ANÁLISE DO GNS3 COMO FERRAMENTA AUXILIAR AO ENSINO DO PROTOCOLO HTTP POR MEIO DA COMUNICAÇÃO ENTRE REDES SIMULADAS

Christopher Renkavieski

Lucas Machado Gutierrez

Marlon Henry Schweigert

Joinville

2016

Christopher Renkavieski
Lucas Machado Gutierrez
Marlon Henry Schweigert

ANÁLISE DO GNS3 COMO FERRAMENTA AUXILIAR AO ENSINO DO PROTOCOLO HTTP POR MEIO DA COMUNICAÇÃO ENTRE REDES SIMULADAS

Relatório de Trabalho de Conclusão de Curso (TCC) apresentado ao Curso de Graduação em Ciência da Computação, da Universidade do Estado de Santa Catarina (UDESC), como requisito parcial da disciplina de Trabalho de Conclusão de Curso.

Orientador: Profº Charles Christian Miers

Joinville
2016

Christopher Renkavieski
Lucas Machado Gutierrez
Marlon Henry Schweigert

ANÁLISE DO GNS3 COMO FERRAMENTA AUXILIAR AO ENSINO DO PROTOCOLO HTTP POR MEIO DA COMUNICAÇÃO ENTRE REDES SIMULADAS

Relatório de Trabalho de Conclusão de Curso (TCC) apresentado ao Curso de Ciência da Computação da UDESC, como requisito parcial para a obtenção do grau de BACHAREL em Ciência da Computação.

BANCA EXAMINADORA

Resumo

Devido ao grande crescimento e popularização da Internet nos últimos anos, ataques como DDoS estão cada vez mais frequentes, sendo difícil encontrar usuários que ao realizar algum serviço online não tenha sofrido com um ataque. O monitoramento do tráfego de um serviço de DNS recursivo, pode ser realizado para a descoberta de ataques DDoS. Uma ferramenta com estas características é o DNSpot, sendo responsável por registrar o tráfego de envio a um serviço de DNS recursivo aberto. Este trabalho de conclusão de curso busca realizar uma nova pesquisa sobre o DNSpot, realizando uma coleta de dados em um período entre oito e nove meses, realizando uma análise de tendências, com o tempo de vida dos nomes usados em ataques DDoS e com que frequência surgem novos nomes.

Palavras-chave: *Domain Name Systeam (DNS)*, *Segurança em redes*, *DNSpot*.

Abstract

Due to the great growth and popularization of the Internet in recent years, as DDoS attacks are becoming more frequent, and difficult to find users to perform some online service has not suffered an attack. Monitoring traffic recursive DNS service can be performed for the discovery of DDoS attacks. A tool with these characteristics is the DNSpot, being responsible for recording sending traffic to an open recursive DNS service. This course conclusion work tries to make a new search on DNSpot, performing a data collection in a period between eight and nine months conducting an analysis of trends, with the lifetime of the names used in DDoS attacks and how often come new names.

Palavras-chave: *Offline Recognition*, *Handwriting Recognition*, *Mathematical Expression*.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

CTO	Chief Technology Officer
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
NAT	Network Address Translation
OVH	Hosted service provider company
RR	Resource Record

1 Introdução

O DNS (*Domain Name System*) (**??**) é um sistema distribuído de resolução de nomes que desempenha um papel fundamental na Internet. Sua principal funcionalidade é traduzir nomes de domínio mais facilmente memorizáveis (como `www.udesc.br`) em endereços IP numéricos (como 200.19.105.194), que são usados pelos protocolos subjacentes de rede para localizar e identificar nós na Internet.

Em vista de sua ampla utilização, o DNS também é tanto um alvo quanto um vetor de ataques. As principais ameaças envolvendo o DNS são resumidas por (**??**), que as divide em duas classes, aquelas em que o DNS é o alvo e aquelas que são oportunizadas pelo DNS. A classe de ameaças ao DNS inclui:

- Negação de serviço: impedir o acesso de usuários ao DNS, com isso prejudicando ou mesmo bloqueando o seu acesso à Internet;
- Corrupção de dados: modificar dados publicados no DNS de forma não autorizada, o que pode, por exemplo, levar usuários a acessar sites ilegítimos (como páginas falsas de bancos ou comércio eletrônico);
- Exposição de informação: revelar informações sobre o comportamento dos usuários, como histórico de sites web acessados (**??**).

O DNS também pode ser usado como um veículo de ataques. A classe de ameaças oportunizadas pelo DNS abrange:

- Ataques de amplificação: servidores DNS mal configurados podem ser usados para realizar ataques de negação de serviço contra terceiros (**??**);
- *Fast flux* DNS: servidores usados para propósitos nefastos, como propagação de software malicioso ou controle remoto de *botnets*, podem ter diversos endereços IP distintos associados. Uma fração desses endereços são associados a um nome DNS específico e trocados com alta frequência, de modo a dificultar a localização dos servidores e a identificação dos seus responsáveis, e até mesmo balancear carga entre servidores (**??**);

- Exfiltração de dados: como o tráfego DNS geralmente não é barrado ou modificado por *firewalls*, ele é usado com frequência para transmitir dados sensíveis (capturados no curso de uma invasão) sem que isso seja percebido pelos mecanismos de defesa da rede.

O maior ataque DDoS foi registrado em setembro de 2016, que conseguiu alcançar picos de 1 Tbps de tráfego.

O serviço de hospedagem OVH (*Hosted service provider company*) na França foi a vítima, dos ataques que conseguiu alcançar a marca de 1 Tbps por segundo, os ataques acabaram utilizando *Smart Devices* para a realização dos ataques. Dispositivos inteligentes faziam parte da *botnet* que foi utilizada para a realização dos ataques.

Octave Klaba, o fundador e CTO (*chief technology officer*) da OVH, apresentou os diversos ataques que foram realizados, e o volume de tráfego que excedia 100 Gbps e atingiam picos de 799 Gbps. O ataque foi realizado por mais de 152000 dispositivos da IoT (*Internet of Things*), que incluíam câmeras e gravadores de vídeo comprometidos (**??**).

Para observar o comportamento de atacantes contra servidores DNS, foi desenvolvido o DNSpot (**??**), um *honeypot* DNS com o propósito de monitorar e registrar o tráfego enviado a um serviço de DNS recursivo aberto. *Honeypots* são recursos computacionais de segurança, cujo objetivo é serem sondados, atacados ou comprometidos em um ambiente controlado (**??**).

O DNSpot foi implantado na rede da UDESC durante 49 dias, entre 09/09/2015 e 28/10/2015. Nesse período, o *honeypot* processou mais de 4 milhões de consultas DNS, mais de 99% das quais relacionadas a ataques distribuídos de negação de serviço (DDoS, *Distributed Denial of Service*). A análise dos dados coletados revelou a existência de nomes DNS projetados para maximizar a amplificação de tráfego nesse tipo de ataque. Conforme mostrado na Tabela 1.1, nove dos 10 nomes ou registros de recursos (RRs, *resource records*) que apareceram com maior frequência não podem mais ser aproveitados em ataques DDoS, seja porque não estão mais ativos ou porque agora geram respostas consideravelmente menores; uma nova verificação dos dados foi realizada em 19/08/2016, cerca de 10 meses após o fim do estudo original. Um outro fato observado no estudo original foi o desaparecimento de domínios usados em ataques DDoS; isso foi constatado especificamente para o domínio l3x.ru, que aparece na Tabela 1.1.

O objetivo deste trabalho de conclusão de curso é realizar uma coleta de dados com

RR	Ativo?	Resposta (bytes)	
		2015	**2016**
hehehe.ru. ANY	sim	3850	221
mototrazit.ru. ANY	não	3853	–
vp47.ru. ANY	sim	3959	151
l3x.ru. A	não	3875	–
. ANY	sim	1503	1790
gransy.com. ANY	sim	3591	594
vp47.ru A	sim	3892	91
lifemotodrive.ru. ANY	não	3969	–
nhl.msk.su. ANY	sim	3965	341
oi69.ru. A	sim	3637	91

Tabela 1.1: Situação em 19/08/2016 dos 10 RRs observados com maior frequência por Longo (2015)

o DNSpot durante um período significativamente mais longo que o estudo original. Isso não apenas permitirá comparar dados recentes com os dados originais, mas principalmente analisar a evolução da atividade maliciosa ao longo de vários meses, buscando respostas para questões como:

- Com que frequência aparecem nomes e domínios anômalos, i.e., projetados para ataques DDoS?
- Por quanto tempo esses domínios permanecem válidos e são usados em ataques?
- Existe alguma característica sazonal no tipo ou no volume de ataques?
- É possível correlacionar tráfego de ataques DDoS com fatores externos, como questões geopolíticas ou econômicas?
- Quais as principais características de um ataque DDoS para um serviços de jogos, existe alguma diferença?

Visando um período de coleta entre oito e nove meses, que vai contribuir com resultados que não conseguiram ser observados no primeiro estudo, devido ao tempo.

1.1 Objetivo

Objetivo geral: Fazer uma análise da evolução temporal de dados coletados pelo DNSpot.

1.2 Objetivos Específicos

Objetivos específicos: Segue uma lista dos principais objetivos a serem realizados no estudo.

- Realizar uma revisão bibliográfica abrangendo segurança do DNS, *honeypots* e trabalhos relacionados;
- Operacionalizar armazenamento de longo prazo no DNSpot;
- Fazer uma coleta de longa duração;
- Comparar os resultados novos com os anteriores;
- Analisar a evolução temporal dos dados observados.

1.3 Metodologia

Este trabalho de conclusão de curso consiste em uma pesquisa aplicada, tendo como principais métodos a pesquisa bibliográfica e o estudo de caso. Primeiramente, serão realizados um estudo sobre o DNSpot e uma revisão bibliográfica sobre aspectos de segurança do DNS e *honeypots*. Nesta fase será avaliada a necessidade de adaptações no DNSpot para coleta de dados de longo prazo. Atualmente, os dados coletados pelo DNSpot são armazenados em um banco de dados, o qual é rotacionado manualmente quando se torna muito grande. Para uma coleta de longo prazo, possivelmente será necessário automatizar o procedimento de rotação da base de dados.

Após, será iniciada a coleta de dados para a realização da análise, juntamente com o estudo.

Por fim será realizado a comparação com os dados originais (**??**) e observando como eles evoluem ao longo do tempo. Serão investigadas tendências de mais longo prazo,

como tempo de vida dos nomes usados em ataques DDoS e com que frequência surgem novos nomes, por exemplo.

1.4 Estrutura do Trabalho

Este trabalho está dividido em cinco capítulos. O Capítulo 1 é uma introdução sobre o reconhecimento de expressões matemáticas, as possíveis aplicações, os tipos de reconhecimento e as etapas do reconhecimento. No Capítulo 2 são apresentados os fundamentos básicos de processamento de imagens, aprendizado de máquina e análise estrutural. O Capítulo 3 é uma revisão dos métodos utilizados na literatura para cada uma das etapas do reconhecimento de expressões matemáticas. O Capítulo 4 apresenta a proposta de uma aplicação *web* que utiliza um reconhecedor de expressões matemáticas e mostra quais métodos serão implementados em cada uma das etapas. O Capítulo 5 são as considerações finais deste trabalho, o que foi estudado, o que foi proposto, o que foi feito até o momento e qual serão as próximas etapas.

2 Fundamentação Teórica

Este capítulo introduz os conceitos necessários para a compreensão do restante do trabalho. A Seção 2.1 apresenta o *Domain Name System* (DNS). A Seção 2.2 discute *honeypots*. Na seção 2.3 é descrito o DNSpot, um *honeypot* específico para servidores DNS recursivos.

2.1 Domain Name System

O *Domain Name System* (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 (**??**).

2.1.1 Definição

DNS é um sistema distribuído de banco de dados, cujo objetivo original era permitir que recursos de rede sejam identificados por nomes em vez de endereços de baixo nível (**??**). Em particular, o DNS permite que usuários refiram-se a nós da rede usando nomes (como `www.udesc.br`) no lugar dos endereços IP (como 200.19.105.51) efetivamente usados para a comunicação entre esses nós. Ao longo do tempo, o escopo do DNS foi ampliado, basicamente devido a sua ampla disseminação, passando a associar vários tipos diferentes de dados a nomes de domínio (**??**). Dada a sua estrutura com abrangência global e a sua ubiquidade, o DNS deve ter boa escalabilidade e desempenho, oferecendo para os usuários baixa latência em redes de larga escala (**??**). O DNS é crítico para o funcionamento da maioria dos serviços encontrados na Internet: embora sempre seja possível referir-se a um nó (por exemplo, um servidor web) usando seu endereço IP, os usuários buscam resolver os endereços utilizando o seu nome (**??**). Além disso, o DNS introduz uma camada de indireção, permitindo, por exemplo, que um nó mude seu endereço IP de forma transparente para os usuários e aplicações que desejem se comunicar com ele.

2.1.2 Hierarquia

O espaço de nomes do DNS segue uma estrutura em árvore (**??**). A cada nó da árvore, seja um nó interno ou uma folha, corresponde um conjunto de recursos, que pode ser vazio. Cada nó possui um rótulo com até 63 bytes de comprimento. Nós irmãos devem ter rótulos distintos, mas o mesmo rótulo pode ser usado para nós que não são irmãos. A raiz da árvore possui um rótulo com comprimento zero, tipicamente representado por um ponto (“.”). O nome de domínio de um nó é a lista de rótulos que formam o caminho do nó até a raiz da árvore. Por exemplo, na árvore DNS mostrada na Figura, o nó mais à esquerda possui o nome de domínio `irs.treasury.gov.`; em geral, o ponto final é omitido, quando isso não causar ambiguidade.

1. eliminar a parte de UNIX da figura

2. incluir um rótulo “irs” em outra subárvore, e mostrar que eles podem coexistir

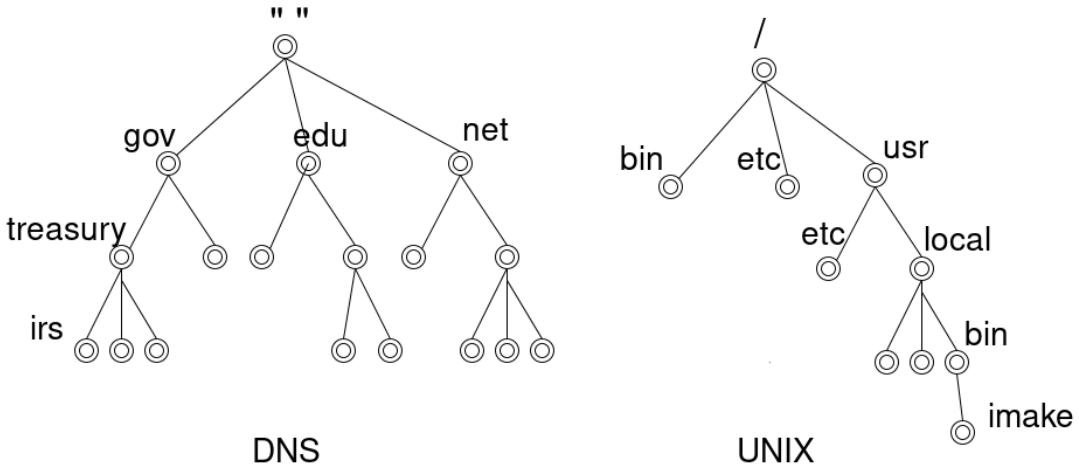

Figura 2.1: DNS vs UNIX estrutura

Na árvore DNS, cada subárvore é um domínio. Um conceito chave no DNS é a administração descentralizada, que consiste em delegar a administração de domínios a entidades autônomas (**??**). A administração de um domínio engloba a criação de nós nesse domínio e a definição dos recursos associados a nomes pertencentes ao domínio. Cada domínio possui um ou mais servidores responsáveis pelos seus nomes, chamados de servidores autoritativos. Em geral, esses servidores são configurados de forma que um deles (servidor primário ou mestre) é o repositório central de dados para o domínio, e os demais (servidores secundários ou escravos) apenas replicam os dados do servidor primário para oferecer balanceamento de carga e tolerância a falhas (**??**). A divisão entre servidores mestres e escravos é transparente para os usuários

do DNS.

Reaproveitei a citação, mas a ordem correta dos autores é (Albitz e Liu 2006), não (Liu e Albitz 2006).

A figura 2.2 ilustra a delegação do subdomínio `treasury.gov` pelo domínio `gov`. A delegação é efetivada atribuindo-se um conjunto de servidores autoritativos que irão administrar os nomes em `treasury.gov` de forma autônoma. Um conceito associado ao de domínio é o conceito de zona, que abrange todas as partes de uma subárvore que não estão delegadas; por exemplo, na figura 2.2 a zona *gov* contém nomes de domínios que forem terminados em *gov* e não estejam em nenhuma zona de delegação.

- **Parece-me que seria mais fácil visualizar a delegação de um subdomínio de 3o nível (por exemplo, `cct.udesc.br`; a zona `udesc.br` conteria `ceart.udesc.br` mas não `cct.udesc.br`). A delegação de um domínio de 2o nível (como `treasury.gov`), embora tecnicamente seja a mesma coisa, é mais difícil de visualizar, pois as pessoas têm dificuldade de imaginar um domínio `gov`.**
- **Também neste caso retire a árvore de UNIX**

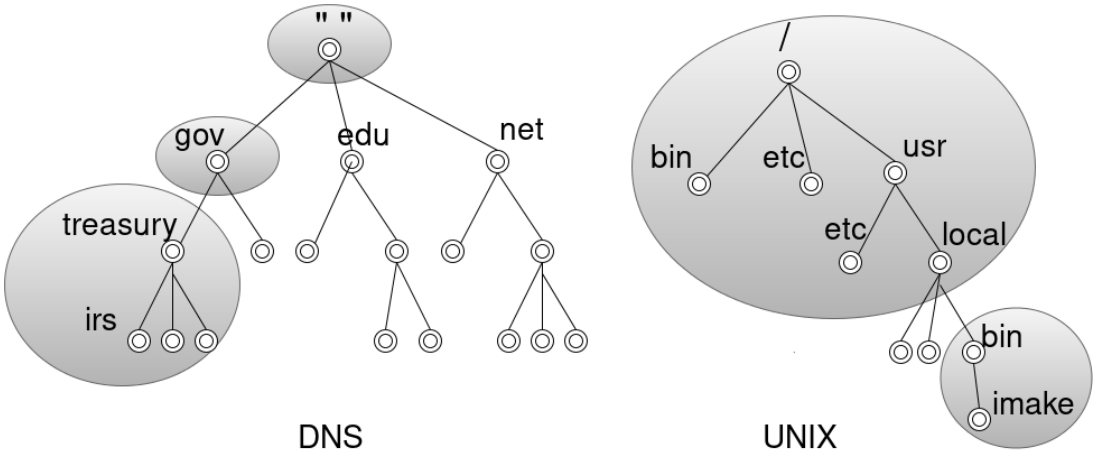

Figura 2.2: DNS vs UNIX Delegação

A solução de um domínio como *host.tex*

2.1.3 Resolução de nomes

2.1.4 Fatores de Segurança

2.1.5 Nome de Domínio

2.2 Honeypot

A mensagem aqui deveria ser que honeypots oferecem uma forma controlada de observar o comportamento dos atacantes, o que é importante para conhecer suas táticas, motivações e ferramentas e assim poder criar novas defesas ou melhorar as defesas existentes. Pontualmente, a última frase é aproveitável, mas as duas primeiras precisam ser reescritas.

Ataques são realizados após uma massiva busca por falhas de seguranças, ao encontrarem falhas existe a tentativa de invasão de uma determinada rede. Uma maneira desenvolvida para a identificação, análise ou controle destas tentativas de invasão é o *honeypot*. Sua mentalidade é a de criar um ambiente isolado onde se possa monitorar tentativas de ataques em uma determinar rede, visando armazenar informações dos ataques recebidos.

2.2.1 Definição

Inclua uma referência ao final da 1a frase.

O *honeypot* é um recurso computacional com o objetivo de ser sondado, atacado ou até mesmo comprometido. Geralmente o *honeypot* é um *host* Internet, possuindo um endereço IP público, mas que não hospeda nenhum serviço anunciado publicamente. Qualquer interação realizada com o *honeypot* já pode-se considerar suspeita, já que é necessário a realização de uma varredura para a descoberta do endereço de IP do *honeypot*. O sistema deve ser monitorado de forma discreta, para garantia que o atacante não suspeite do sistema, e acabe descobrindo o seu monitoramento (**??**).

A estrutura que pode ser observada na figura 2.3, leva em consideração o funcionamento do *honeypot* em uma rede, como retratado buscando esconder quaisquer suspeitas que um usuário que busque atacar a rede consiga identificar.

- **Em relação à figura, é muito pouco recomendável colocar o honeypot junto da rede interna, o melhor seria colocá-lo como uma perna adicional do firewall. Observo aqui que o DNSpot está na nossa rede interna, mas isso só ocorre porque ele é um honeypot para uma aplicação específica, e a conveniência de mantê-lo na rede interna compensa o pequeno risco de que ele seja comprometido e usado como plataforma para outros ataques.**

- **Outro ponto é que olhando a figura o leitor não consegue ver nenhum elemento que permita que o honeypot não desperte suspeitas. Esse ponto, aliás, já é tratado na última frase do parágrafo anterior, e pode ser omitido aqui. Sugiro colocar uma figura e explicar de que forma colocar o honeypot em uma rede segregada, por exemplo, facilita a monitoração e a contenção do tráfego; se quiser, acrescente a necessidade de contenção de tráfego originado no honeypot no parágrafo anterior.**

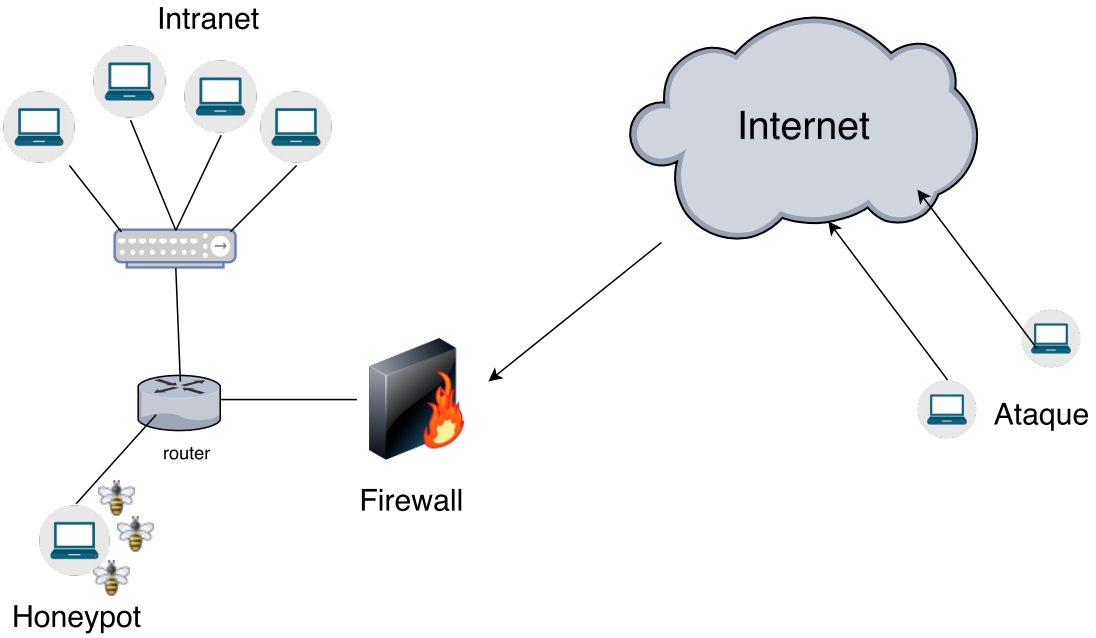

Figura 2.3: Honeypot

2.2.2 Honeynet

Cuidado, uma honeynet é uma rede que abriga um conjunto de honeypots, geralmente distintos (por exemplo, usando sistemas operacionais diferentes). Essa discussão que você colocou aqui sobre a estrutura da rede pode aplicar-se quase da mesma forma a um honeypot isolado, pois ele precisa de elementos auxiliares para prover conectividade, monitorar e conter o tráfego.

Uma *Honeynet* é considera uma rede onde o *Honeypot* está localizado, retratando os dispositivos que compõem esta estrutura. Uma *Honeynet* pode estar composta por alguns elementos como:

- A estrutura pode ser composta por diversos computadores;
- *Firewall*, responsável pela realização de contenção e coleta de informações;
- IDS (Intrusion Detection System) tem o objetivo de observar a rede, buscando atividades em comum ou não autorizadas que podem danificar o sistema;
- roteadores, *switches* e hubs para a composição da estrutura de rede (**??**)

O baixo custo e a interação do atacante com um ambiente real, contribuem com um estudo sobre as ferramentas utilizadas e vulnerabilidades exploradas.

O parágrafo abaixo confunde conceitos. Uma honeynet virtual consiste em um conjunto de honeypots implementados em máquinas virtuais em um mesmo host físico (cf. `http://old.honeynet.org/papers/virtual/`); em uma honeynet real, cada honeypot é um host físico separado. Um honeypot/honeynet de pesquisa tem o propósito de estudar o comportamento dos atacantes; em contrapartida, um honeypot/honeynet de produção tem o objetivo de detectar ataques e responder a eles (cf. `http://www.it-docs.net/ddata/792.pdf`, p. 62). Acho que uma ideia aqui é pensar o que você precisa explicar para tornar o texto autocontido. Não vejo muito sentido em esmiuçar conceitos de honeypots e honeynets porque você não vai propor uma nova ferramenta, mas usar uma que já existe; o importante é que o leitor entenda o que é o DNSpot e suas principais características, e não que ele raciocine sobre as escolhas de projeto do DNSpot (isso compete ao TCC do Felipe).

Existem duas classificações para os *honeypots*, uma rede projetada especificamente para ser atacada e testada, visando a utilização de mecanismo de controle é conhecida como

honeynet, e uma rede com alta interatividade que busca obter informações dos usuários que estão realizando o ataque, também conhecida como *honeynets virtuais* ou *honeypot* de pesquisa (**??**).

2.2.3 Aplicação

Os *honeypots* podem ser classificados em duas categorias, *honeypot* de alta e baixa interatividade (como apresentado na 2.2.2). O *honeypot* de baixa interatividade busca identificar ataques internos e varreduras, também realiza identificação de máquinas comprometidas e códigos maliciosos. Já por outro lado o *honeypot* de alta interatividade apresenta risco para a rede, podendo ser utilizado com o mesmo propósito do *honeypot* de baixa interatividade, seu principal objetivo é estudar o comportamento detalhadamente dos atacantes, juntamente com técnicas e ferramentas utilizadas para explorar alguma vulnerabilidade (**??**).

Aplicação na rede

2.3 DNSpot

O DNSpot é um *honeypot* projetado especificamente para monitorar e analisar o tráfego DNS (**??**). Seu objetivo é permitir a observação das interações de usuários potencialmente maliciosos com servidores DNS recursivos.

2.3.1 Definição

2.3.2 Arquitetura

A arquitetura do DNSpot pode ser observada na figura 2.4. Ele possui um *proxy* que escuta na porta 53/UDP, que é a porta padrão do serviço DNS. Ao receber uma consulta, o *proxy* será responsável por armazenar a consulta em um banco de dados e logo em seguida repassá-la a um servidor DNS recursivo real. Esse servidor real, que aceita apenas consultas originadas na própria máquina, vai interagir com servidores autoritativos na Internet para a resolução desta consulta. Por último, o *proxy* irá receber a resposta do servidor recursivo, armazená-la no banco de dados e encaminhá-la para o cliente que enviou a consulta (**??**).

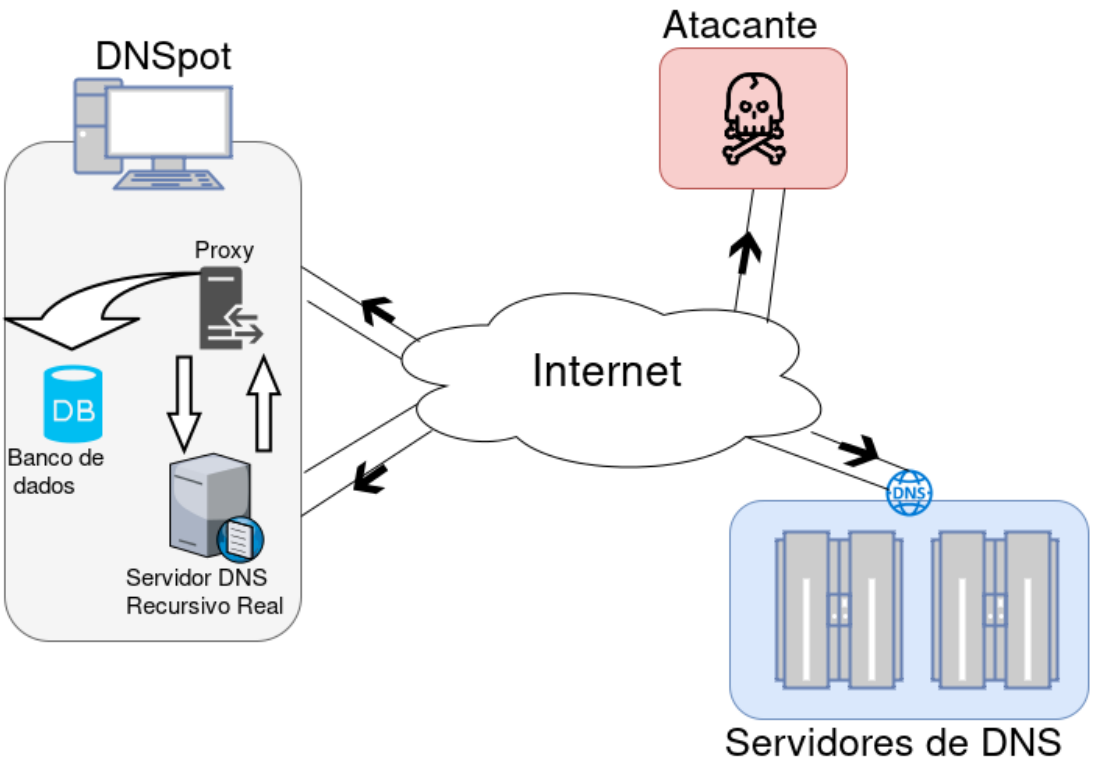

Figura 2.4: Arquitetura DNSpot

O texto abaixo confunde dois mecanismos distintos. O SERVFAIL aleatório é para simular um servidor DNS inconfiável, tentando não levantar suspeitas caso o DNSpot seja desligado ou não consiga processar algumas consultas. Por sua vez, a limitação de consultas funciona como um mecanismo de contenção do tráfego gerado pelo DNSpot; ele permite que um usuário humano interaja com o honeypot, mas restringe a quantidade de tráfego gerada em caso de ataques de DoS por reflexão.

O critérios de decisão escolhidos foram dois:

1. Randomização: uma porcentagem é definida para as consultas, determinando se receberão uma resposta em tempo real ou não, e o *proxy* faz uma decisão aleatória para determinar se será respondido a consulta ou será retornado um erro;

2. Limitação: um limite diário é determinado para o número de consultas atendidas para cada endereço IP de origem; caso o limite seja atingido o *proxy* passa a ignorar novas consultas do mesmo endereço, até o dia seguinte (onde a atividade é retornada novamente) (**??**).

2.4 Estatísticas

Acho que aqui você queria comentar os resultados do DNSpot, certo? Nesse caso, deveria ser uma *subsection*, não uma *section*.

3 Trabalhos Relacionados

Os trabalhos encontrados visam observar ataques DDoS em servidores raiz, ou a análise do comportamento de algumas características na rede. Existe diferenças nos períodos e tipos de análise realizadas.

Está seção busca apresentar algumas destas características e demonstrar algumas relações e diferenças com o trabalho apresentado. Dentre as diversas áreas de estudo sobre o DNS, como monitoramento, análise e detecção de anomalias

3.1 Conceitualização

David Conrad descreve primeiramente em seu trabalho (**??**), conceitos para o entendimento do DNS e sua funcionalidade, ainda demonstrando uma conceitualização histórica. O trabalho demonstra a necessidade dos serviços do DNS para o funcionamento da *Internet*, juntamente com todas as ameaças que este serviço possui.

3.2 Análises

Roberto Perdisci busca apresentar em seu trabalho (**??**)

3.3 Comparativo

Para melhor entender as relações entre cada trabalho apresentando na seção 3, foi criado a tabela **??** onde é apresentando as principais características de cada trabalho.

4 Proposta

O objetivo deste trabalho é desenvolver um estudo sobre a evolução temporal de dados coletados pelo DNSpot. Será levado em consideração as informações coletadas em um estudo anterior (**??**).

O estudo observou interações de usuários potencialmente maliciosos com servidores DNS recursivos, observando a atitude tomada pelos usuários. A ferramenta foi implantada na rede da Universidade do Estado de Santa Catarina (UDESC), por um período de 49 dias.

Com as informações apresentadas pelo estudo (**??**), será possível observar o surgimento de algumas características que não foram possíveis ser analisadas em um período de (49 dias). Possibilitando entender o comportamento de certos ataques não observados em outros estudos devido ao período que a análise foi proposta.

Levando em consideração os trabalhos apresentados na seção 3, é possível destacar os períodos de observação das redes, muitas das vezes por não serem desenvolvidos em períodos grandes de tempo, não é possível a realização de certas análise. Este trabalho busca apresentar uma análise em um período grande de tempo (6 meses), para a realização de uma análise evolucionária em relação aos dados observados.

Para efetuar a análise algumas modificações foram realizadas no DNSpot, focando em modificar algumas características do sistema, garantindo um melhor funcionamento em um período maior de tempo. Como relatado no trabalho (**??**), foram encontrados problemas devido ao crescimento do banco de dados, o que é um problema ao se realizar uma análise maior como a deste trabalho.

A solução aborda foi a remoção de alguns campos que eram salvas no banco de dados, com isto o crescimento do banco foi controlado, mas ainda é possível observar que o banco vai apresentar um crescimento levando em consideração o período de análise.

4.0.1 Implantação

Para a realização da coleta de dados, uma máquina foi disponibilizada pela UDESC. A máquina foi implantada na rede interna da universidade, onde está realizando a coleta de

dados, que iniciaram no dia 17/09/2016.

A rede utiliza endereços reservados, por este motivo é necessário a utilização do NAT (Network Address Translation) para realizar o redirecionamento do tráfego para porta 53/UDP. O NAT é um método utilizado para remapear espaços de endereços IPs, realizando a modificação no cabeçalho dos pacotes no momento em que estes se encontram no dispositvo de roteamento (**??**).

A configuração do *hardware* e *software* da máquina utilizada, segue:

- Sistema Operacional: OpenBSD 5.7 i386;
- Processador: Intel Core2 Duo CPU E6550 @ 2.33GHz (“GenuineIntel"686-class);
- Memória RAM: 1 GB;
- Servidor DNS recursivo: Unbound, versão 1.5.2;
- Python, versão 3.4.2;
- DNSLib, versão 0.9.4;
- SQLIte3, versão 3.8.6.

A máquina está localiza em um dos laboratórios da UDESC, onde realiza a coleta de dados 24/7, o serviço é verificado todos os dias para a garantia do seu funcionamento.

Durante o período que o sistema já esta executando as coletas, ocorreram algumas interrupções do serviço devido a queda de energia e interrupção do *firewall* que da acesso a *Internet* (consequencia da queda de energia).

4.0.2 Tabelas no SQLite

4.0.3 Proposta de testes

Levando em consideração os trabalhos apresentados na seção 3, e o trabalho realizado pelo (**??**), foi determinar uma proposta de testes para este trabalho. A proposta leva em consideração algumas características observadas em trabalhos anteriores, e algumas propostas em comum, para realização de um comparativo entre os trabalhos.

Com os diferentes **períodos de monitoramento**, será possível realizar uma análise quanto a quantidade de informações capturadas em períodos diferentes. E realizar uma comparação entre a coleta realizada em um período inferior de tempo do *Longo:2015:tcc*.

Com o total de **Transações** será possível realizar uma contagem do número de usuários com intenção maliciosa, já que é necessário a descoberta do endereço, como se trata de um servidor DNS não anunciado. Também será possível verificar o número de requisições que não foram respondidas e as transações ignoradas.

O **Volume de dados em bytes** ajudara para a descoberta dos tamanhos das consultas mais comuns juntamente com o tamanho das consultas e respostas solicitadas.

Clientes IP, para apresentar as localizações geográficas, juntamente com os endereços que realizaram o maior número de consultas. **Domínios** para o número de transações. Distribuição empírica de requisições por **RR** e número de transações.

Ataques DoS visando o tamanho de consulta e resposta, quantidade de ataques recebido.

Anomalias podem ser detectadas, levando em consideração os resultados já encontrados nos trabalhos anteriores *Longo:2015:tcc*.

Desaparecimento de domínios, devido ao período estendido de análise será possível observar o surgimento e desaparecimento de muitos domínios, com os resultados é esperado conseguir um melhor entendimento deste comportamento devido ao período.

PRECISO REVISAR ISSO AKI

5 Considerações Finais

Neste trabalho é apresentado o objetivo de realizar uma análise de um período grade (6 meses) de análise do tráfego, na Universidade do Estado de Santa Catarina. Após um estudo de trabalhos encontrados na área foi possível verificar que os períodos das análises registradas em períodos anteriores não são realizados em períodos grandes (maiores que um mes ou até mesmo dias), está trabalho foca em uma análise em um período maior de tempo (6 meses), com o objetivo de verificar o surgimento de alguns fatores/características que não foram observados devido ao período da análise destes outros trabalhos.

5.1 O que foi feito

No início deste período de estudo, que durou um total de três meses, foi realizado a formulação de um plano para o desenvolvimento deste trabalho, algumas das caracteríticas abordadas neste plano podem ser observadas como:

(1) Formulação do plano do TCC, especificação de algumas características para o início do trabalho;

(2) Revisão sobre DNS, *honeypots* e DNSpot, para um melhor entendimento das principais características e funcionalidade da ferramenta que está sendo utilizada para a captura de informação;

(3) Revisão de trabalhos correlatos, identificação dos principais trabalhos relacionados com a pesquisa. Buscando analisar as análises utilizadas em outros trabalhos e o período que a pesquisa acabou ocorrendo. O principal fator analisado foi o período que as análises ocorreram;

(4) Adaptação no DNSpot para coletas de longo prazo, algumas modificações foram realizadas para que o DNSpot consiga lidar com o período de coleta, removendo algumas características que não torna-se essenciais para este estudo;

(5) Coleta de dados, o início da coleta de dados foi no dia 17/09/2016;

(6) Definição das análises a serem realizadas, com um melhor entendimento e caracterização de alguns trabalhos na área, foi possível definir algumas características para a análise a ser realizada;

(7) Escrita da monografia da primeira parte (TCC-I).

5.2 Próximas etapas

(8) Análise dos resultados obtidos, com uma análise a longo prazo será possível observar algumas características e comportamentos não vistos em uma análise realizada em um período pequeno (um mes ou até mesmo dias);

(9) Escrita da monografia da segunda parte.

5.3 Cronograma

O cronograma proposto para a primeira etapa 5.1, pode ser observador na tabela 5.3.

Etapas	**2016**												**2017**											
	J	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**	**J**	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**
1								x	x															
2									x	x														
3									x															
4										x	x	x	x	x	x	x	x	x						
5										x	x													
6														x	x	x	x	x						
7																x	x	x						

REFAZER ESSA TABELAAAAAA