo Nmap

2.3.2 Hping3

Hping3 é outra ferramenta livre que possui uma comandos e saídas muito semelhantes às implementações originais das ferramentas de ping, porém ela é muito mais completa e é capaz de fazer testes de estado utilizando o protocolo TCP, através de mensagens SYN, ao invés de usar apenas o ICMP. (Disponível em <http://www.hping.org/>, Acesso em: 07 nov. 2012)

Utilizando-se a opção -S na sintaxe a operação de ping é realizada utilizando o protocolo TCP. Na listagem 4 se tem um exemplo de seu uso:

```
# hping3 -S -p 80 www.google.com.br

HPING www.google.com.br (wlan0 74.125.234.120): S set, 40 headers + 0 data
bytes
len=44 ip=74.125.234.120 ttl=54 id=17752 sport=80 flags=SA seq=0 win=62920
rtt=59.0 ms
len=44 ip=74.125.234.120 ttl=54 id=17752 sport=80 flags=SA seq=1 win=62920
rtt=63.7 ms
len=44 ip=74.125.234.120 ttl=54 id=17752 sport=80 flags=SA seq=2 win=62920
rtt=83.4 ms
len=44 ip=74.125.234.120 ttl=54 id=17752 sport=80 flags=SA seq=3 win=62920
rtt=60.9 ms
len=44 ip=74.125.234.120 ttl=54 id=17752 sport=80 flags=SA seq=4 win=62920
rtt=71.4 ms
^C

--- www.google.com.br hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 59.0/67.7/83.4 ms
```

Listagem 4 - Exemplo dos resultados gerados pelo Hping3

Pode-se notar que embora utilizando o protocolo TCP os resultados são muito próximos aos obtidos com o ping por ICMP o que a torna uma ferramenta muito interessante.

2.3.4 TCPTraceroute

O tcptraceroute é uma ferramenta livre, licenciada pela GPL v2, que possui a mesma funcionalidade que o tradicional traceroute porém utilizando apenas pacotes TCP. Enquanto o traceroute original utiliza por padrão mensagens ICMP para rastrear o caminho percorrido pelos pacotes até o destino, o tcptraceroute envia os pacotes TCP SYN e por isso é capaz de executar a operação de rota com sucesso em ambientes aonde o protocolo ICMP está desativado por motivos de segurança. Conforme mencionado anteriormente o fato de se usar mensagens TCP SYN significa que não necessariamente é gerada uma conexão TCP/IP completa e sim uma técnica conhecida como “half-open scanning” em que o host de origem envia um TCP SYN e o destino retorna um SYN|ACK (host ativo) ou um RST (host fechado) e se para por aí, sem efetuar o chamado *three-way handshake* que estabelece a conexão. (TOREN, 2012).

A sintaxe e a saída é muito similar às implementações do traceroute que utilizam o protocolo ICMP. Abaixo segue uma demonstração na listagem 5 do tcptraceroute:

```
    # tcptraceroute www.google.com.br

    Selected device wlan0, address 192.168.8.130, port 56450 for outgoing
packets

    Tracing the path to www.google.com.br (177.99.189.231) on TCP port 80
(www), 30 hops max

    1  192.168.8.8  1.244 ms  2.400 ms  1.371 ms
    2  192.168.25.1  2.002 ms  1.751 ms  1.686 ms
    3  gvt-l0.b4.cta.gvt.net.br (177.42.104.1)  6.398 ms * *
    4  corporativo134.static.gvt.net.br (200.139.125.134)  7.863 ms  5.180
ms  5.439 ms
    5  gvt-te-0-0-4-0-rc02.cta.gvt.net.br (187.115.212.22)  13.771 ms
7.708 ms  11.086 ms
    6  gvt-te-0-1-0-0.rc03.cta.gvt.net.br (189.59.247.41)  7.736 ms
12.816 ms  11.864 ms
    7  googlecom231.static.host.gvt.net.br (177.99.189.231) [open]  6.091
ms  8.069 ms  6.762 ms
```

Listagem 5 - Exemplo dos resultados gerados pelo TCPTraceroute

3 IMPLEMENTAÇÃO

Na parte experimental é implementada uma rede simples e realizadas as tarefas de verificação de estado utilizando as mensagens ICMP e coletando os resultados. Em sequência o protocolo ICMP é bloqueado e feitos testes para comprovar que as operações utilizando o ICMP não podem ser realizadas. Então são aplicadas as soluções alternativas encontradas analisando se elas conseguem realizar as tarefas de verificação de status (ex.: ping) e analise da rota até ele (ex.: traceroute) com a mesma eficiência que utilizando o protocolo ICMP. Por fim é feito um teste simples para se verificar a diferença aproximada em operações de ping utilizando o protocolo ICMP e os pacotes TCP Syn.

3.1 TESTES DAS SOLUÇÕES EM UMA REDE EXPERIMENTAL

A rede experimental consiste em 2 hosts, conectados atráves de um ponto de acesso, sendo o primeiro de origem aonde as ferramentas são aplicadas e o host de destino aonde o protocolo ICMP é bloqueado, através do firewall iptables,

e aonde as soluções propostas são testadas. O host de origem possui o ip 10.0.0.154 e o host de destino possui o ip 10.0.0.155. Na figura 4 se tem um diagrama da estrutura da rede:

Figura 4 - Estrutura da rede experimental

Fonte: Autoria própria

Primeiramente é executado o ping normal entre eles para verificar se a conexão está configurada corretamente conforme segue na listagem 6:

```
# ping 10.0.0.155

PING 10.0.0.155 (10.0.0.155) 56(84) bytes of data.
64 bytes from 10.0.0.155: icmp_req=1 ttl=64 time=0.485 ms
64 bytes from 10.0.0.155: icmp_req=2 ttl=64 time=0.457 ms
64 bytes from 10.0.0.155: icmp_req=3 ttl=64 time=0.459 ms
64 bytes from 10.0.0.155: icmp_req=4 ttl=64 time=0.420 ms
64 bytes from 10.0.0.155: icmp_req=5 ttl=64 time=0.465 ms
64 bytes from 10.0.0.155: icmp_req=6 ttl=64 time=0.459 ms
64 bytes from 10.0.0.155: icmp_req=7 ttl=64 time=0.462 ms
64 bytes from 10.0.0.155: icmp_req=8 ttl=64 time=0.424 ms
64 bytes from 10.0.0.155: icmp_req=9 ttl=64 time=0.464 ms
64 bytes from 10.0.0.155: icmp_req=10 ttl=64 time=0.484 ms
^C
--- 10.0.0.155 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8998ms
rtt min/avg/max/mdev = 0.420/0.457/0.485/0.035 ms
```

Listagem 6 - Rede experimental - Resultado do ping para verificar se a conexão está funcionando

Como visto na listagem 6 a conectividade entre os hosts está funcionando corretamente pois 10 pacotes ICMP com 64 bytes foram enviados para o host 10.0.0.155 e pelas estatísticas se pode notar que os 10 pacotes foram enviados corretamente e que o tempo mínimo foi de 0,420ms, médio 0,457 e máximo de 0,485.

Agora é aplicado o bloqueio do protocolo ICMP no destino se utilizando o firewall iptables, conforme listagem 7:

```
# iptables -A INPUT -s 0.0.0.0/0 -p icmp -j DROP
```

Listagem 7 - Rede Experimental - Comando para bloquear o protocolo ICMP no destino

O teste de conectividade é repetido para verificar se o protocolo ICMP realmente foi bloqueado, conforme listagem 8:

```
# ping  10.0.0.155
PING 10.0.0.155 (10.0.0.155) 56(84) bytes of data.
^C
--- 10.0.0.155 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 8999ms
```

Listagem 8 - Rede experimental - Teste para verificar se o ICMP realmente foi bloqueado

Os resultados mostram que 10 pacotes foram transmitidos e que 100% deles foram perdidos, significando que o protocolo ICMP foi bloqueado com sucesso.

3.1.1 Nmap na rede experimental bloqueada

O primeiro teste feito com o ICMP bloqueado será feito com a ferramenta nmap:

```
# nmap -PS 10.0.0.155

Starting Nmap 5.00 ( http://nmap.org ) at 2012-12-03 17:32 BRST
Interesting ports on 10.0.0.155:
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 08:00:27:F8:54:F6 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

Listagem 9 - Rede Experimental - Resultado Nmap

Mesmo com o protocolo ICMP bloqueado, o nmap atráves dos pacotes TCP Syn foi capaz de identificar que o host 10.0.0.155 está ativo e que as portas 22, 80, 111 estão abertas.

3.1.2 Hping3 na rede experimental bloqueada

Agora o teste é feito se utilizando a ferramenta hping3:

```
    # hping3 -S -p 80 10.0.0.155

    HPING 10.0.0.155 (wlan0 10.0.0.155): S set, 40 headers + 0 data bytes
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840
rtt=0.4 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840
rtt=0.4 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840
rtt=0.4 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840
rtt=0.6 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=5840
rtt=0.4 ms
    ^C
    --- 10.0.0.155 hping statistic ---
    10 packets transmitted, 10 packets received, 0% packet loss
    round-trip min/avg/max = 0.4/0.5/0.6 ms
```

Listagem 10 - Rede Experimental - Resultado Hping3

Pode-se observar que o hping3 foi capaz de executar a operação de ping e ofereceu uma saída muito similar ao da obtida pelo comando ping tradicional do Linux. Nota-se também que foram transmitidos 10 pacotes com sucesso e pelas estatísticas o tempo mínimo foi de 0,400ms, médio 0,500ms e máximo de 0,600ms, o que representa valores muito aproximados aos dos obtidos pelo ping convencional.

3.1.3 TCPTraceroute na rede experimental bloqueada

Na rede experimental bloqueada é utilizado o comando traceroute convencional para o host de destino 10.0.0.155:

```
    # traceroute -I 10.0.0.155

    traceroute to 10.0.0.155 (10.0.0.155), 30 hops max, 60 byte packets
     1  * * *
     2  * * *
     3  * * *
     4  * * *
     5  * * *
     6  * * *
     7  * * *
     8  * * *
     9  * * *
    10  * * *
    11  * * *
    12  * * *
    13  * * *
    14  * * *
    15  * * *
    16  * * *
    17  * * *
    18  * * *
    19  * * *
    20  * * *
    21  * * *
    22  * * *
    23  * * *
    24  * * *
    25  * * *
    26  * * *
    27  * * *
    28  * * *
    29  * * *
    30  * * *
```

Listagem 11 - Rede Experimental - Resultado traceroute tradicional

Observa-se na listagem 11 que por o protocolo ICMP estar bloqueado não foi possível traçar a rota até o destino.

Agora é utilizada a ferramenta tcptraceroute:

```
    # tcptraceroute 10.0.0.155

    Selected device wlan0, address 10.0.0.149, port 55551 for outgoing
packets
    Tracing the path to 10.0.0.155 on TCP port 80 (www), 30 hops max
     1  10.0.0.155 [open]  4.005 ms  0.294 ms  0.143 ms
```

Listagem 12 - Rede Experimental - Resultado TCPTraceroute

Com a ferramenta tcptraceroute na listagem 12 foi possível traçar a rota corretamente, mesmo com o protocoloco ICMP bloqueado no destino, por conta dessa ferramenta utilizar os pacotes TCP Syn para a operação.

3.1.4 Comparação de velocidade entre o ping convencional e o hping3 na rede experimental

O último teste na rede experimental é para verificar a diferença de velocidade entre o método convencional de ping , utilizando o protocolo ICMP, e o hping3, que utiliza os pacotes TCP Syn como padrão.

Primeiramente a regra de firewall que bloqueia o protocolo ICMP no host de destino é removida com o seguinte comando:

```
# iptables -F
```

Listagem 13 - Rede Experimental - Comando para limpar as regras do firewall

Para garantir que o estado da rede seja igual para ambos os comandos eles foram executados em terminais diferentes no mesmo host de origem para o mesmo host de destino e ao mesmo tempo.

Na listagem 14 se tem os resultados para o ping convencional:

```
# ping 10.0.0.155
PING 10.0.0.155 (10.0.0.155) 56(84) bytes of data.
64 bytes from 10.0.0.155: icmp_req=1 ttl=64 time=0.410 ms
64 bytes from 10.0.0.155: icmp_req=2 ttl=64 time=0.581 ms
64 bytes from 10.0.0.155: icmp_req=3 ttl=64 time=0.486 ms
64 bytes from 10.0.0.155: icmp_req=4 ttl=64 time=0.479 ms
64 bytes from 10.0.0.155: icmp_req=5 ttl=64 time=0.324 ms
64 bytes from 10.0.0.155: icmp_req=6 ttl=64 time=0.597 ms
64 bytes from 10.0.0.155: icmp_req=7 ttl=64 time=0.320 ms
64 bytes from 10.0.0.155: icmp_req=8 ttl=64 time=0.363 ms
64 bytes from 10.0.0.155: icmp_req=9 ttl=64 time=0.628 ms
64 bytes from 10.0.0.155: icmp_req=10 ttl=64 time=0.493 ms
^C
--- 10.0.0.155 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8997ms
rtt min/avg/max/mdev = 0.320/0.468/0.628/0.106 ms
```

Listagem 14 - Rede Experimental - Tempo de resposta do ping convencional

Nos resultados se pode ver que que o tempo mínimo encontrado foi 0,320ms, o médio 0,468ms e o máximo 0,628ms.

Na listagem 15 se tem os resultados do hping3:

```
    # hping3 -S -p 80 10.0.0.155
    HPING 10.0.0.155 (wlan0 10.0.0.155): S set, 40 headers + 0 data bytes
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840
rtt=0.3 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840
rtt=0.9 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840
rtt=0.7 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840
rtt=0.3 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=5840
rtt=0.6 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=5840
rtt=0.5 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=5840
rtt=0.3 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=5840
rtt=0.8 ms
    len=44 ip=10.0.0.155 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=5840
rtt=0.5 ms
    ^C
    --- 10.0.0.155 hping statistic ---
    10 packets transmitted, 10 packets received, 0% packet loss
    round-trip min/avg/max = 0.3/0.5/0.9 ms
```

Listagem 15 - Rede Experimental - Tempo de resposta do Hping3

Nos resultados do hping3 se observa que o tempo mínimo encontrado foi 0,300ms, o médio 0,500ms e o máximo 0,900ms em 10 pacotes transmitidos. Comparando os tempos médios pode-se observar que o ping convencional teve o tempo de resposta aproximadamente 6,4% mais rápido que o hping3. A figura 5 ilustra a comparação dos resultados obtidos:

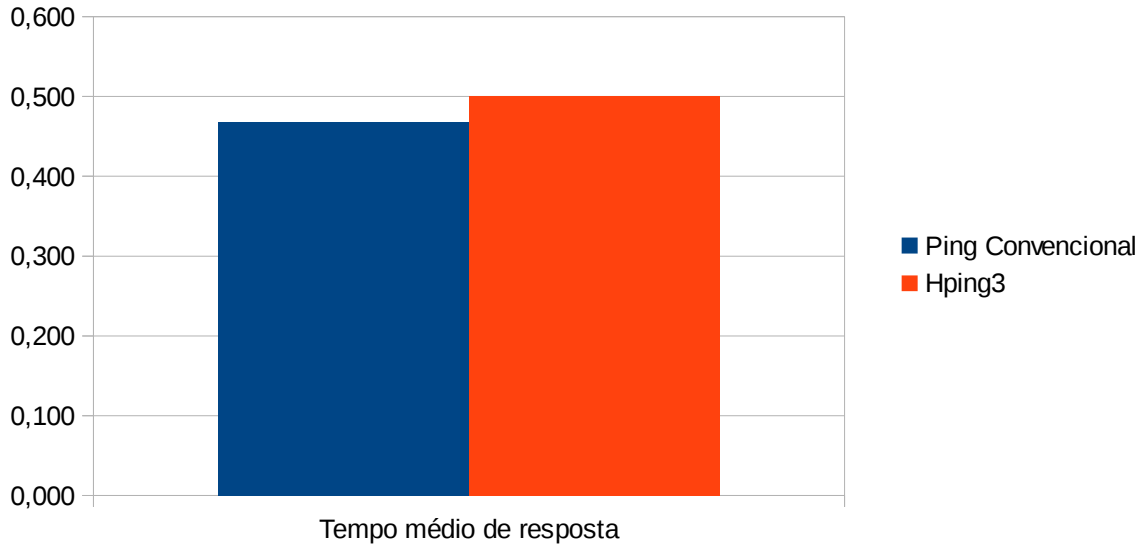

Figura 5 - Comparação do tempo médio de resposta entre o Ping convencional e o Hping3 na rede experimental
Fonte: Autoria própria

3.2 TESTES DAS SOLUÇÕES EM UMA REDE EM PRODUÇÃO

Para os testes em produção é utilizado o endereço de domínio da própria Univesidade Técnológica Federal do Paraná (www.utfpr.edu.br). Para começar o host é acessado normalmente através de um browser para garantir que ele esteja funcionando:

Figura 6 - Domínio da UTFPR funcionando corretamente

Fonte: www.utfpr.edu.br (Acesso em: 03 dez. 2012)

Na figura 6 se observa que o *host* está corretamente acessível. Em seguida, conforme listagem 16 é testado se o ping tradicional funciona para o host:

```
# ping www.utfpr.edu.br

PING www.utfpr.edu.br (200.19.73.171) 56(84) bytes of data.
^C
--- www.utfpr.edu.br ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9071ms
```

Listagem 16 - Rede em Produção – Resultado ping convencional

Pode-se notar que dos 10 pacotes transmitidos houve 100% dos pacotes foram perdidos, dando a falsa impressão de que existe algum problema com a conectividade do host, mas que na verdade o que ocorre é que o protocolo ICMP está bloqueado nesse host.

3.2.1 Nmap na rede de produção bloqueada

Continuando com os testes agora é aplicada a solução do nmap para verificar se o host está ativo ou não:

```
        # nmap -PS  www.utfpr.edu.br

        Starting Nmap 5.00 ( http://nmap.org ) at 2012-12-03 18:51 BRST
        Warning: Hostname www.utfpr.edu.br resolves to 3 IPs. Using
200.19.73.182.
        Interesting ports on 200.19.73.182:
        Not shown: 998 filtered ports
        PORT    STATE SERVICE
        80/tcp  open  http
        443/tcp open  https

        Nmap done: 1 IP address (1 host up) scanned in 11.13 seconds
```

Listagem 17 - Rede em Produção - Resultado Nmap

Observa-se que em 11,13 segundos o nmap constatou que o endereço testado está ativo (1 host up) e que possui as portas 80 e 443 abertas.

3.2.2 Hping3 na rede de produção bloqueada

Dando continuidade aos testes em produção agora é aplicada a ferramenta hping3 no mesmo host, conforme listagem 18:

```
    # hping3 -S -p 80 www.utfpr.edu.br

    HPING www.utfpr.edu.br (wlan0 200.19.73.182): S set, 40 headers + 0
data bytes
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=0
win=5840 rtt=59.5 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=1
win=5840 rtt=54.0 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=2
win=5840 rtt=57.4 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=3
win=5840 rtt=55.8 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=4
win=5840 rtt=51.5 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=5
win=5840 rtt=53.5 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=6
win=5840 rtt=53.3 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=7
win=5840 rtt=54.0 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=8
win=5840 rtt=76.9 ms
    len=44 ip=200.19.73.182 ttl=55 DF id=0 sport=80 flags=SA seq=9
win=5840 rtt=57.5 ms
    ^C
    --- www.utfpr.edu.br hping statistic ---
    10 packets transmitted, 10 packets received, 0% packet loss
    round-trip min/avg/max = 51.5/57.3/76.9 ms
```

Listagem 18 - Rede em Produção - Resultado Hping3

Conforme mostrado acima o hping3 conseguiu com exito executar a operação de ping no host www.utfpr.edu.br, que possui o protocolo ICMP bloqueado. Dos 10 pacotes transmitidos, 100% foram recebidos e sendo que o tempo mínimo encontrado foi 51,5ms, o médio 57,3ms e o máximo 76,9ms.

3.2.3 TCPTraceroute na rede de produção bloqueada

Para a operação de traceroute primeiramente é executado o comando tradicional implementado no linux no endereço de destino www.utfpr.edu.br:

```
    # traceroute www.utfpr.edu.br
    traceroute to www.utfpr.edu.br (200.19.73.182), 30 hops max, 60 byte
packets
     1  10.0.0.148 (10.0.0.148)  3.063 ms  3.974 ms  4.484 ms
     2  201-34-149-254.jvece702.dsl.brasiltelecom.net.br (201.34.149.254)
49.312 ms  53.589 ms  58.102 ms
     3  BrT-G1-1-1-ctme-pr-rotb-j01.brasiltelecom.net.br (177.2.196.184)
118.808 ms  119.789 ms  120.927 ms
     4  as10881.pr.ptt.br (200.219.140.3)  85.019 ms  87.378 ms  91.039 ms
     5  cefetpr-ge-1-3-r2.pop-pr.rnp.br (200.19.74.110)  98.747 ms
102.340 ms  106.906 ms
     6  fw1.cefetpr.br (200.17.97.41)  113.123 ms  55.086 ms  54.746 ms
     7  * * *
     8  * * *
     9  * * *
    10  * * *
    11  * * *
    12  * * *
    13  * * *
    14  * * *
    15  * * *
    16  * * *
    17  * * *
    18  * * *
    19  * * *
    20  * * *
    21  * * *
    22  * * *
    23  * * *
    24  * * *
    25  * * *
    26  * * *
    27  * * *
    28  * * *
    29  * * *
    30  * * *
```

Listagem 19 - Rede em Produção - Resultado traceroute

Nota-se que do nó 1 até o 6 a operação do traceroute tradicional utilizando o protocolo ICMP transcorre sem problemas, porém a partir do sétimo nó a leitura se perde e mesmo continuando o procedimento até os pacotes com ttl 30 nenhuma informação da rota é obtida mais, representando que o próximo *host* do caminho possui um bloqueio das mensagens ICMP.

Agora é utilizado o tcptraceroute para o mesmo domínio:

```
    # tcptraceroute www.utfpr.edu.br
    Selected device wlan0, address 10.0.0.155, port 46208 for outgoing
packets
    Tracing the path to www.utfpr.edu.br (200.19.73.182) on TCP port 80
(www), 30 hops max
     1  10.0.0.148  2.370 ms  2.277 ms  2.304 ms
     2  201-34-149-254.jvece702.dsl.brasiltelecom.net.br (201.34.149.254)
44.068 ms  45.484 ms  42.715 ms
     3  BrT-G1-1-1-ctme-pr-rotb-j01.brasiltelecom.net.br (177.2.196.184)
55.449 ms  53.646 ms  50.907 ms
     4  as10881.pr.ptt.br (200.219.140.3)  56.154 ms  73.382 ms  53.087 ms
     5  cefetpr-ge-1-3-r2.pop-pr.rnp.br (200.19.74.110)  51.645 ms  51.913
ms  56.774 ms
     6  fw1.cefetpr.br (200.17.97.41)  53.151 ms  61.085 ms  54.409 ms
     7  200.19.73.182 [open]  53.035 ms  52.053 ms  54.583 ms
```

Listagem 20 - Rede em Produção - Resultado TCPTtraceroute

Percebe-se que utilizando o tcptraceroute a rota da origem ao destino é totalmente descrita sem a ocorrência de nunhum erro.

3.2.4 Comparação de velocidade entre o ping convencional e o hping3 na rede de produção

Para testar a diferença de velocidade entre o método convencional de ping, utilizando o protocolo ICMP, e o hping3, que utiliza os pacotes TCP Syn como padrão, o seguinte domínio é utilizado: www.google.com.br. Ele possui o protocolo ICMP habilitado e por isso é possível obter os resultandos tanto com o ping quanto com o hping3 (utlizando TCP Syn). Para garantir que o estado da rede seja igual para ambos os comandos, eles foram executados em terminais diferentes no mesmo host e ao mesmo tempo. Primeiro se tem os resultados do ping convencional:

```
    # ping www.google.com.br
    PING www.google.com.br (74.125.234.159) 56(84) bytes of data.
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=1
ttl=54 time=62.6 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=2
ttl=54 time=63.0 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=3
ttl=54 time=64.8 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=4
ttl=54 time=63.9 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=5
ttl=54 time=63.4 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=6
ttl=54 time=64.2 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=7
ttl=54 time=64.9 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=8
ttl=54 time=67.2 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=9
ttl=54 time=62.8 ms
    64 bytes from gru03s13-in-f31.1e100.net (74.125.234.159): icmp_req=10
ttl=54 time=60.4 ms
    ^C
    --- www.google.com.br ping statistics ---
    10 packets transmitted, 10 received, 0% packet loss, time 9011ms
    rtt min/avg/max/mdev = 60.407/63.752/67.203/1.706 ms
```

Listagem 21 - Rede em Produção - Tempo de resposta do ping convencional

Nos resultados acima se pode ver que que o tempo mínimo encontrado foi 60,407ms, o médio 63,752ms e o máximo 67,203.

Na listagem 22 se tem os resultados do hping3:

```
    # hping3 -S -p 80 www.google.com.br
    HPING www.google.com.br (wlan0 74.125.234.159): S set, 40 headers + 0
data bytes
    len=44 ip=74.125.234.159 ttl=54 id=6747 sport=80 flags=SA seq=0
win=14300 rtt=59.8 ms
    len=44 ip=74.125.234.159 ttl=54 id=6749 sport=80 flags=SA seq=1
win=14300 rtt=59.3 ms
    len=44 ip=74.125.234.159 ttl=54 id=6751 sport=80 flags=SA seq=2
win=14300 rtt=62.1 ms
    len=44 ip=74.125.234.159 ttl=54 id=6753 sport=80 flags=SA seq=3
win=14300 rtt=62.0 ms
    len=44 ip=74.125.234.159 ttl=54 id=6755 sport=80 flags=SA seq=4
win=14300 rtt=58.8 ms
    len=44 ip=74.125.234.159 ttl=54 id=6757 sport=80 flags=SA seq=5
win=14300 rtt=59.9 ms
    len=44 ip=74.125.234.159 ttl=54 id=6759 sport=80 flags=SA seq=6
win=14300 rtt=60.8 ms
    len=44 ip=74.125.234.159 ttl=54 id=6761 sport=80 flags=SA seq=7
win=14300 rtt=61.3 ms
    len=44 ip=74.125.234.159 ttl=54 id=6763 sport=80 flags=SA seq=8
win=14300 rtt=66.8 ms
    len=44 ip=74.125.234.159 ttl=54 id=6765 sport=80 flags=SA seq=9
win=14300 rtt=62.6 ms
    ^C
    --- www.google.com.br hping statistic ---
    10 packets transmitted, 10 packets received, 0% packet loss
    round-trip min/avg/max = 58.8/61.3/66.8 ms
```

Listagem 22 - Rede em Produção - Tempo de resposta do Hping3

Nos resultados do hping3 se pode notar que o tempo mínimo encontrado foi 58,800ms, o médio 61,300ms e o máximo 66,800ms.

Comparando os tempos médios pode-se observar que o ping convencional teve o tempo de resposta aproximadamente 4% mais lento que o hping3. Na figura 7 está um gráfico que representa os resultados:

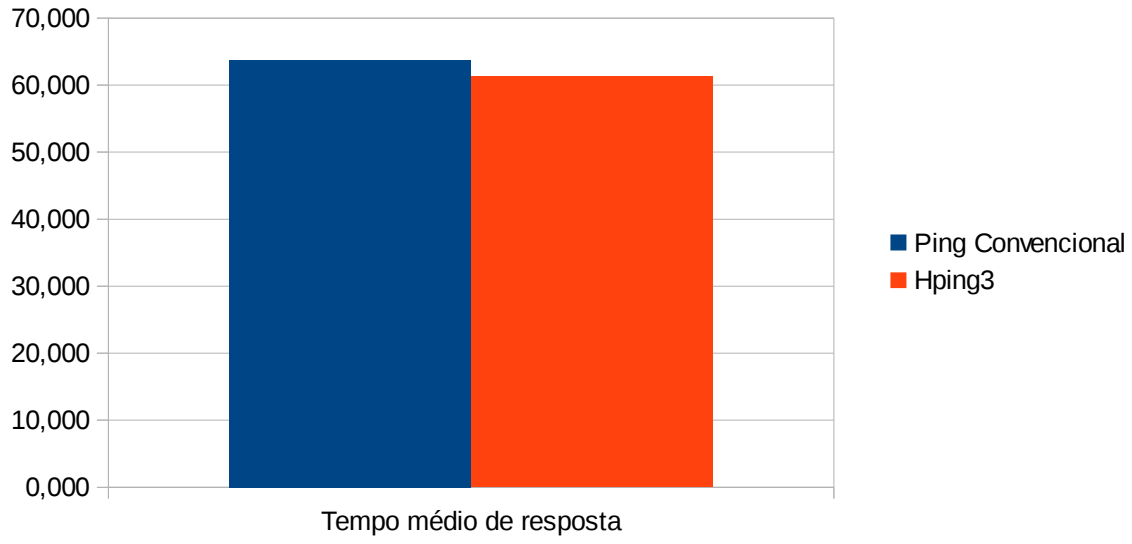

Figura 7 - Comparação do tempo médio de resposta entre o Ping convencional e o Hping3 na rede de produção
Fonte: Autoria própria

3.3 RELATÓRIO

Após a execução dos testes tanto no ambiente experimental quanto no ambiente de produção pode-se constatar:

- O bloqueio do protocolo ICMP nos servidores realmente prejudica o funcionamento das ferramentas tradicionais de ping e traceroute conforme detalhado nos items 3.1 e 3.2;

- Em ambos os ambientes se constatou que o nmap é uma ferramenta poderosa de verificação de estados de hosts e que além de conseguir operar usando apenas os pacotes TCP Syn ela forcece muito mais informações do que um ping convencional ofereceria, como a indicação de quais portas estão abertas para determinado host por exemplo (items 3.1.1 e 3.2.1).

- A ferramenta hping3 é uma alternativa perfeita ao ping tradicional porque nos testes foi comprovado que em ambientes aonde o protocolo ICMP esteja bloqueado ela consegue efetuar tranquilamente a operação de ping (Items 3.1.2 e 3.2.2), fornecendo ainda uma sintaxe e resultados muito similares ao que se está acostumado implementações do comando ping.

- A aplicação tcptraceroute foi capaz de executar as operações de traceroute tanto no ambiente experimental quanto no ambiente de produção com o protocolo ICMP bloqueado (Items 3.1.3 e 3.2.3) fornecendo uma sintaxe e resultados idênticos aos das implementações padrão.

- Através de um teste simples comparando a velocidade entre o ping convencional e o hping3 percebe-se uma diferença de aproximadamente 6,4% entre os dois métodos nos testes da rede experimental (Item 3.1.4) e de 4% na rede de produção (Item 3.2.4), o que nos indica que ao utilizar os pacotes TCP Syn os dados coletados referente aos tempos de resposta aproximados não diferem muito dos tempos obtidos com o protocolo ICMP e por isso podem ser utilizados, sem muita precisão, como referência.

4 CONCLUSÃO

Através do referencial teórico foi possível entender que os diversos ataques que exploram o protocolo ICMP são a razão pela qual é comum e desejável que esse protocolo seja bloqueado, e que os pacotes TCP Syn pela natureza de seu funcionamento podem ser utilizados como alternativa ao protocolo ICMP.

Nas atividades práticas, tanto na rede experimental quanto em produção, pode-se constatar que ao se bloquear o protocolo ICMP as ferramentas convencionais de ping e traceroute deixam de funcionar e que no entanto as ferramentas alternativas propostas, nmap, hping3 e tcptraceroute funcionam perfeitamente para essas atividades e inclusive proporcionam algumas funcionalidades a mais do que as encontradas nas ferramentas baseadas em mensagens ICMP.

Pode-se também, através das atividades práticas, considerar que os tempos de resposta obtidos pelas ferramentas que utilizam os pacotes TCP Syn são tão confiáveis quanto às que utilizam o ICMP.

5 REFERÊNCIAS BIBLIOGRÁFICAS

COMER, Douglas Earl; **Redes de computadores e internet.** Editora Bookman, São Paulo, 2006.

DEFRAWY, Karim El. **Optimal Filtering for DDoS Attacks.** ArXiv.org, 2006.

HPING. **Hping**. Disponível em <http://www.hping.org/>. Acesso em: 07 nov. 2012.

KAUSHIK, Atul Kant, **Network Forensic System for ICMP Attacks.** International Journal of Computer Applications (0975 – 8887) Volume 2 – No.3, Maio de 2010.

MORIMOTO, Carlos E.. **Redes, Guia Prático 2ª Ed**. GDH Press e Sul Editores, 2011.

NMAP. **Nmap ("Network Mapper").** Disponível em <http://nmap.org/>. Acesso em: 07 nov. 2012.

SIQUEIRA, Luciano Antonio Siqueira. **Certificação LPI-1**. Linux New Media do Brasil Ltda, 2009.

SIQUEIRA, Luciano Antonio Siqueira. **Certificação LPI-2**. Linux New Media do Brasil Ltda, 2009.

TOREN, Michael C. **Tcptraceroute - A traceroute implementation using TCP packets.** Disponível em <http://michael.toren.net/code/tcptraceroute/>. Acesso em: 07 nov. 2012.