UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
MESTRADO EM COMPUTAÇÃO APLICADA - PPGCA

TIAGO HEINRICH

CARACTERIZAÇÃO DE ATAQUES DRDOS MULTIPROTOCOLO

JOINVILLE

2018

TIAGO HEINRICH

CARACTERIZAÇÃO DE ATAQUES DRDOS MULTIPROTOCOLO

Dissertação submetida ao Programa de Pós-Graduação em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, para a obtenção do grau de Mestre em Computação Aplicada.

Orientador: Dr. Rafael Rodrigues Obelheiro
Coorientador: Dr. Nome do Co-Orientador

JOINVILLE

2018

Tiago Heinrich
Caracterização de Ataques DRDoS multiprotocolo/ Tiago Heinrich. – Joinville, 2018-
49 p. : il. (algumas color.) ; 30 cm.

Dr. Rafael Rodrigues Obelheiro

– Universidade do Estado de Santa Catarina - UDESC, 2018.

1. Tópico 01. 2. Tópico 02. I. Prof. Dr. xxxxx. II. Universidade do Estado de Santa Catarina. III. Centro de Ciências Tecnológicas. IV. identificação xxxx

CDU 02:121:005.7

Tiago Heinrich

Caracterização de Ataques DRDoS multiprotocolo

Esta dissertação foi julgada adequada para a obtenção do título de **Mestre em Computação Aplicada** área de de concentração em "Sistemas de Computação", e aprovada em sua forma final pelo Curso de Mestrado em Computação Aplicada do Centro de Ciências Tecnológicas da Universidade ddo Estado de Santa Catarina.

Banca Examinadora:

Rafael Rodrigues Obelheiro
Orientador

Professor
Charles Christian Miers

Professor
Guilherme Koslovski

Joinville, 10 de Dezembro de 2018

Dedico este trabalho aos meus familiares, amigos, colegas e professores que me acompanharam e me deram forças nessa magnífica trajetória.

AGRADECIMENTOS

Agradeço ao apoio dos meus queridos pais que, sempre estiveram ao meu lado e me auxiliaram nesta caminhada. Em especial agradeço o meu irmão, ao qual sempre este presente nestes anos de estudo na UDESC e compartilhou comigo esta jornada, tanto nos dias bons como nos dias ruins. Ao Prof. Dr. Rafael Rodrigues Obelheiro por ter me orientado e guiado ao longo deste período, e ter se tornando um amigo ao qual sempre lembrarei e espero ainda continuar convivendo, buscando ajudar mesmo nos problemas aos quais não estiveram relacionado com a pesquisa.

Sou grato também a Prof. Dr. Rebeca Schroeder Freitas pelos ensinamentos e trabalhos realizados na graduação da UDESC, ao qual contribui para o momento que estou agora.

Aos professores Dr. Guilherme Piegas Koslovski, Dr. Mauricio Aronne Pillon e Dr. Charles Christian Miers pelo apoio ao longo desta jornada e ensinamentos ao decorrer destes anos.

Sou grato também ao Departamento de Ciência da Computação (DCC) por ter contribuído com os laboratórios ao qual foram utilizados durante longas horas nas madrugadas para acabar trabalhos e experimentos. Também sou grato ao meu amigo Leonardo Rosa Rodrigues que sempre esteve presente colaborando para os trabalhos, e ajudando nos experimentos realizados durante as madrugadas no DCC, mas principalmente por sempre estar ao meu lado sem hesitar para ajudar. E ao Gustavo Diel que apesar de estarmos em períodos diferentes sempre buscou ajudar e estar presente.

Por fim, agradeço a todos aqueles colegas que estiveram presente na minha caminhada e que tiveram uma contribuição direta ou indireta com a minha caminhada durante este período, vocês tiveram uma contribuição para o momento que estou agora, sendo que sempre poderão contar comigo para auxilio, por fim um, Muito obrigado.

“"Learn the rules like a pro, so you can break them like an artist."”

Pablo Picasso

RESUMO

A Internet proporciona a conexão entre usuários que usufruem de diferentes serviços, por consequência a segurança computacional virou um fator de importância em decorrência das atividades realizadas neste ambiente. Uma problemática nos últimos anos são ataques *Distributed Reflection Denial of Service* (DRDoS), estes ataques visam explorar diferentes protocolos de rede e sistemas computacionais para realizar a amplificação de mensagens com o intuito de envia-las para uma vítima e esgotar recursos computacionais. O respectivo trabalho tem o objetivo de estudar este tipo de ataque em situações que diferentes protocolos são utilizados para a realização de um ataque, visando caracterizar ataques que explorem multiprotocolo.

Palavras-chaves: Ataques de Amplificação, Segurança de rede e Ataque de Negação de Serviço.

ABSTRACT

The Internet provides the connection between users who enjoy different services, consequently the computer security has become a factor of importance as a result of the activities who carried out in this environment. One problem in recent years is DRDoS attacks, these attacks aim to exploit different network protocols and computer systems to perform message amplification in order to send them to a victim and deplete computational resources.This work studies that type of attacks in situations that different protocols are used to carry out an attack, aiming to characterize attacks that exploit multiprotocol.

Keywords: Amplification Attacks, Network Security, and Denial of Service Attack.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

CCTV *Closed-Circuit Television Camera*

Chargen *Character Generator Protocol*

CFAA *Computer Fraud and Abuse Act*

CLDAP *Connection-less Lightweight Directory Access Protocol*

CPU *Central Processing Unit*

DNS *Domain Name System*

DNSSEC *Domain Name System Security Extensions*

DDoS *Distributed Denial of Service*

DRDoS *Distributed Reflection Denial of Service*

ESM *End System Multicast*

FTP *File Transfer Protocol*

HTTP *Hypertext Transfer Protocol*

ICMP *Internet Control Message Protocol*

IGMP *Internet Group Management Protocol*

IoT *Internet of Things*

IP *Internet Protocol*

ISP *Internet Service Provider*

ISPs *Internet Service Providers*

Kad *Kad network*

LDAP *Lightweight Directory Access Protocol*

mDNS *Multicast Domain Name System*

ML *Machine Learning*

NetBios *Network Basic Input/Output System*

NTP *Network Time Protocol*

PLATO *Programmed Logic for Automatic Teaching Operations*

P2P *Peer-to-peer*

QOTD *Quote of the Day*

RIPv1 *Routing Information Protocol*

SIP *Session Initiation Protocol*

SNMP *Simple Network Management Protocol*

SSDP *Simple Service Discovery Protocol*

SSH *Secure Shell*

TCP *Transmission Control Protocol*

TFTP *Trivial File Transfer Protocol*

UDP *User Datagram Protocol*

UDESC Universidade do Estado de Santa Catarina

UPnP *Universal Plug and Play*

XMAS *Christmas (Xmas) tree attack*

WTO *World Trade Organization*

LISTA DE SÍMBOLOS

$\approx$	Aproximação
#	Sinal numérico

SUMÁRIO

1 INTRODUÇÃO

Ataques ataque de negação de serviço DDoS estão presente na Internet há cerca de 20 anos (MANSFIELD-DEVINE, 2015). Nesses ataques um conjunto de máquinas envia tráfego para uma vítima de forma coordenada. Este volume de dados é responsável pela saturação de recursos computacionais na vítima, causando indisponibilidade de serviços e prejudicando clientes legítimos (NAZARIO, 2008).

Um tipo particular de ataque DDoS são os ataques distribuídos de negação de serviço por reflexão (*Distributed Reflection Denial of Service*, DRDoS), nos quais o tráfego de ataque não é enviado diretamente para a vítima, mas para um conjunto de intermediários, chamados de refletores (PAXSON, 2001). O atacante envia tráfego para um refletor usando como endereço *Internet Protocol* (IP) de origem o endereço da vítima, fazendo o refletor direcione o tráfego de resposta para a vítima e não de volta para o atacante. Ataques DRDoS oferecem as seguintes vantagens para um atacante (ROSSOW, 2014):

1. Fica mais difícil identificar a origem dos ataques, uma vez que o tráfego recebido pela vítima vem dos refletores, que são meros intermediários explorados inadvertidamente;

2. O tráfego refletido para a vítima geralmente é bem maior (em largura de banda) do que o tráfego enviado pelo atacante, pois é comum que as respostas sejam maiores que as requisições correspondentes. Esse efeito é conhecido como amplificação;

3. O uso simultâneo de múltiplos refletores permite que um ataque altamente distribuído seja efetuado a partir de um conjunto reduzido de máquinas.

Diversos protocolos podem ser explorados para ataques DRDoS, tais como *Domain Name System* (DNS), *Network Time Protocol* (NTP) e *Simple Service Discovery Protocol* (SSDP) (PROLEXIC, 2013; RYBA et al., 2015). Embora haja a predominância de protocolos de aplicação que adotam o *User Datagram Protocol* (UDP) como protocolo de transporte, ataques DRDoS também podem explorar o *Transmission Control Protocol* (TCP) (KÜHRER et al., 2014b).

Tendo em vista a relevância dos ataques DRDoS, um foco importante de pesquisa tem sido a análise e caracterização do tráfego associado a esses ataques, com vistas a compreender melhor o seu funcionamento na prática, e assim permitir uma

evolução dos mecanismos de defesa. Os trabalhos encontrados na literatura que abordam ataques DRDoS podem ser classificados em dois grupos. O primeiro grupo consiste de trabalhos que estudam um único protocolo, realizando uma caracterização dos ataques e métodos explorados, como pode ser visto em (ANAGNOSTOPOULOS et al., 2013; RUDMAN; IRWIN, 2015; BAIA, 2018; HEINRICH; LONGO; OBELHEIRO, 2017). O segundo grupo abrange trabalhos que abordam diversos protocolos (KÜHRER et al., 2014a; ROSSOW, 2014; THOMAS; CLAYTON; BERESFORD, 2017), verificando como tais protocolos estão sendo explorados e qual o fator de amplificação obtido pelos atacantes. Embora esses trabalhos englobem vários protocolos, eles consideram cada protocolo isoladamente.

Uma tendência recente em DRDoS tem sido a ocorrência de ataques multiprotocolo, ou seja, ataques que usam múltiplos protocolos simultaneamente contra uma mesma vítima (NETSCOUT; ARBOR, 2017). Esses ataques conseguem atingir volumes de tráfego próximos a 2 Tbps (DYN, 2018; SKOTTLER, 2018), mas ainda foram pouco explorados na literatura científica.

Este trabalho pretende então preencher essa lacuna por meio da análise e caracterização de tráfego de ataques DRDoS multiprotocolo. A ideia geral é usar tráfego coletado por um *honeypot* para investigar como esses ataques vem sendo conduzidos na prática, explorando questões como a duração e intensidade dos ataques, com que frequência eles ocorrem, quais protocolos são mais usados, e quem são as vítimas mais afetadas.

1.1 OBJETIVO

O objetivo geral do trabalho é analisar e caracterizar o tráfego de ataques DRDoS multiprotocolo coletado por um *honeypot*.

Esse objetivo geral desdobra-se nos seguintes objetivos específicos:

- Projetar e implementar um *honeypot* específico para tráfego DRDoS;
- Implantar o *honeypot* na rede da UDESC, e realizar uma coleta de dados de longa duração (6–9 meses);
- Analisar os dados coletados pelo *honeypot* sob a perspectiva de ataques DRDoS multiprotocolo.

Este trabalho adota a pesquisa aplicada quantitativa como método de pesquisa. A primeira etapa do trabalho consistiu de uma pesquisa bibliográfica, na qual foi efetuada a revisão de literatura, com destaque para a identificação dos protocolos mais relevantes em ataques DRDoS e como eles são explorados pelos atacantes.

A fase seguinte da pesquisa envolve procedimentos experimentais. Inicialmente, foi projetado e implementado um *honeypot* que pode ser usado (de forma controlada) como um refletor em ataques DRDoS, e que permite a coleta de dados sobre esses ataques. Esse *honeypot* já foi implantado na rede da Universidade do Estado de Santa Catarina (UDESC), e atualmente estã coletando dados. A última fase da pesquisa é a análise dos dados coletados por esse *honeypot*.

1.2 ESTRUTURA DO DOCUMENTO

Este estudo esta estruturado em cinco capítulos. O Capítulo 2 mostra a fundamentação teórica necessária para o entendimento do trabalho. O 3 apresenta uma descrição da problemática e proposta do trabalho. Por fim, o Capítulo 4 discute a implementação e os resultados parciais do trabalho até o momento, e o Capítulo 5 apresenta as considerações parciais.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma revisão de conceitos necessários ao entendimento do trabalho. A Seção 2.1 trata de ataques DDoS em geral, e a Seção 2.2 discute de forma mais específica ataques DDoS por reflexão. A Seção 2.3 apresenta os principais aspectos de *honeypots*.

2.1 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDOS)

Um ataque DDoS possui o objetivo de deixar sistemas computacionais e redes indisponíveis para os usuários, através da saturação de recursos dos respectivos. O ataque não tem a finalidade de invadir ou coletar informações dos usuários e sim impossibilitar o acesso de certo recursos. O ataque explora um conjunto de sistema para realizar a amplificação das consultas e encaminha-las para as vítimas (CERT.BR, 2016).

Um fator que contribui para a utilização deste tipo de ataque é a facilidade por trás da sua realização (considerando que a predominância dos ataques acaba explorando serviços que realizem conexões UDP, os atacantes só possuem a necessidade de realizar um *IP Spoofing*[1]), onde um usuário com pouco conhecimento possui a capacidade de realizar este tipo de ataque através da utilização de *scripts*. Por outro lado a prevenção já não apresenta a mesma facilidade, pois depende da cooperação dos *Internet Service Providers* (ISPs) para a realização de metidas preventivas contra os ataques ou até mesmo uma prevenção em tempo real para a minimização de danos a rede (BOSWORTH; KABAY; WHYNE, 2012).

A Figura 1 ilustra de forma simplificada um ataque DDoS. Um atacante, representado na figura pelo *master*, controla um conjunto de *hosts* intermediários, chamados de agentes. Esses agentes recebem comandos do *master* para enviar tráfego de ataque para uma ou mais vítimas. Em muitos casos, os agentes são *bots*, máquinas infectadas com *malware* que permite que elas sejam controladas à distancia, e o conjunto de agentes forma uma *botnet*. Em outros casos, os agentes são máquinas de voluntários que participam de campanhas de hacktivismo (MANSFIELD-DEVINE, 2015).

A Tabela 1 retrata a evolução dos ataques DDoS ao longo dos anos. A finalidade é a demonstrar qual o impacto que grandes ataques obtiveram ao decorrer dos anos e

[1] IP Spoofing visa modificar o cabeçalho IP com um endereço de origem falso, desta forma ao realizar o ataque os pacotes serão enviados para a vítima (CERT, 1996).

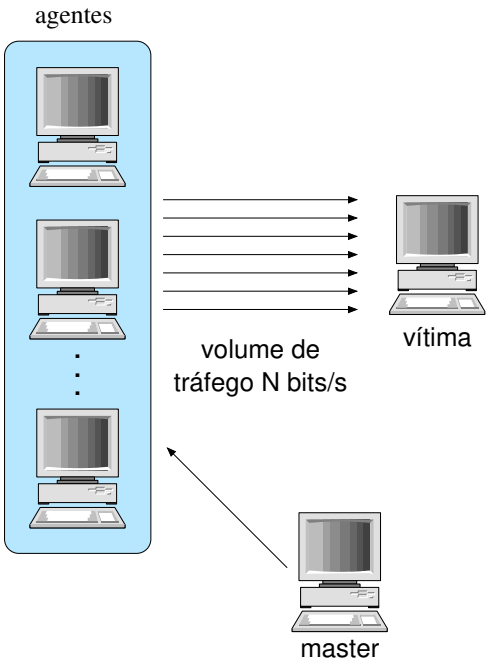

Figura 1 – Representação de uma infraestrutura para a realização de ataques DDoS.

Fonte: Autor.

quais os métodos explorados para a sua realização (REVUELTO; MEINTANIS; SOCHA, 2017).

A Figura 2 mostra a vazão atingida pelo maior ataque DDoS registrado em cada ano, considerando o período entre 2004 e 2018. Ela ilustra o crescimento na intensidade dos ataques ao longo dos anos. (BIENKOWSKI; ARBOR, 2018) aponta que o volume de tráfego não é a única característica que tem crescido, a complexidade nos ataques também evoluiu.

Diversas classificações de ataques DDoS já foram propostas na literatura, tais como (MIRKOVIC; REIHER, 2004; SPECHT; LEE, 2004; BOSWORTH; KABAY; WHYNE, 2012; DEKA; BHATTACHARYYA; KALITA, 2017). A classificação adotada neste estudo foi a de Zargar, Joshi e Tipper (2013), que define dois grupos:

1. O primeiro grupo inclui ataques DDoS que afetam as camadas de rede e transporte, explorando TCP, UDP e ICMP. Esses ataques podem usar quatro técnicas:
    - **Saturar** a rede não permitindo o acesso de usuários legítimos.
    - Explorar **vulnerabilidade ou bug** de algum serviço da vítima, com a finalidade de exaurir recursos.

[2] O github é um serviço de hospedagem web responsável por oferecer controle de versionamento através do git (GIT, 2018)

1974	O primeiro ataque registrado acabou sendo realizado explorando uma vulnerabilidade em um mainframe conhecido como *Programmed Logic for Automatic Teaching Operations* (PLATO) (DENNIS, 2010).
1980	Robert Morris criou um *malware* conhecido atualmente como *worm* (Morris worm), este foi responsável por paralisar grande parte da Internet (WOODY; SHOEMAKER; MEAD, 2012). Um total de 6000 sistemas UNIX foram infectados para a realização do ataque, por consequência foi a primeira pessoa a ser condenada pela *Computer Fraud and Abuse Act* (CFAA) (CORNELL, 1984).
1995	O *Strano Network* abria inúmeras conexões em páginas web como forma de protesto contra a política nuclear do governo francês (COX, 2014).
1997	A primeira demostração pública do ataque DDoS foi realizada por Khan C. Smith, durante o evento grandes corporações acabaram sendo atacadas.
1998	*The Electronic Disturbance Theater* atraves do *FloodNet* realizou ataques até o final de 1999, auxiliando protestos no México e realizando ataques em *World Trade Organization* (WTO). Em 1998 também foi realizado o primeiro ataque de reflexão conhecido como *Smurf attacks* que explora o *Internet Control Message Protocol* (ICMP) (RYBA et al., 2015).
1999	Surgimento da *botnet Trinoo* utilizada para a realização de ataques DDoS (LEMOS, 2016). No mesmo ano foi avisado sobre a possibilidade de utilizar o DNS para a realização de ataques DDoS (NIST, 1999; CERT/TCC, 1999).
2003	O primeiro *flash worm* (*Slammer worm*) infectou 75 milhões de *hosts* em dez minutos e alcançou 80 milhões de pacotes por segundo.
2009	O *worm MyDoom* foi reaproveitado para infectar 50 mil *hosts* e realizar um ataque que alcançou picos de 13Gbps (ZETTER, 2009).
2012	Crescimento nos ataques DRDoS explorando DNS, *Character Generator Protocol* (Chargen), NTP e *Simple Network Management Protocol* (SNMP) (PROLEXIC, 2013).
2013	30.000 DNS servers fizeram parte em um ataque contra a *Spamhaus* que atingiu picos de 300 Gbps (PRINCE, 2013). Outros ataques realizados que obtiveram um fator de amplificação próximo a 100 Gbps (RYBA et al., 2015; BREWSTER, 2013)
2014	Com um crescimento no número dos ataques DRDoS (PRINCE, 2014), o NTP foi explorado para realizar ataques que atingiram picos de 400 Gbps (LOPES, 2015).
2016	Mais de 150.000 dispositivos *Internet of Things* (IoT) são explorados para realizar ataques que alcançaram ≈ 1 Tbps de tráfego (em sua grande maioria o tráfego foi gerado por *Closed-Circuit Television Camera* (CCTV)) (KHANDELWAL, 2016).
2018	Atacantes exploram servidores que deixaram serviços Memcached abertos na Internet para realizar ataques ao github.com[2]. O ataque deixou os serviços do Github indisponíveis por dois períodos de tempo e alcançou picos de ≈ 1.4 Tbps de tráfego, sendo classificado como o maior ataque de amplificação já registrado (NEWMAN, 2018). Uma semana depois deste ataque a NETSCOUT (BIENKOWSKI; ARBOR, 2018) registrou um ataque de ≈ 1.7 Tbps de tráfego, que foi realizado pelo mesmo vetor explorado anteriormente.

Fonte: Autor, 2018

TABELA 1 Linha temporal ataques DDoS

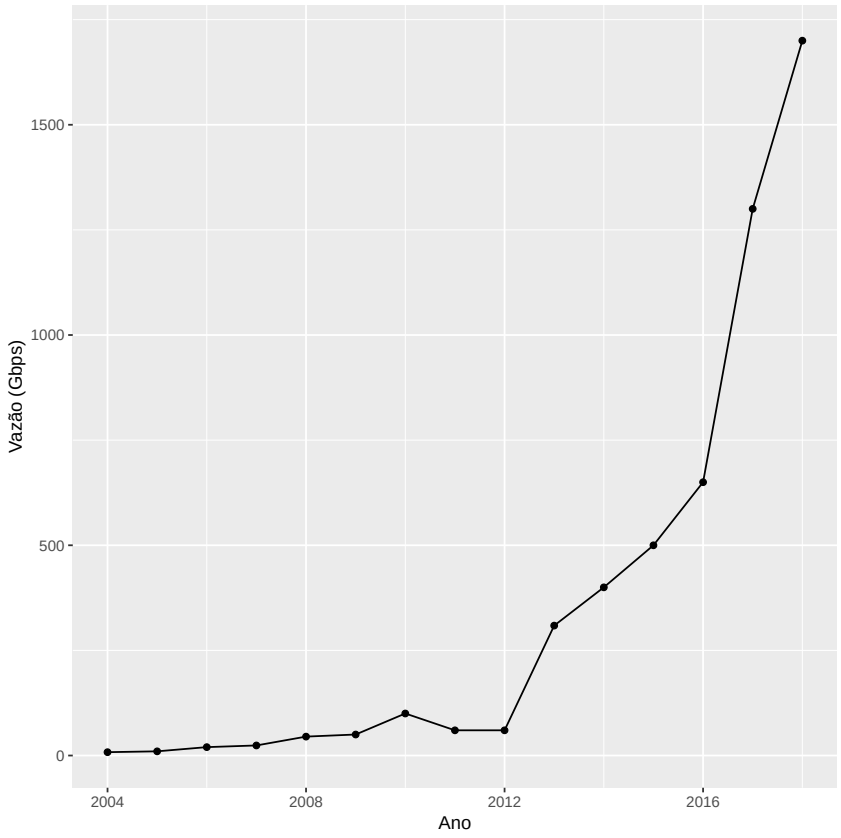

Figura 2 – Evolução anual da vazão de ataques DDoS (2004–2018).

Fonte: (BIENKOWSKI; ARBOR, 2018).

- Utilizar um serviço para realizar a **reflexão** de consultas para uma vítima, desta forma evitando enviar um conjunto de requisições diretamente para a vítima.
- Realizar consultas em um serviço com a finalidade de gerar **amplificação** das consultas.

2. O segundo grupo tem enfoque na camada de aplicação, a finalidade do ataque é exaurir os recursos do serviço. Sendo subdividido em dois grupos:

   - Ataques de **amplificação** e **reflexão** também podem ser realizados na camada de aplicação, com a finalidade de adicionar uma carga de trabalho no servidor.
   - **Ataques *Hypertext Transfer Protocol* (HTTP)**, o ataque consiste da realização de um número elevado de conexões ou alta carga de trabalho para o servidor.

Ataques DRDoS volumétricos são realizados na cama 3 e 4 (rede e transporte), o ataque explora o envio de uma quantidade alta de fluxo para sobrecarregar um *web*

server. Consumindo *bandwidth* e prejudicando usuários autênticos de utilizar o serviço (CERT, 2014). Já o ataque na camada 7 (aplicação) visa sobrecarregar alguns elementos característicos encontrados no ambiente.

2.2 ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO POR REFLEXÃO (DRDOS)

Os ataques de DRDoS exploram sistemas computacionais que possuam algum tipo de taxa de amplificação (CERT, 2018). O atacante utiliza um terceiro sistema com o intuito de realizar a amplificação das consultas antes de serem enviadas para a vítima. Um conjunto de protocolos que podem ser explorado é apresentado por (PAXSON, 2001). Uma demonstração do ataque é apresentado na Figura 3, ao qual um conjunto de agentes explora um terceiro sistema para a realização da amplificação do tráfego.

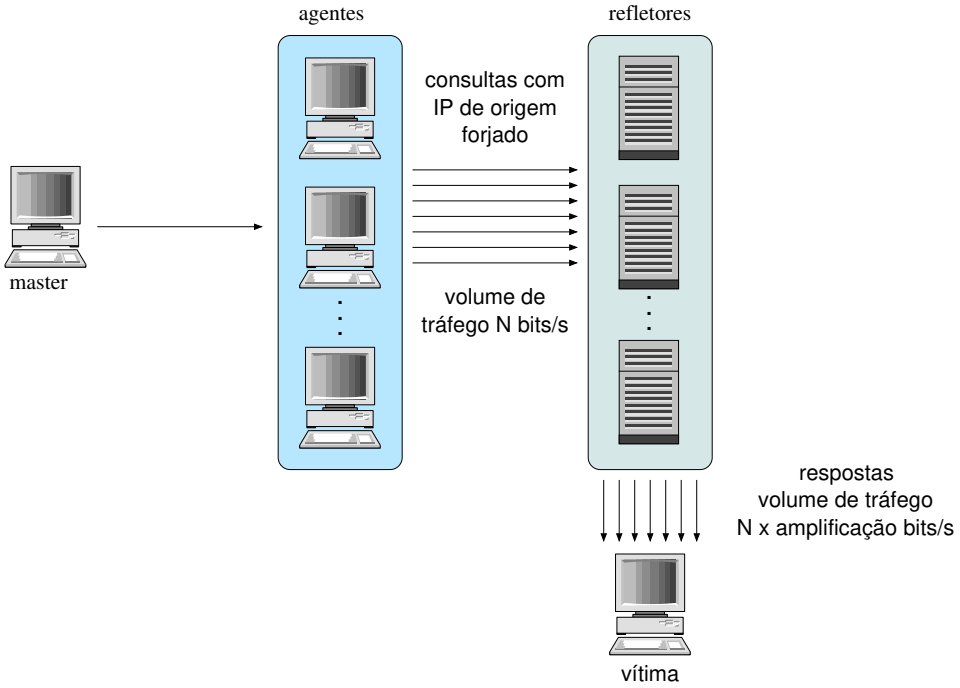

Figura 3 – Representação de uma infraestrutura para a realização de ataques DRDoS.

Fonte: Autor.

Um conjunto destes protocolos faz parte da infraestrutura pública da Internet ou acabam fazendo parte de instalações padrões de sistemas, o que contribui para a proliferação de sistemas que possam ser explorados para a realização dos ataques e acabe dificultando a eliminação ou exaustão destes recursos explorados para a realização dos ataques (CERT.BR, 2016).

O fator de amplificação de um ataque DRDoS é dado pela razão entre o tamanho das respostas enviadas pelos refletores e o tamanho das respectivas consultas. Devido à amplificação, um atacante precisa gerar menos tráfego para produzir o

mesmo resultado sobre a a vítima, quando comparado a um ataque DDoS sem reflexão.

Ataques DRDoS também oferecem uma camada a mais de segurança para os atacantes, em decorrência da utilização de refletores a identificação da localização destes acaba tendo mais um nível.

O critério que acaba sendo considerado para a realização deste ataque é o fator de amplificação encontrado em diferentes serviços, já que estes acabam possuindo uma influencia direta nos ataques. Um sistema com amplificação alta acaba poupando recursos dos atacantes, sendo que não é necessário a utilização de um número elevado de *bots* para gerar o volume de tráfego, o que não acaba ocorrendo em outros tipos de ataque.

2.2.1 Protocolos usados em DRDoS

Existem diversos protocolos que podem ser usados para efetuar ataques DRDoS. Esta seção apresenta os protocolos mais relevantes com base em (DDOSMON, 2018), e discute as características desses protocolos que são exploradas nos ataques.

Os ataques DRDoS com maior popularidade acabam explorando o DNS e NTP devido a sua popularidade. O NTP já colaborou para uns dos maiores ataques já registrados (CZYZ et al., 2014), ultrapassando o tráfego em escala global do DNS. O DNS é um sistema de importância e só uma simples consulta já oferece uma amplificação e vem sendo explorado a nos (PAXSON, 2001).

O DNS desempenha uma funcionalidade essencial para a operação da Internet, sendo responsável por, entre outras funcionalidades, realizar a associação de um nome de domínio com um endereço IP. O sistema é implementado como uma estrutura hierárquica, possuindo servidores raiz, que são responsáveis por atualizar a lista de nomes e endereços IPs (GAO et al., 2013). O DNS é explorado como um refletor onde o atacante envia um número elevado de consultas com o endereço IP forjado para um servidor DNS recursivo, o ataque é facilitado pelo fato de consultas DNS pequenas poderem gerar respostas grandes.

NTP é um protocolo utilizado para a sincronização de relógios através da rede. Os atacantes exploram sistemas com suporte a solicitações de listas de *peers* um exemplo clássico é o MONLIST, que retorna uma lista com os últimos 600 *hosts* que utilizaram o serviço.

Memcached é um sistema de *cache* em memória com ampla utilização para otimização de banco de dados (MEMCACHED, 2009). Os atacantes acabam explorados sistemas aos quais ficam abertos na Internet para a realização dos ataques (NEWMAN, 2018), as duas maneiras mais populares são:

- Realizar consultas com o IP forjado solicitando estatísticas do sistema; e
- Realizar a inserção de uma chave no sistema, com um conteúdo relativamente alto de informações relacionado, após esta etapa realizar inúmeras consultas com o IP forjado e a chave que foi inserida no banco (BAIA, 2018).

O *Quote of the Day* (QOTD) e Chargen são ferramentas de depuração e medição (POSTEL, 1983b; POSTEL, 1983a), o primeiro independente da requisição envia uma mensagem e o segundo é um gerador de caracteres sequenciais que atua sobre o mesmo princípio.

SSDP (GOLAND et al., 1999) é utilizado para anúncio e descoberta de serviços na rede, com o intuito de divulgar a presença de certo dispositivo no ambiente. O atacante explora roteadores que possuam vulnerabilidade no protocolo *Universal Plug and Play* (UPnP), aos quais estão conectados na Internet e permitem o acesso para qualquer usuário.

O *Routing Information Protocol* (RIPv1) é um protocolo utilizado para o roteamento de pacotes na Internet. Para realizar a divulgação das tabelas o RIPv1 envia *broadcasts* na rede, através deste o atacante consegue explorar o protocolo realizando consultas que podem gerar respostas de até 504 bytes (AKAMAI, 2016).

Connection-less Lightweight Directory Access Protocol (CLDAP) e *Lightweight Directory Access Protocol* (LDAP) são protocolos utilizados pela Microsoft para o compartilhamento, busca e atualização de diretórios através da rede (CHOI; KWAK, 2017). Com um *payload* de 52 bytes o atacante consegue gerar uma amplificação de até setenta vezes.

Plataforma de jogos como a Steam oferecem opções aos usuários para virar *host* dos seus próprios servidores e até mesmo *hosts* privados podem ser explorados para a realização dos ataques (NOLLA, 2013). Este tipo de ataque acaba explorando diferentes *payloads* e protocolos, como por exemplo RCON, Quake e Half-life.

Smurf attack explora mensagens ICMP para realizar os ataques, a ideia por traz é explorar estruturas que aceitem *Broadcast Domain*. A amplificação fica diretamente interligada com o número de *hosts* presentes ($N * M$, onde N representa a quantidade de *ICMP Request* e M o número de *hosts*) (KUMAR, 2007).

Responsável por transmitir informações de dispositivos e sensores o SNMP é explorado por possuir um conjunto de vulnerabilidades (principalmente nas verões SNMPv1 e SNMPv2). Para realização do ataque, o atacante envia requisições (*BulkGetRequest*) com o IP forjado para o sistema, ao qual será encaminhado para a vítima (PROLEXIC, 2012; BITAG, 2015).

Dispositivos IoT já foram explorados para realização de ataques, e estimasse que em 2020 existam 200 Bilhões de dispositivos. Em (HENGST, 2016) é apresentada um estudo sobre a vulnerabilidade destes dispositivos para a realização de ataques DDoS, com o enfoque em SSDP e ICMP. Apesar da existência de diferentes dispositivos, é comprovado que estes sistemas podem ser explorados como refletores, sendo demonstrado o impacto que estes sistemas poderão atingir em 2020.

O *Trivial File Transfer Protocol* (TFTP) possibilita o *Download* e *Upload* de dados para um serviço, o protocolo utiliza o UDP e possui um conjunto de vulnerabilidades (inclusive *buffer overflow*). O protocolo é explorado ao realizar um *write* no serviço, este acaba sendo agravado em decorrência da existência de inúmeros campos no pacotes com a possibilidade de definição de tamanho (SIEKLIK; MACFARLANE; BUCHANAN, 2016) .

Christmas (Xmas) tree attack (XMAS) ataque[3] possui a finalidade de utilizar múltiplas *flags* no cabeçalho do pacote TCP (foi registrado ataques de até 100 Gbps) (SU et al., 2016; AKAMAI, 2014).

O TCP pode ser explorado para realizar ataques DRDoS, mas o fator de amplificação acaba ficando limitado ao tamanho do *SYN* já que o *ACK* não será maior que o *SYN* (existe a possibilidade de retransmissão, ao qual é representado na Tabela). Ataques acabam explorando o TCP para exaustar as conexões ou atrasar a camada de aplicação (KÜHRER et al., 2014b). Três tipos de ataques são explorados para amplificação SYN/ACK, PSH e RST que exploram *File Transfer Protocol* (FTP), HTTP, *Network Basic Input/Output System* (NetBios),*Session Initiation Protocol* (SIP), *Secure Shell* (SSH) e Telnet.

A Tabela 2 apresenta o conjunto de protocolos encontrados junto com alguns dos trabalhos que acabaram explorando este protocolo. A Tabela apresenta o fator de amplificação, ao qual acaba sendo o fator de maior relevância para os atacantes. Com uma variedade de protocolos *legacy*, aplicações *Peer-to-peer* (P2P) e protocolos de jogos.

2.3 *HONEYPOTS*

O *honeypot* é um recurso computacional ao qual possui o objetivo de ser sondado, atacado ou até mesmo comprometido (HOEPERS; STEDING-JESSEN; CHAVES, 2007). Este recurso é utilizado para estudar comportamento e atividades dos atacantes, através de um conjunto de rotinas.

Geralmente um *honeypot* é um *host* que possui um endereço público na In-

[3] *Christmas tree packet:* possui a finalidade de utilizar todas as *flags* possíveis em um pacote, este ocorre independente do protocolo.

#	**Protocolo**	**Detalhes**	**Amplificação**
1	DNS	(PAXSON, 2001)	28-54
2	NTP	(CZYZ et al., 2014)	556.9
3	NetBios	(ROSSOW, 2014)	3.8
4	SSDP	(HENGST, 2016)	30.8
5	SNMP v2	(PROLEXIC, 2012)	6.3
6	RIPv1	(AKAMAI, 2016)	131.24
7	mDNS [a]	(CERT, 2018)	2-10
8	Portmap	(CERT, 2018)	7-28
9	LDAP	(CERT, 2018)	46-55
10	CLDAP	(CHOI; KWAK, 2017)	33-70
11	TFTP	(SIEKLIK; MACFARLANE; BUCHANAN, 2016)	60
12	DNSSEC [b]	(RIJSWIJK-DEIJ; SPEROTTO; PRAS, 2014)	40-55
13	ICMP	(KUMAR, 2007)	não disponível
14	IGMP [c]	(SARGENT et al., 2017)	100
15	Memcached	(BAIA, 2018)	10.000-51.000
16	Chargen	(ROSSOW, 2014)	358.8
17	QOTD	(CERT, 2018)	140.3
18	BitTorrent	(SIA, 2006)	3.8
19	*Kad network* (Kad)	(CERT, 2018)	16.3
20	*End System Multicast* (ESM)	(SUN; TORRES; RAO, 2010)	não disponível
21	Quake 3	(ROSSOW, 2014) (Quake, DOOM 3 ...)	63.9
22	Steam	(CERT, 2018) (*RCON*)	5.5
23	*half-life*	(NOLLA, 2013) (Call of Duty 2/4, CS Condition Zero e CS Source, Team Fortress 2 ...)	109.8
24	Gamespy	(NOLLA, 2013) (f.e.a.r)	107
25	SIP	(KÜHRER et al., 2014b)	5-80
26	XMAS	(SU et al., 2016)	não disponível
27	HTTP	(BECKETT; SEZER, 2017)	79-100

[a] *Multicast Domain Name System* (mDNS) é responsável pela resolução de nomes de *hosts* para um endereço IP em uma rede (CHESHIRE; KROCHMAL, 2018).

[b] O *Domain Name System Security Extensions* (DNSSEC) é uma versão segura do DNS que utiliza assinatura digital. Seu desenvolvimento tem a finalidade de solucionar problemas como *cache poisoning* e ataques DDoS (ARENDS; AUSTEIN, 2018).

[c] A finalidade do *Internet Group Management Protocol* (IGMP) é permitir que *hosts* e roteadores troquem informações de *status* através do multicast (FENNER, 2018).

Tabela 2 – Visão geral dos protocolos de rede analisados

ternet, o qual não é anunciado. Por consequência o *host* precisa ser descoberto para a realização de qualquer tipo de interação com o sistema, o que exige algum tipo de mapeamento realizado pelos atacantes. Desta forma é possível afirmar que qualquer interação realizada com o *honeypot* é considerada suspeita.

A utilização de um *honeypot* traz alguns riscos devido a iteração que o sistema realiza com os ataques e o os estudos realizados acaba ficando limitados em decorrência do tipo de ataque está sendo estudado (SPITZNER, 2003). No caso de ataques DRDoS ao qual refere este trabalho o *honeypot* utilizado possui a funcionalidade de refletor, ou seja o tráfego recebido já passou por *spoofing* (o IP registrado é o da vítima).

Os *honeypots* podem ser classificados de acordo com o seu nível de interatividade (SPITZNER, 2003). Um *honeypot* de baixa interatividade basicamente emula algumas funcionalidades de um sistema vulnerável, permitindo uma observação mais restrita do comportamento dos atacantes mas oferecendo um risco menor. Um *honeypot* de alta interatividade, por outro lado, permite que atacantes interajam com aplicações e serviços reais, o que oferece uma visão mais detalhada de suas atividades mas introduz um nível maior de risco. Entre esses extremos se situam os *honeypots* de média interatividade, que oferecem níveis intermediários de visibilidade e risco.

2.4 CONSIDERAÇÕES DO CAPÍTULO

Ataques DDoS têm sido um problema crescente na Internet ao longo dos anos. Ataques DDoS por reflexão oferecem algumas vantagens aos atacantes, como amplificação do tráfego e maior dificuldade de localização da origem de um ataque devido ao uso de intermediários. A variedade de protocolos que podem ser usados em ataques DRDoS e a ampla disponibilidade de refletores abertos na Internet ajudam a explicar o uso frequente dessa técnica de ataque. *Honeypots* são ferramentas úteis para compreender o funcionamento de ataques e acompanhar a evolução das técnicas usadas pelos atacantes.

O próximo capítulo delimita o escopo da pesquisa e explica como pretende-se analisar o tráfego de ataques DRDoS com base em dados coletados por *honeypots*.

3 DELIMITAÇÃO DO PROBLEMA E PROPOSTA

Este capítulo define o escopo da pesquisa e a proposta do trabalho. A Seção 3.1 discute os trabalhos relacionados. A Seção 3.2 delimita o problema de pesquisa e apresenta a proposta. A Seção 3.3 aborda o planejamento da pesquisa.

3.1 TRABALHOS RELACIONADOS

Ao considerar ataques DDoS e DRDoS o primeiro fator avaliado pela literatura é o quesito histórico, desta maneira demonstrando o impacto que os ataques obtiveram ao decorrer dos anos e o fator de amplificação alcançado através de uma linha temporal, como pode ser visto em (DEKA; BHATTACHARYYA; KALITA, 2017; RYBA et al., 2015).

Um fator que influencia no crescimento de ataques DDoS são os mercados de *booters*, ao qual oferece serviços *online* que efetuam ataques mediante pagamento (DDoS-for-hire). Os vetores explorados para a realização dos ataques, o meio de pagamento e o perfil dos usuários que utilizam estes serviços são o principal enfoque das pesquisas, já que estes serviços são prestados a partir de $1 (MANSFIELD-DEVINE, 2015; SANTANNA et al., 2015; KARAMI; PARK; MCCOY, 2016). O Chargen e DNS tem destaque por serem os vetores mais explorados para a realização de ataques DRDoS pelo *booters*.

Uma investigação sobre vítimas de ataques DDoS foi apresentada em (NOROOZIAN et al., 2016). Os autores usaram um *honeypot* (KRÄMER et al., 2015) que implementava refletores para seis protocolos (QOTD,Chargen,DNS,NTP,SNMP e SSDP), com o intuito de descobrir os serviços mais atacados, os provedores e os países das vítimas. O trabalho não realiza uma avaliação para a identificação de ataques multi-protocolo, limitando a análise por protocolo e vítimas.

Dentre os trabalhos encontrados na literatura é possível apontar um enfoque para *Smuft Attack* ou ataques DDoS que utilizam o DNS ou NTP, como (SHARMA; GULERIA; SINGLA, 2018). (LIU et al., 2015) apresenta um algoritmo, com o intuito de identificar ataques DDoS e tomar medidas para minimizar o impacto. Outra visão também explorada para a identificação de ataques DDoS é através de técnicas de inteligência artificial(ZHANG; ZHANG; YU, 2017) e *Machine Learning* (ML) (MEITEI; SINGH; DE, 2016).

Com maior proximidade a esta pesquisa, é possível apontar três trabalhos. A primeira abordagem próxima ao estudo é apresentada por (ROSSOW, 2014). O es-

tudo tem o enfoque em ataques DRDoS, apresentando um levantamento de protocolos vulneráveis para a realização destes ataques, ao qual foi justificado por um mapeamento que acabou consistindo do número total de amplificadores encontrados por protocolo e o fator de amplificação. Com o intuito de aproximar o estudo a um caso real, foi realizado uma caracterização de tráfego de um *Internet Service Provider* (ISP) europeu, visando identificar vítimas, amplificadores e mapeamentos para portas UDP vindo de *darknets*.

O segundo trabalho (RYBA et al., 2015) é um *Survey* ao qual visa apresentar trabalhos com a finalidade de prever, identificar e filtrar ataques DRDoS. A principal contribuição para o presente estudo é a apresentação de uma linha temporal, ao qual destaca os principais ataques, vetores e protocolos explorados.

O terceiro (THOMAS; CLAYTON; BERESFORD, 2017) consiste de uma coleta de dados utilizando sensores, que teve uma duração de 1010 dias. A coleta foi realizada através de sensores, ao qual consiste de um total médio de 65 sensores ao decorrer deste período. O estudo realiza uma avaliação do número de ataques realizados por protocolo (com um total de oito protocolos observados), valor de amplificação obtido e duração dos ataques. Uma abordagem em relação aos mapeamentos recebidos pelo sensores contribui para o esclarecimento de qual a frequência destas atividades por parte dos atacantes. Destacam-se nesse trabalho o número considerável de sensores dispostos em diferentes localizações e a variedade de protocolos investigados.

Por fim é possível destacar que os trabalhos apontados com maior proximidade ao respectivo estudo acabam não realizando uma abordagem em relação a ataques multiprotocolos.

3.2 PROPOSTA

Estudos recentes (NETSCOUT; ARBOR, 2017) apontam a ocorrência de ataques DRDoS em que uma mesma vítima é atacada usando múltiplos protocolos de forma simultânea. No entanto, esse fenômeno não foi ainda abordado na literatura científica. A revisão de trabalhos relacionados mostrou que mesmo as pesquisas que analisam tráfego de ataques DRDoS e estudam mais de um protocolo (ROSSOW, 2014; THOMAS; CLAYTON; BERESFORD, 2017) consideram esses protocolos de forma isolada, sem dar atenção a ataques que exploram vários protocolos ao mesmo tempo.

O problema abordado nesta dissertação de mestrado é justamente a análise de tráfego DRDoS considerando ataques multiprotocolo. As questões que serão exploradas nesta pesquisa incluem:

- Qual a proporção de ataques multiprotocolo e de ataques monoprotocolo?

- Qual a duração e intensidade de ataques DRDoS multiprotocolo? Como essas características se comparam as de ataques monoprotocolo?
- Quantos e quais protocolos são usados em ataques DRDoS multiprotocolo?
- Quais são as vítimas de ataques DRDoS multiprotocolo?

A lista acima não é exaustiva, e a própria busca de respostas a essas questões pode suscitar outras questões a serem exploradas.

3.3 PLANEJAMENTO DA PESQUISA

Em priori foi realizado uma revisão bibliográfica, ao qual é apresentada na Seção 3.1 para a identificação de lacunas e auxiliar na definição da proposta apresentada na Seção 3.2.

Para a definição do projeto foram elencados quais os fatores necessários para a realização do estudo, estes são: (1) definição dos protocolos a serem observados; (2) necessidade de uma estrutura voltada para a coleta de informações de ataques DRDoS (um *honeypot* para ataques DRDoS); (3) implantação da estrutura para a realização de coleta de dados; e (4) análise de dados coletados.

Os protocolos definidos foram DNS, NTP, Memcached, SSDP, Steam, QOTD e Chargen, a escolha dos protocolos considera popularidade dos protocolos junto com a taxa de amplificação alcançada (ROSSOW, 2014; RYBA et al., 2015; THOMAS; CLAYTON; BERESFORD, 2017; NETSCOUT; ARBOR, 2017; DDOSMON, 2018). Desta maneira é possível apontar que os protocolos escolhidos estão sendo explorados para a realização de ataques na atualidade.

Para a realização da coleta de dados, torna-se necessário a implementação de uma infraestrutura que consiga comportar o conjunto de protocolos proposto e não seja afetado pela carga gerada pelos ataques DRDoS. O desenvolvimento desta estrutura consiste da implementação de um *honeypot* que consiga comportar os protocolos e realizar o armazenamento do tráfego para análises posteriores.

Após a implementação do *honeypot* foi realizado a implantação do sistema na rede da UDESC. Este é responsável por realizar a coleta de dados

A última etapa consiste da análise dos dados, ao qual tem a finalidade de explorar este conjunto de dados para a identificação de ataques multiprotocolo. Ainda é possível apontar que serão adicionados novos protocolos na estrutura do *honeypot* com o intuito de aprimorar o conjunto de protocolos. Protocolos que ainda serão adicionados são Quake, Kad e LDAP.

3.4 CONSIDERAÇÕES DO CAPÍTULO

Uma revisão da literatura envolvendo ataques DRDoS revela a existência de abordagens e análises com enfoques variados, mas não foi encontrado um trabalho que considere ataques multiprotocolo. Essa lacuna justifica a importância deste trabalho de mestrado.

A proposta do trabalho é efetuar a análise e caracterização de tráfego de ataques DRDoS com base em dados coletados por um *honeypot*. O próximo capítulo apresenta o projeto e implementação do *honeypot*, e discute alguns resultados preliminares da análise de tráfego coletado por esse *honeypot* na rede da UDESC.

4 IMPLEMENTAÇÃO E RESULTADOS PRELIMINARES

Este capítulo apresenta os resultados já obtidos neste trabalho de mestrado. A Seção 4.1 descreve o projeto e implementação do *honeypot* usado para a coleta de dados, e a Seção 4.2 analisa dados coletados no primeiro mês de operações do *honeypot*.

4.1 IMPLEMENTAÇÃO DO HONEYPOT

A análise e caracterização do tráfego de ataques DRDoS pressupõe que se tenha acesso a tráfego dessa natureza. Seguindo experiências anteriores (NOROOZIAN et al., 2016; HEINRICH; LONGO; OBELHEIRO, 2017; THOMAS; CLAYTON; BERESFORD, 2017), neste trabalho é usado um *honeypot* para interagir com atacantes e capturar o tráfego de ataque. Esse *honeypot* deve aparentar atuar como um refletor para diversos protocolos, sem no entanto participar efetivamente de ataques DRDoS. Em outras palavras, a ideia é que o *honeypot* receba as requisições enviadas pelos agentes mas envie uma quantidade mínima de respostas, registrando todas as interações.

Uma análise de *honeypots* disponíveis publicamente (NAZARIO, 2018) não revelou nenhuma ferramenta existente que pudesse ser aproveitada com pouca ou nenhuma modificação. Portanto, constatou-se a necessidade de desenvolver um novo *honeypot* que seja voltado especificamente para coleta e análise de tráfego DRDoS e que suporte múltiplos protocolos. Os principais requisitos funcionais para esse *honeypot* são os seguintes:

- **RF1** – Armazenar todo o tráfego (requisições e respostas) referente aos protocolos suportados pelo *honeypot*;
- **RF2** – Receber requisições de variados protocolos;
- **RF3** – Descartar tráfego gerado por projetos que varrem a Internet em busca de refletores;
- **RF4** – Contabilizar o tráfego recebido, agregando os dados em ataques; e
- **RF5** – Responder de forma convincente a uma fração configurável de requisições por cliente, oferecendo a ilusão de interação com um refletor real.

Os requisitos não funcionais mais importantes dizem respeito a flexibilidade, desempenho e plataforma operacional, e são os seguintes:

- **RNF1** – Ter facilidade para adicionar, remover, habilitar e desabilitar protocolos no *honeypot*;
- **RNF2** – Realizar o processamento inicial de requisições (descarte, contabilização e decisão de processamento) sem exigir acessos a disco;
- **RNF3** – Evitar a execução de procedimentos internos de manutenção durante a ocorrência de ataques; e
- **RNF4** – Ser implementado em plataforma compatível com Unix.

A arquitetura definida para o *honeypot* é mostrada na Figura 4. Para satisfazer o RF1, a aplicação cria um subprocesso que executa a ferramenta Tcpdump (GARCIA, 2010) para capturar e armazenar todo o tráfego de/para as portas TCP e UDP referentes aos protocolos suportados pelo *honeypot*. O Tcpdump armazena os dados em formato binário e com acesso sequencial, garantindo assim eficiência de escrita (KLEPPMANN, 2017). Para evitar problemas com arquivos grandes e facilitar a transferência e compressão dos arquivos de captura, o armazenamento é feito em *chunks* de 100 MB, sendo que o próprio Tcpdump se encarrega de gerenciar a rotação de *chunks*. Esses arquivos de captura são oportunamente transferidos para outro sistema onde será efetuada a análise de dados.

Cada protocolo é implementado em um módulo separado, de modo a atender os requisitos RF2 e RNF1. Foi definido um conjunto de funcionalidades que um módulo deve implementar, e a adição e remoção de módulos requer apenas a modificação de um arquivo fonte da aplicação principal.

Existem diversos projetos que varrem a Internet em busca de refletores que podem ser usados em ataques DRDoS, como (SHODAN, 2013; SHADOWSERVER, 2004). Em muitos casos, os refletores identificados são reportados a organismos de atendimento e coordenação de incidentes de segurança, como o CERT.br (CERT.BR, 2016) e o CAIS (CAIS, 2018), que notificam os responsáveis para que estes desativem os refletores ou restrinjam o acesso a eles. Para evitar que o *honeypot* seja erroneamente reportado como um refletor aberto, é necessário descartar o tráfego de varredura gerado por esses projetos, como estipula o RF3. Para isso, optou-se por compilar uma lista de endereços IP usados por tais projetos para efetuar as varreduras e bloquear todo o tráfego originado nesses IPs usando um filtro de pacotes (não mostrado na Figura 4).

Para efetuar a contabilização de requisições e a sua agregação em ataques (RF4), considera-se que um ataque é formado pelo conjunto de requisições de um dado protocolo com mesmo endereço IP de origem e com intervalo máximo de 5 minutos entre requisições sucessivas. Essa definição é baseada na análise apresentada

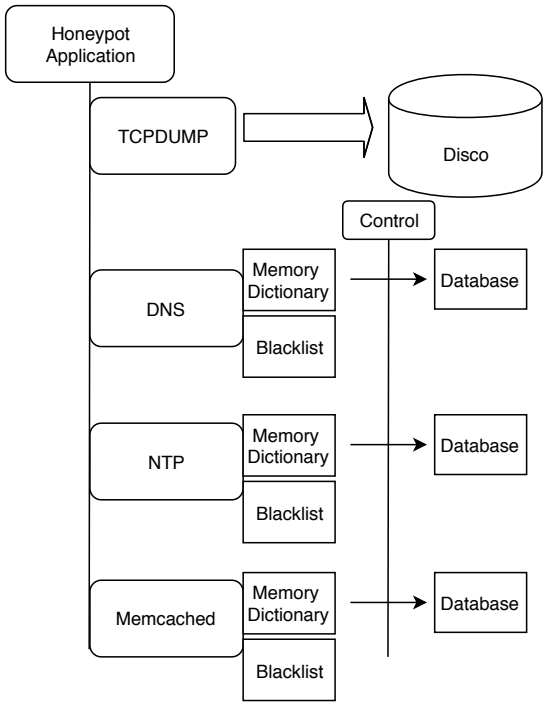

Figura 4 – Arquitetura do *honeypot*

em (HEINRICH; LONGO; OBELHEIRO, 2017) e em (DDOSMON, 2018), que aponta que 39% dos ataques DRDoS duram até 5 minutos.

Para contabilizar os ataques, um módulo mantém uma lista de ataques em andamento, onde cada entrada é formada pelo endereço IP de origem da requisição, um contador de requisições e os *timestamps* da primeira e da última requisições. Se existe na lista um ataque com o mesmo endereço IP de origem e cuja última requisição ocorreu há no máximo 5 min, considera-se que a nova requisição pertence a esse ataque, e atualiza-se o contador de requisições e o *timestamp* da última requisição. Caso contrário, cria-se uma nova entrada na lista de ataques em andamento. Para obter eficiência nesse processamento, atendendo ao requisito RNF2, a lista de ataques é implementada usando uma tabela *hash* em memória, representada na Figura 4 como "Memory Dictionary".

O requisito RF5 determina que um módulo seja capaz de retornar uma resposta coerente a uma requisição, fornecendo um atacante que esteja interagindo com o *honeypot* a ilusão de que este é um refletor real. No entanto, o requisito também exige que o número de respostas por atacante seja limitado, para evitar que o *honeypot* contribua significativamente em ataques DRDoS. Para atender a esse requisito, cada módulo controla o número de requisições recebidas de cada cliente. Quando essa contagem ultrapassa 5 requisições, o endereço IP do cliente é inserido em uma *blacklist*. Ao receber uma requisição, o módulo produz uma resposta apenas se o endereço IP de origem não estiver na *blacklist*. Para satisfazer o requisito RNF2, a lista de

requisições por cliente e a *blacklist* também são implementadas usando tabelas *hash* em memória.

As estruturas de dados em memória passam por uma limpeza periódica a cada 10 minutos, de forma a limitar o consumo de recursos. A lista de ataques pendentes é percorrida, e todos os ataques cuja última requisição ocorreu há mais de 5 minutos são salvos em um banco de dados e removidos da lista. Do mesmo modo, os endereços inseridos na *blacklist* há mais de 24 h são removidos, assim como os endereços na lista de contagem de requisições por cliente que não receberam tráfego nas últimas 24 h (*timestamps* associados a cada entrada são usados para esse fim). Para atender ao requisito RNF3, a *thread* de controle representada na Figura 4 suspende os procedimentos de limpeza quando o *honeypot* está recebendo ataques. Caso uma limpeza seja interrompida, ela só será retomada no próximo período (isto é, após 10 minutos).

Para satisfazer o requisito RNF4, o *honeypot* foi implementado na linguagem Python, e as demais ferramentas usadas (Tcpdump, SQLite, Unbound e memcached) estão disponíveis em diversas variantes de Unix. Assim, embora a versão atual do *honeypot* utilize a plataforma Linux, o sistema não está atrelado a esse sistema operacional, podendo ser facilmente adaptado a outros sistemas Unix-*like*.

A Figura 5 representa o fluxo de processamento de requisições. Uma requisição enviada por um atacante (1) chega ao *honeypot* e é contabilizada (2). O *honeypot* então consulta o endereço acIP de origem na *blacklist* para decidir se uma resposta deve ou não ser enviada. Caso negativo, o processamento da requisição encerra (3). Caso afirmativo, o *honeypot* produz uma resposta para a requisição (4), conforme será detalhado no próximo parágrafo. A resposta obtida é então enviada para o cliente, que pode ser uma vítima (no caso de ataque por reflexão) ou o próprio atacante quando este envia *probes* para o *honeypot*. O passo 6 representa a coleta de tráfego com o Tcpdump, e o passo 7 a limpeza periódica das tabelas *hash* em memória, com armazenamento persistente dos dados relevantes para análise posterior em um banco de dados.

O tratamento dado às requisições no passo 4 depende do protocolo. A maioria dos protocolos implementados – Chargen, NTP, QOTD, SSDP e Steam – admite respostas fixas, e portanto o próprio módulo sintetiza uma resposta. Por outro lado, DNS e Memcached têm semânticas mais complexas, onde a resposta é dependente do conteúdo da requisição (por exemplo, em uma resolução de nomes usando o DNS a resposta depende inteiramente do nome consultado). Para esses protocolos, as requisições são repassadas para um servidor local para processamento, e a resposta recebida desse servidor é encaminhada para o cliente. Os servidores locais usam apenas a interface de *loopback*, e não interagem diretamente com clientes externos.

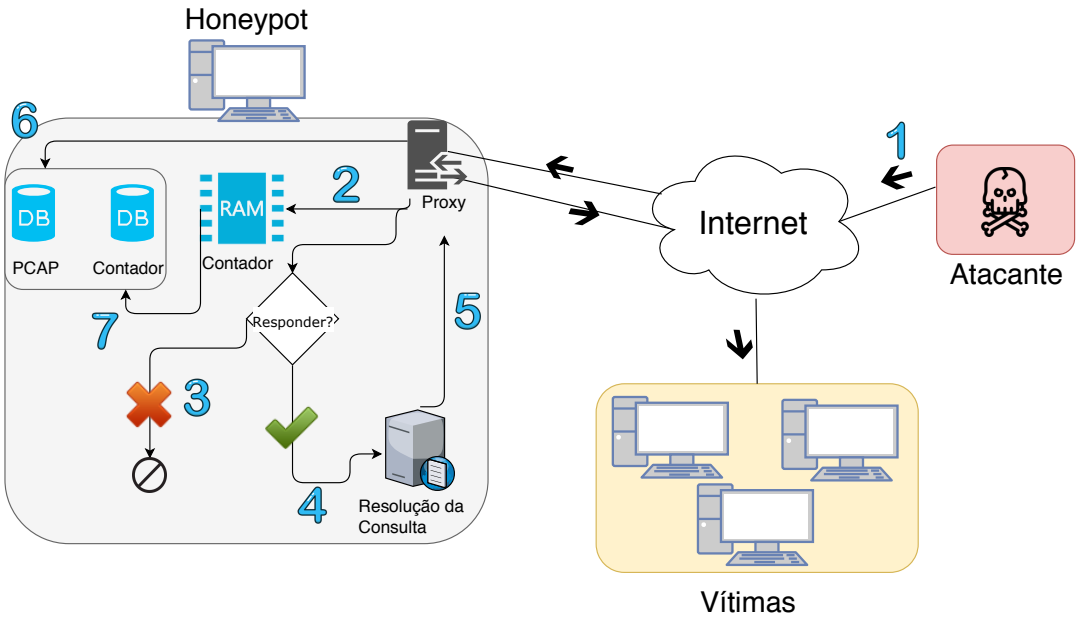

Figura 5 – Fluxo do processamento de requisições no *honeypot*

4.2 RESULTADOS PRELIMINARES

Esta seção analisa os dados disponíveis no banco de dados de ataques, que registra protocolo, endereço IP do cliente, número de requisições e *timestamps* de início e fim para cada ataque. Futuramente serão explorados os dados coletados pelo *Tcpdump*, pois, em decorrência do volume de dados, algumas medidas para a otimização das análises ainda se fazem necessárias.

4.2.1 Implantação

O *honeypot* está utilizando um *host* com 4 GB de memória e um processador *AMD Phenom(tm) II X4 B93 Processor*. Este *host* está localizado na rede da UDESC, realizando a coleta de dados 24/7.

A análise de dados descrita nesta seção teve início no dia 28/09/2018 e término no dia 28/10/2018, totalizando uma coleta de 30 dias.

Apesar de considerar este período como teste, o *honeypot* não teve *downtime* de mais de um dia e até o momento nenhuma alteração foi necessária no sistema. O único problema encontrado foi a necessidade de atualizar os endereços na *blacklist* do sistema manualmente, em decorrência do conjunto de protocolos utilizados. Sendo possível afirmar que um conjunto relativamente alto de endereços já foi bloqueado (53 *subnets*).

Considerando o período de implantação é possível apontar algumas avaliações realizadas para verificar o impacto dos ataques no sistema operacional. Para esta

avaliação foi selecionado um período de uma hora e meia, no qual ocorreram dois ataques, os detalhes são apresentados na Tabela 3. O sistema recebeu uma média de 737.9 pacotes por minuto, com um mínimo de 435.5 e máximo de 1033.0 pacotes por minuto. Nesse período a utilização de *Central Processing Unit* (CPU) ficou entre 2% e 5%, e a utilização de memória em 7.3% (93% considerando *buffers* e *cache*). A utilização de disco ficou entre 3 e 5%, devido à captura de tráfego pelo *Tcpdump*.

#	Duração	Requisições
1	1.15 minutos	55.697
2	1.29 horas	1.381

Tabela 3 – Informações dos ataques observados.

4.2.2 Classificação de DDoS

Para realizar a classificação dos ataques DRDoS foi considerada a definição apresentada em (HEINRICH; LONGO; OBELHEIRO, 2017) para ataques DoS usando o DNS:

> Um ataque DoS é formado por um conjunto com no mínimo 5 consultas com o mesmo IP de origem e com espaçamento máximo de 60 segundos entre consultas consecutivas, e pelas respostas a essas consultas.

Uma análise preliminar dos dados coletados no *honeypot* permitiu concluir que a mesma definição é aplicável aos demais protocolos implementados, tendo sido assim mantida nesta análise.

4.2.3 Análise

Durante este período de atividade o *honeypot* processou 381.660.799 transações, um valor médio de 12.722.027 requisições por dia. Ao todo o sistema foi explorado para amplificar tráfego para um total de 14.274 vítimas, distribuídas entre os 7 protocolos. Avaliando as transações recebidas por protocolo, junto ao limite de requisições definido na Seção 4.1, o *honeypot* respondeu 0.02% das requisições que fazem parte de um ataque DRDoS, sendo 99.9% das consultas ignoradas e 0.008% das requisições recebidas compondo um *scan*.

A Tabela 4 apresenta a distribuição de consultas por protocolo. É possível apontar uma dominância de consultas explorando o Chargen, que oferece um alto fator de amplificação para um *payload* de apenas um byte. O DNS e Memcached apesar da sua baixa proporção em consideração ao Chargen estão presentes em ataques multi-protocolo.

#	Protocolos	%
1	Chargen	93.1
2	Memcached	4.1
3	DNS	2.5
4	SSDP	0.1
5	NTP	0.0
6	QOTD	0.0
7	Steam	0.0
8	Total	100

Tabela 4 – Requisições por protocolo.

Foi observado um volume relativamente alto de consultas que correspondem a mapeamentos (*scan*) de rede. visando excluir estes valores das análises foi definido que:

> Considera-se um *scan* quando são recebidos até quatro pacotes de um dado endereço IP de origem para a mesma porta de destino em um intervalo de até 5 minutos.

Com base nessa definição, a Tabela 5 apresenta a proporção de requisições que constituem ataques e *scans*. Observa-se que menos da metade (46.5%) das requisições processadas pelo *honeypot* se encaixa na definição de ataque, com os 53.5% restantes correspondendo a *scans*.

#	Estatísticas	%
1	Ataques	46.5
2	Scan	53.5
3	Total	100.0

Tabela 5 – Proporção de ataques e *scans* considerando o número de requisições.

A duração dos ataques é apresentada na Tabela 6. A terceira coluna não considera ataques multiprotocolos, a avaliação considera o período de cada interação realizada por protocolo, já a quarta coluna apresenta a avaliação considerando ataques DRDoS que utilizaram multiprotocolo. A análise consiste do tempo de duração das consultas realizadas no *honeypot*, é possível destacar um crescimento de dezoito vezes entre o desvio padrão por protocolo para multiprotocolo. A média entre protocolo e multiprotocolo apresenta uma diferença de doze vezes, sendo possível apontar um crescimento no período de duração dos ataques multiprotocolo.

A Tabela 7 apresenta a quantidade de protocolos distintos utilizados para atacar uma vítima, sem considerar se esses ataques são simultâneos (multiprotocolo) ou ocorrem em períodos separados. Observa-se que 670 vítimas (4.7% do total) receberam tráfego de mais de um protocolo.

#	Estatísticas	Por protocolo (segundos)	Multiprotocolo (segundos)
1	Média	1100.62	13422.75
2	Desvio padrão	3085.33	57975.37
3	Mínimo	0.00	5.79
4	1 percentil	0.00	9.95
5	5 percentil	3.88	25.56
6	1 quartil	57.25	96.15
7	Mediana	202.48	305.66
8	3 quartil	1110.77	1536.08
9	95 percentil	3710.40	57653.61
10	99 percentil	11435.15	358488.13
11	Máximo	136546.27	538030.70

Tabela 6 – Duração das consultas em cada protocolo.

#	Número de Protocolos	Número de Vítimas
1	1	13604
2	2	627
3	3	26
4	4	8
5	5	4
6	6	2
7	7	3

Tabela 7 – Quantidade de protocolos explorados por vítima.

Para avaliar ataques multiprotocolo, foi dividido os períodos de ataques por vítima. O resultado é um conjunto de períodos temporais ao qual o *honeypot* foi explorado como vetor de amplificação para os ataques em uma vítima. Estes períodos são avaliados utilizando uma árvore de intervalos (CORMEN et al., 2009), possibilitando associar quais ataques são multiprotocolo. A Tabela 8 apresenta o número de ataques multiprotocolo por vítima. A primeira coluna indica o número de ataques (zero retrata a quantidade de ataques que não são multiprotocolo) e a segunda coluna representa a quantidade de vítimas atacadas. Observa-se que 149 vítimas (1.04% do total) sofreram ataques que exploram simultaneamente mais de um protocolo para gerar amplificação do tráfego, reforçando a hipótese deste trabalho.

#	Número de Ataques	Número de Vítimas
1	0	14125
2	1	95
3	2	29
4	3	13
5	4	6
6	5	3
7	7	2
8	12	1

Tabela 8 – Número de ataques multiprotocolo por vítima.

A Tabela 9 apresenta a distribuição de consultas por vítima. A terceira coluna mostra as consultas recebidas por protocolo, sem considerar ataques multiprotocolo e a quarta coluna considera somente ataques multiprotocolo. A média demonstra uma diferença entre o número de consultas recebidas por protocolo em relação a ataques multiprotocolo, com um crescimento de seis vezes. Apesar de um máximo maior por protocolo é possível observar uma distribuição maior de consultas em ataques multiprotocolo.

#	Estatísticas	Por protocolo	Multiprotocolo
1	Média	19510.68	123876.46
2	Desvio padrão	163499.20	458215.14
3	Mínimo	5.00	10.00
4	1 percentil	5.00	35.10
5	5 percentil	7.00	59.00
6	1 quartil	154.00	3689.25
7	Mediana	1283.00	12514.50
8	3 quartil	6837.50	54782.25
9	95 percentil	56882.35	489057.50
10	99 percentil	274831.30	2086023.80
11	Máximo	8599667.00	6463143.00

Tabela 9 – Número de consultas multiprotocolo por vítima.

A Figura 6 apresenta a distribuição de ataques e *scans* recebidos pelo *honeypot* por dia, subdivididos por protocolos (devido à grande variação no número de requisições por protocolo, o eixo y tem escalas diferentes em cada protocolo para facilitar a visualização). É possível apontar a existência de dias em que o *honeypot* não foi utilizado. O SSDP apresentou um período alto de fluxos por dia, que se explica pela existência de inúmeras consultas para vítimas em uma mesma sub-rede; apesar do volume de requisições ser pequeno (≈ 40), o número de vítimas é alto.

A Figura 7 apresenta a distribuição de requisições recebidas pelo *honeypot* por dia. Como já foi apresentado na Tabela 4 é possível destacar a predominância de consultas realizadas para o Chargen, mas existe uma participação dos outros protocolos em ataques DRDoS com exceção de QOTD e Steam, que não chegam a atingir 10 ataques por dia.

4.3 CONSIDERAÇÕES DO CAPÍTULO

Com a avaliação parcial dos dados é possível apontar a existência de ataques DRDoS multiprotocolo. Considerando que este período de coleta é relativamente curto e o *honeypot* está há pouco tempo sendo explorado como vetor para amplificação de tráfego, é possível destacar que a taxa de utilização do *honeypot* tende a aumentar,

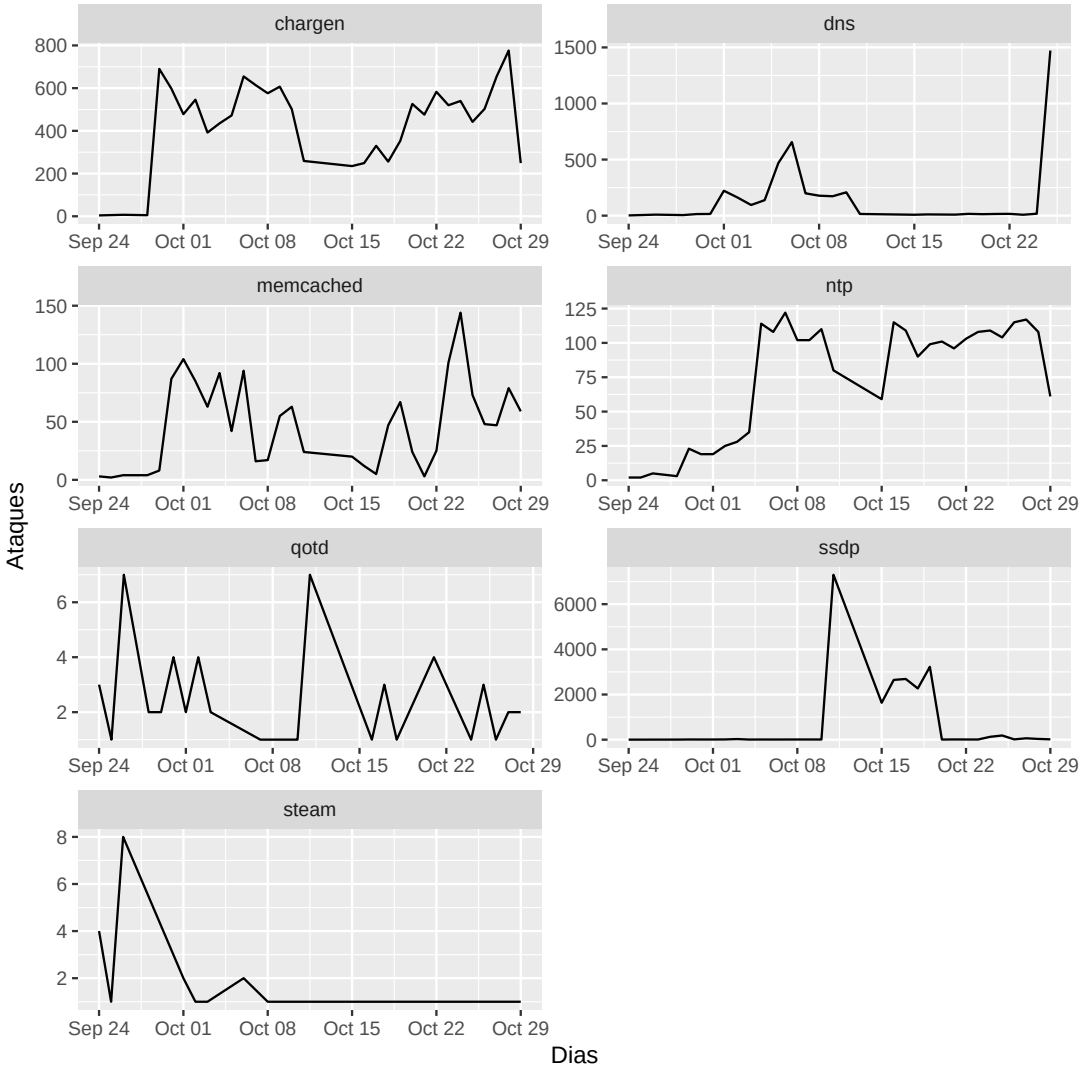

Figura 6 – Distribuição de ataques e *scans* por dia. O eixo y tem escalas diferentes em cada gráfico devido à grande variação no número de requisições por protocolo.

Fonte: O próprio autor

já que ele deve ser encontrado em novas varreduras e ser incorporado em listas de refletores abertos usadas por ferramentas de ataque.

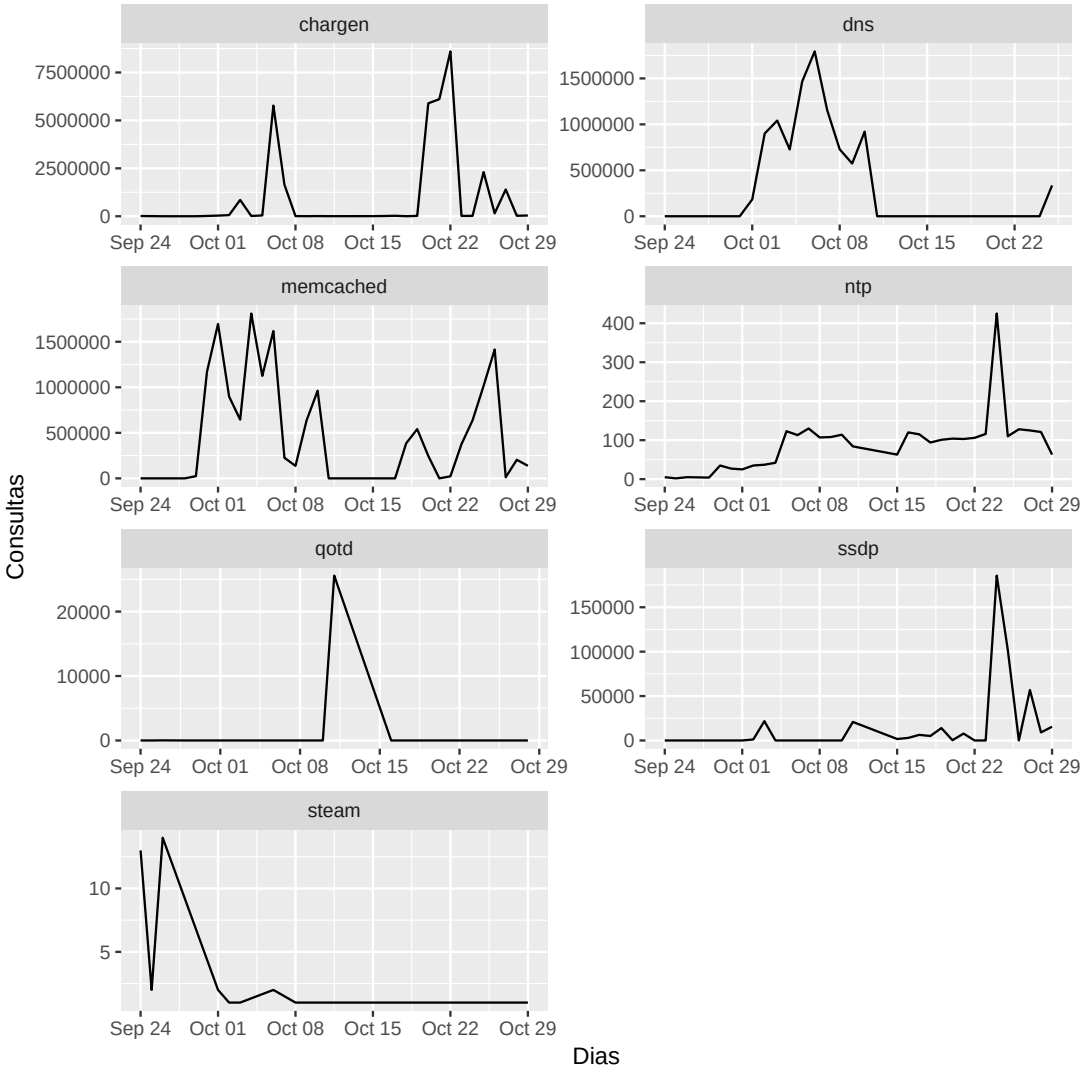

Figura 7 – Distribuição de consultas por dia. O eixo y tem escalas diferentes em cada gráfico devido à grande variação no número de requisições por protocolo.

Fonte: O próprio autor

5 CONSIDERAÇÕES FINAIS

Os ataques DRDoS são amplamente utilizados e apresentam um impacto em decorrência do volume de dados gerado pela amplificação do tráfego. A existência de um conjunto de protocolos de rede que pode ser explorado para a amplificação é um dos fatores que contribui para sua utilização.

Avaliando os estudos realizados sobre ataques DRDoS é possível apontar um escopo não abordado para ataques multiprotocolos. Desta maneira a proposta apresentada consiste na análise de ataques DRDoS multiprotocolo. A coleta de dados está sendo realizada com um *honeypot* voltado para ataques DRDoS, onde um conjunto de protocolos foi desenvolvido para que seja possível avaliar o comportamento de ataques multiprotocolos.

Apesar do tempo pequeno de coleta de dados, já foi possível a identificação de ataques multiprotocolos. Com um período maior de coleta será possível avaliar novos comportamentos e um crescimento na taxa de utilização do *honeypot*. O estudo apresentado até o momento só considera o banco de dados dos dicionários, fornecidos pelo próprio *honeypot*. Em decorrência da necessidade de observar o sistema neste primeiro período o enfoque foi a prevenção de problemáticas na arquitetura, já que o sistema aparenta estar funcionando devidamente as próximas etapas consideram a avaliação das informações coletadas pelo *tcpdump*, ao qual oferecem mais detalhes quanto aos ataques.

O principal obstaculo para as atividades futuras será o processamento destas informações, o volume de dados acaba necessitando de algumas medidas para garantir o correto funcionamento das rotinas. Desta forma deve-se evitar reprocessar informações a cada momento em que novas informações são adicionadas no banco de dados. Como buscar explorar a melhor otimização de consultas a serem realizadas para a análise.

Um conjunto novo de protocolos já esta em desenvolvimento, a princípio mais três protocolos ainda serão adicionados. Estes protocolos tem o intuito de auxiliar em algumas análises, ao qual até o momento não foi possível a identificação de ataques DRDoS, como por exemplo o protocolo da Steam que apresenta uma taxa de utilização muito baixa.

REFERÊNCIAS

AKAMAI. **Akamai [state of the Internet]**. [S.l.], 2014.

AKAMAI. **Akamai [state of the Internet]**. [S.l.], 2016. Threat Advisory: RIPv1 Reflection DDoS.

ANAGNOSTOPOULOS, M. et al. DNS amplification attack revisited. **Computers & Security**, Elsevier, v. 39, p. 475–485, 2013.

ARENDS, R.; AUSTEIN, R. **DNS Security Introduction and Requirements**. 2018. <https://tools.ietf.org/html/rfc4033>.

BAIA, K. Analysis and prevention of memcache udp reflection amplification attack. International Journal of Science, v. 5, 2018.

BECKETT, D.; SEZER, S. Http/2 tsunami: Investigating http/2 proxy amplification ddos attacks. In: IEEE. **Emerging Security Technologies (EST), 2017 Seventh International Conference on**. [S.l.], 2017. p. 128–133.

BIENKOWSKI, T.; ARBOR, N. **No Sooner Did the Ink Dry: 1.7Tbps DDoS Attack Makes History**. 2018. CERT-EU Security Whitepaper 17-003, <https://www.netscout.com/news/blog/security-17tbps-ddos-attack-makes-history> visited in November 2018.

BITAG. Report, **SNMP Reflected Amplification DDoS Attack Mitigation**. 2015. A Near-Uniform Agreement Report.

Computer security handbook. In: BOSWORTH, S.; KABAY, M. E.; WHYNE, E. (Ed.). John Wiley & Sons, Inc., 2012. Disponível em: <https://doi.org/10.1002/9781118851678>.

BREWSTER, T. **Cyber Attacks Strike Zimbabweans Around Controversial Election**. 2013. <https://www.silicon.co.uk/workspace/zimbabwe-election-cyber-attacks-123938?inf_by=5bdcee79671db805298b4e9b> visited in November 2018.

CAIS. **Centro de Atendimento a Incidentes de Segurança**. 2018. <http://www.cais.rnp.br/> visited in September 2018.

CERT. **Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks**. 1996. <https://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1996-21.html>, visited in November 2018.

CERT. **DDoS Quick Guide**. 2014. <https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf> visited in November 2018.

CERT. **Alert (TA14-017A) UDP-Based Amplification Attacks**. 2018. <https://www.us-cert.gov/ncas/alerts/TA14-017A> visited in November 2018.

CERT.BR. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. 2016. Disponível em <http://www.cert.br/docs/whitepapers/ddos/>.

CERT/TCC. **Advisory CA-1999-14 Multiple Vulnerabilities in BIND**. 1999. <https://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1999-14.html> visited in November 2018.

CHESHIRE, S.; KROCHMAL, M. **Multicast DNS**. 2018. <https://tools.ietf.org/html/rfc6762> visited in September 2018.

CHOI, S.-J.; KWAK, J. A study on reduction of ddos amplification attacks in the udp-based cldap protocol. In: IEEE. **Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on**. [S.l.], 2017. p. 1–4.

CORMEN, T. H. et al. **Introduction to Algorithms**. 3rd. ed. Cambridge, MA: MIT Press, 2009.

CORNELL. **Fraud and related activity in connection with computers**. 1984. <https://www.law.cornell.edu/uscode/text/18/1030> visited in November 2018.

COX, J. **The History of DDoS Attacks as a Tool of Protest**. 2014. <https://motherboard.vice.com/en_us/article/d734pm/history-of-the-ddos-attack> visited in November 2018.

CZYZ, J. et al. Taming the 800 pound gorilla: The rise and decline of ntp ddos attacks. In: ACM. **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.], 2014. p. 435–448.

DDOSMON. **Insight into Global DDoS Threat Landscape**. 2018. <https://ddosmon.net/insight/> visited in November 2018.

DEKA, R. K.; BHATTACHARYYA, D. K.; KALITA, J. K. Ddos attacks: Tools, mitigation approaches, and probable impact on private cloud environment. **arXiv preprint arXiv:1710.08628**, 2017.

DENNIS, D. **Perhaps the First Denial-of-Service Attack?** 2010. <http://www.platohistory.org/blog/2010/02/perhaps-the-first-denial-of-service-attack.html> visited in November 2018.

DYN. **DDoS attack against Dyn managed DNS**. 2018. <https://www.dynstatus.com/incidents/nlr4yrr162t8> visited in November 2018.

FENNER, W. **Internet Group Management Protocol, Version 2**. 2018. <https://tools.ietf.org/html/rfc2236>.

GAO, H. et al. An empirical reexamination of global DNS behavior. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, v. 43, n. 4, p. 267–278, ago. 2013. ISSN 0146-4833. <http://doi.acm.org/10.1145/2534169.2486018>.

GARCIA, L. M. **tcpdump & libpcap**. 2010. <https://www.tcpdump.org/> visited in November 2018.

GIT. **git –fast-version-control**. 2018. <https://git-scm.com> visited in September 2018.

GOLAND, Y. Y. et al. **Simple Service Discovery Protocol/1.0 Operating without an Arbiter**. 1999. <https://tools.ietf.org/html/draft-cai-ssdp-v1-03> visited in November 2018.

HEINRICH, T.; LONGO, F. S.; OBELHEIRO, R. R. Experiências com um honeypot DNS: Caracterização e evolução do tráfego malicioso. Joinville, Novembro de 2017. XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).

HENGST, K. Ddos through the internet of things. In: **An analysis determining the potential power of a DDoS attack using IoT devices-Twente Student Conference on IT**. [S.l.: s.n.], 2016.

HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. **Honeypots e Honeynets: Definições e Aplicações**. 2007. <http://www.cert.br/docs/whitepapers/honeypots-honeynets/>.

KARAMI, M.; PARK, Y.; MCCOY, D. Stress testing the booters: Understanding and undermining the business of ddos services. In: INTERNATIONAL WORLD WIDE WEB CONFERENCES STEERING COMMITTEE. **Proceedings of the 25th International Conference on World Wide Web**. [S.l.], 2016. p. 1033–1043.

KHANDELWAL, S. **World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices**. 2016. <https://thehackernews.com/2016/09/ddos-attack-iot.html> visited in September 2018.

KLEPPMANN, M. **Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems**. first. [S.l.]: O'Reilly Media, 2017. v. 1. 624pgs.

KRÄMER, L. et al. Amppot: Monitoring and defending against amplification ddos attacks. In: SPRINGER. **International Workshop on Recent Advances in Intrusion Detection**. [S.l.], 2015. p. 615–636.

KÜHRER, M. et al. Exit from hell? reducing the impact of amplification ddos attacks. In: **USENIX Security Symposium**. [S.l.: s.n.], 2014. p. 111–125.

KÜHRER, M. et al. Hell of a handshake: Abusing tcp for reflective amplification ddos attacks. In: **WOOT**. [S.l.: s.n.], 2014.

KUMAR, S. Smurf-based distributed denial of service (ddos) attack amplification in internet. In: IEEE. **Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on**. [S.l.], 2007. p. 25–25.

LEMOS, R. **How DDoS Attacks Techniques Have Evolved Over Past 20 Years**. 2016. <http://www.eweek.com/security/how-ddos-attacks-techniques-have-evolved-over-past-20-years> visited in November 2018.

LIU, C. et al. Detect the reflection amplification attack based on udp protocol. In: IEEE. **Communications and Networking in China (ChinaCom), 2015 10th International Conference on**. [S.l.], 2015. p. 260–265.

LOPES, W. R. **Ataques DDoS Panorama, Mitigação e Evolução**. 2015. <ftp://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf> visited in November 2018.

MANSFIELD-DEVINE, S. The growth and evolution of ddos. **Network Security**, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 2015, n. 10, p. 13–20, out. 2015. ISSN 1353-4858. Disponível em: <http://dx.doi.org/10.1016/S1353-4858(15)30092-1>.

MEITEI, I. L.; SINGH, K. J.; DE, T. Detection of ddos dns amplification attack using classification algorithm. In: ACM. **Proceedings of the International Conference on Informatics and Analytics**. [S.l.], 2016. p. 81.

MEMCACHED. **Memcached**. 2009. <https://memcached.org> visited in November 2018.

MIRKOVIC, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, v. 34, n. 2, p. 39–53, abr. 2004.

NAZARIO, J. DDoS attack evolution. Elsevier, v. 2008, n. 7, p. 7–10, 2008. Network Security.

NAZARIO, J. **An awesome list of honeypot resources**. 2018. <https://github.com/paralax/awesome-honeypots> visited in November 2018.

NETSCOUT; ARBOR. **Insight into the Global Threat Landscape**. 2017. Netscout Arbor's 13th Annual Worldwide Infrastructure Security Report.

NEWMAN, L. H. **GITHUB Survived the Biggest DDoS Attack Ever Recorded**. 2018. <https://www.wired.com/story/github-ddos-memcached/> visited in September 2018.

NIST. **CVE-1999-1379 Detail**. 1999. <https://nvd.nist.gov/vuln/detail/CVE-1999-1379> visited in November 2018.

NOLLA, A. **Amplification DDoS attackswith game servers**. 2013. <http://grehack.org/files/2013/talks/talk_3_5-nolla-ddos_amplification_attacks_with_game_servers-grehack.pdf> visited in November 2018.

NOROOZIAN, A. et al. Who gets the boot? analyzing victimization by ddos-as-a-service. In: SPRINGER. **International Symposium on Research in Attacks, Intrusions, and Defenses**. [S.l.], 2016. p. 368–389.

PAXSON, V. An analysis of using reflectors for distributed denial-of-service attacks. **ACM SIGCOMM Computer Communication Review**, ACM, v. 31, n. 3, p. 38–47, 2001.

POSTEL, J. **Character Generator Protocol**. 1983. <https://tools.ietf.org/html/rfc864> visited in November 2018.

POSTEL, J. **Quote of the Day Protocol**. 1983. <https://tools.ietf.org/html/rfc865> visited in November 2018.

PRINCE, M. **The DDoS That Almost Broke the Internet**. 2013. <https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/> visited in November 2018.

PRINCE, M. **Technical Details Behind a 400Gbps NTP Amplification DDoS Attack**. 2014. <https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/> visited in November 2018.

PROLEXIC. **An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks**. 2012. Part II of the DrDoS White Paper Series.

PROLEXIC. **Distributed Reflection Denial of Service (DrDoS) Attacks An Introduction to the DrDoS White Paper Series**. 2013. <https://news.asis.io/sites/default/files/Distributed_Reflection_DoS_Attacks_White_Paper_A4_031513.pdf> visited in November 2018.

REVUELTO, V.; MEINTANIS, S.; SOCHA, K. **DDoS Overview and Response Guide**. 2017. CERT-EU Security Whitepaper 17-003, <https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf> visited in November 2018.

RIJSWIJK-DEIJ, R. van; SPEROTTO, A.; PRAS, A. Dnssec and its potential for ddos attacks: a comprehensive measurement study. In: ACM. **Proceedings of the 2014 Conference on Internet Measurement Conference**. [S.l.], 2014. p. 449–460.

ROSSOW, C. Amplification hell: Revisiting network protocols for ddos abuse. In: **In Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS**. [S.l.: s.n.], 2014.

RUDMAN, L.; IRWIN, B. Characterization and analysis of ntp amplification based ddos attacks. In: IEEE. **Information Security for South Africa (ISSA), 2015**. [S.l.], 2015. p. 1–5.

RYBA, F. J. et al. Amplification and drdos attack defense–a survey and new perspectives. **arXiv preprint arXiv:1505.07892**, 2015.

SANTANNA, J. J. et al. Booters—an analysis of ddos-as-a-service attacks. In: IEEE. **Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on**. [S.l.], 2015. p. 243–251.

SARGENT, M. et al. On the potential abuse of igmp. **ACM SIGCOMM Computer Communication Review**, ACM, v. 47, n. 1, p. 27–35, 2017.

SHADOWSERVER. **The Shadowserver Foundation**. 2004. <https://www.shadowserver.org/wiki/pmwiki.php/Main/HomePage> visited in September 2018.

SHARMA, R.; GULERIA, A.; SINGLA, R. Characterizing network flows for detecting dns, ntp, and snmp anomalies. In: **Intelligent Computing and Information and Communication**. [S.l.]: Springer, 2018. p. 327–340.

SHODAN. **The search engine**. 2013. <https://www.shodan.io/> visited in September 2018.

SIA, K. C. Ddos vulnerability analysis of bittorrent protocol. **UCLA: Techical Report**, Citeseer, 2006.

SIEKLIK, B.; MACFARLANE, R.; BUCHANAN, W. J. Evaluation of tftp ddos amplification attack. **Computers & security**, Elsevier, v. 57, p. 67–92, 2016.

SKOTTLER. **February 28th DDoS Incident Report**. 2018. <https://githubengineering.com/ddos-incident-report/> visited in September 2018.

SPECHT, S. M.; LEE, R. B. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In: **ISCA PDCS**. [S.l.: s.n.], 2004. p. 543–550.

SPITZNER, L. Honeypots: Catching the insider threat. In: **Proceedings of the 19th Annual Computer Security Applications Conference**. Washington, DC, USA: IEEE Computer Society, 2003. (ACSAC '03), p. 170–. ISBN 0-7695-2041-3. <http://dl.acm.org/citation.cfm?id=956415.956438>.

SU, T.-J. et al. Attack detection of distributed denial of service based on splunk. In: IEEE. **Advanced Materials for Science and Engineering (ICAMSE), International Conference on**. [S.l.], 2016. p. 397–400.

SUN, X.; TORRES, R.; RAO, S. Preventing ddos attacks on internet servers exploiting p2p systems. **Computer Networks**, Elsevier, v. 54, n. 15, p. 2756–2774, 2010.

THOMAS, D. R.; CLAYTON, R.; BERESFORD, A. R. **1000 days of UDP amplification DDoS attacks**. 2017. 79–84 p. Electronic Crime Research (eCrime), 2017 APWG Symposium on.

WOODY, C.; SHOEMAKER, D.; MEAD, N. **Foundations for Software Assurance**. 2012. <https://www.us-cert.gov/bsi/articles/knowledge/principles/foundations-software-assurance> visited in November 2018.

ZARGAR, S. T.; JOSHI, J.; TIPPER, D. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. **IEEE communications surveys & tutorials**, IEEE, v. 15, n. 4, p. 2046–2069, 2013.

ZETTER, K. **Lazy Hacker and Little Worm Set Off Cyberwar Frenzy**. 2009. <https://www.wired.com/2009/07/mydoom/> visited in November 2018.

ZHANG, B.; ZHANG, T.; YU, Z. Ddos detection and prevention based on artificial intelligence techniques. In: IEEE. **Computer and Communications (ICCC), 2017 3rd IEEE International Conference on**. [S.l.], 2017. p. 1276–1280.