UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Tecnologia

Paulo Antunes Vieira Neto

Explorando a Viabilidade do Ataque DNS *Spoofing* Por Meio de Sequestro de Rotas BGP

Limeira
2023

Paulo Antunes Vieira Neto

Explorando a Viabilidade do Ataque DNS *Spoofing* Por Meio de Sequestro de Rotas BGP

Dissertação apresentada à Faculdade de Tecnologia da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Engenheiro de Telecomunicações.

Orientador: Prof. Dr. André Leon Sampaio Gradvohl

Este trabalho corresponde à versão final da Dissertação defendida por Paulo Antunes Vieira Neto e orientada pelo Prof. Dr. André Leon Sampaio Gradvohl.

Limeira
2023

FOLHA DE APROVAÇÃO

Abaixo se apresentam os membros da comissão julgadora da sessão pública de defesa de dissertação para o Título de Engenheiro de Telecomunicações na área de concentração , a que se submeteu o aluno Paulo Antunes Vieira Neto, em 16 de outubro de 2023 na Faculdade de Tecnologia – FT/UNICAMP, em Limeira/SP.

Prof. Dr. André Leon Sampaio Gradvohl
Presidente da Comissão Julgadora

Prof. Dr. Edson Luiz Ursini
FT/UNICAMP

Prof. Dr. Henri Alves de Godoy
FATEC/Americana

Ata da defesa, assinada pelos membros da Comissão Examinadora, encontra-se no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós Graduação da Faculdade de Tecnologia.

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Faculdade de Tecnologia
Mariana Xavier - CRB 8/9615

V673e

Vieira Neto, Paulo Antunes, 2000-
Explorando a viabilidade do ataque DNS *spoofing* por meio de sequestro de rotas BGP / Paulo Antunes Vieira Neto. – Limeira, SP : [s.n.], 2023.

Orientador: André Leon Sampaio Gradvohl.
Trabalho de Conclusão de Curso (graduação) – Universidade Estadual de Campinas, Faculdade de Tecnologia.

1. Redes de computadores - Medidas de segurança. 2. Redes de computadores - Protocolos. 3. Nomes de domínio na Internet. 4. Roteamento (Administração de redes de computadores). I. Gradvohl, André Leon Sampaio,1973-. II. Universidade Estadual de Campinas. Faculdade de Tecnologia. III. Título.

Informações adicionais, complementares

Título em outro idioma: Exploring the viability of DNS spoofing attack through BGP route hijacking
Palavras-chave em inglês:
Computer networks - Security measures
Computer network protocols
Internet domain names
Routing (Computer network management)
Titulação: Engenheiro de Telecomunicações
Banca examinadora:
André Leon Sampaio Gradvohl [Orientador]
Edson Luiz Ursini
Henri Alves de Godoy
Data de entrega do trabalho definitivo: 16-10-2023

Agradecimentos

A realização deste trabalho não seria possível sem o apoio de algumas pessoas às quais desejo agradecer e dedicar este trabalho:

O incentivo ao estudo e o apoio de minha mãe e familiares foram fundamentais durante minha permanência em outro estado.

Os colegas da Faculdade de Tecnologia, que apoiaram e encorajaram a ideia inicial do trabalho ainda em 2022.

Os profissionais da área que, mesmo de forma indireta, emitiram suas opiniões, também contribuíram para a construção desta pesquisa.

Agradeço também à Universidade Estadual de Campinas e à Faculdade de Tecnologia por me proporcionarem acesso aos estudos em nível superior de forma livre e pública.

Agradeço ao Prof. Dr. André Leon Sampaio Gradvohl por toda a orientação e suporte no desenvolvimento desta pesquisa.

Resumo

Este trabalho investiga a viabilidade de conduzir ataques de DNS *Spoofing* utilizando-se de técnicas de sequestro (*hijacking*) no protocolo BGP. O experimento envolveu o anúncio de uma rota mais específica para um bloco de endereços IP alvo e o redirecionamento da resolução DNS para um servidor malicioso. O ataque foi bem-sucedido em redirecionar o domínio alvo para um *site* falso, demonstrando o potencial do uso do sequestro BGP para ataques de DNS *Spoofing*. O trabalho discute o impacto causado por esses ataques e recomenda medidas de mitigação, como filtragem de prefixo e o sistema de validação de origem de rotas, o *Resource Public Key Infrastructure*.

Palavras-chave: Segurança de Redes, *Border Gateway Protocol* (BGP), *Hijacking*, *Domain Name System* (DNS), *Spoofing*, Filtragem de Prefixo.

Abstract

This work investigates the viability of conducting DNS Spoofing attacks using hijacking techniques in the BGP protocol. The experiment involved announcing a more specific route for a target IP address block and redirecting DNS resolution to a malicious server. The attack successfully redirected the target domain to a fake site, demonstrating the potential of using BGP hijacking for DNS Spoofing attacks. The work discusses the impact caused by these attacks and recommends mitigation measures, such as prefix filtering and the route origin validation system, *Resource Public Key Infrastructure*.

Key-words: Network Security, Border Gateway Protocol (BGP), Hijacking, Domain Name Service (DNS), Spoofing, Prefix Filtering.

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

AMS-IX	*Amsterdam Internet Exchange*
ARTEMIS	*Automatic and Real-Time Detection and Mitigation System*
AS	Sistemas Autônomos
BCP	*Best Current Practice*
BGP	*Border Gateway Protocol*
DE-CIX	*Deutscher Commercial Internet Exchange*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Denial of Sevice*
eBGP	*external Border Gateway Protocol*
eNSP	*Enterprise Network Simulation Platform*
EVE-NG	*Emulated Virtual Environment – Next Generation*
FTP	*File Transfer Protocol*
HEAP	*Hijacking Event Analysis Program*
HTTP	*Hypertext Transfer Protocol*
IANA	*Internet Assigned Numbers Authority*
iBGP	*internal Border Gateway Protocol*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IGRP	*Interior Gateway Routing Protool*
IP	Protocolo Internet
IRR	*Internet Routing Registries*
MAC	*Media Access Control*
MANRS	*Mutually Agreed Norms for Routing Security*

OSPF	*Open Shortest Path First*
PTT	Ponto de Troca de Trafego
RFC	*Request for Comments*
RIP	*Routing Information Protocol*
RIPE NCC	*Réseaux* IP *Européens Network Coordination Centre*
ROA	*Route Origin Authorization*
RPKI	*Resource Public Key Infrastructure*
RRI	Registo Regional da Internet
SIDR	*Secure Inter-Domain Routing*
TCP	*Transmission Control Protocol*
TLD	*Top-Level Domain*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*

Sumário

Capítulo 1

Introdução

A Internet tem como princípio realizar a intercomunicação entre diferentes dispositivos, servidores, computadores, roteadores dentre diversos outros equipamentos. Desta forma, funciona como uma rede de comunicação onde todos os pontos se comunicam direta ou indiretamente entre si. Para a realização dessa comunicação, foram desenvolvidos diversos protocolos de roteamento. Dentre eles estão os protocolos dinâmicos *Open Shortest Path First* (OSPF) (K. LOUGHEED, 1989), *Routing Information Protocol* (RIP) (HEDRICK, 1988), IS-IS (ORAN, 1990), *Interior Gateway Routing Protool* (IGRP) (CISCO SYSTEMS, 2005) e *Border Gateway Protocol* (BGP) (K. LOUGHEED, 1989), dentre outros que foram introduzidos por meio das chamadas *Request for Comments* (RFC). As RFCs são padrões técnicos disponibilizadas pelo *Internet Engineering Task Force* (IETF).

O BGP é o principal protocolo de roteamento entre os Sistemas Autônomos (AS). Esses são dispositivos como roteadores e *switches* administrados por uma empresa por meio de uma política de roteamento única. A Universidade Estadual de Campinas, por exemplo, está registrada como AS 53187 e anuncia cinco prefixos de endereços do Protocolo Internet (IP), sendo três blocos com endereços IPv4 e dois blocos com endereços IPv6. Esses dados são utilizados pelo protocolo BGP para estabelecer a comunicação da UNICAMP (AS 53187) com os demais pares.

O BGP foi primeiramente introduzido pela RFC 1105 em junho de 1989. Posteriormente, ocorreram diversas mudanças e melhorias desde seu lançamento. Atualmente, para comunicação por IPv4 e IPv6, o padrão utilizado está descrito na RFC 4271 (REKHTER; HARES; LI, 2006).

O roteamento dinâmico do protocolo BGP é baseado na escolha da melhor rota com base no próximo salto de um AS vizinho e também das políticas de roteamento interno da organização responsável pelo sistema autônomo. O BGP utiliza-se de um acordo mútuo entre os ASs, onde são acordadas métricas de saltos para alcançar o AS desejado, blocos que podem ser trafegados pelos pares e também a confiança entre eles para trafegar as informações com integridade e privacidade. No entanto, o protocolo BGP traz uma vulnerabilidade para a comunicação. Nos padrões RFC publicados referentes ao BGP não se menciona que um AS possa anunciar rotas para um bloco IP que já tenha sido anunciado por outro sistema autônomo.

Os incidentes envolvendo anúncio de rotas conhecidas previamente e o desvio do tráfego são denominados como BGP *Route Hijacking* ou também BGP *Route Leaking*. Dependendo do contexto do evento utilizamos um ou outro termo. A seguir estão as definições.

- ***Route Hijacking***: Em tradução literal, um sequestro de rotas causado por um sistema autônomo com intenção de desviar o tráfego de um determinado serviço.
- ***Route Leaking***: Ocorrendo o vazamento não intencional de uma rota, geralmente ocasionado por uma configuração incorreta em um dos roteadores de borda, uma falha humana.

Diariamente, observa-se a ocorrência de tais eventos. Eles são monitorados pela ferramenta BGP *Stream*, que foi desenvovida pela empresa estadunidense Cisco Systems (LYSTRUP, 2015). A ferramenta relata a indisponibilidade das rotas e os sistemas autônomos afetados.

Caso um serviço de Resolução de Nomes, ou *Domain Name System* (DNS), que utilizamos para obter o endereço IP de um servidor web por meio de um endereço *Uniform Resource Locator* (URL), seja comprometido, um usuário final é impactado diretamente. Isso ocorre, por ser necessária a utilização do serviço para conexão em todos os sites, pressupondo que um usuário não tenha previamente o endereço IP de um *site*. Um DNS sequestrado pode levar ao redirecionamento a páginas distintas que podem conter um código fonte malicioso.

Para mitigar este tipo de ataque a sessões BGP, o IETF, por meio da RFC 6480 (LEPINSKI; KENT, 2012), disponibilizada em fevereiro de 2012, introduziu o *Resource Public Key Infrastructure* (RPKI). O RPKI é uma tecnologia de verificação e validação de rotas anunciadas por um AS em um banco de dados. Esse sistema utiliza de uma assinatura digital disponibilizada pelo órgão regional como o Registro.br que atende o Brasil ou o *Réseaux* IP

Européens Network Coordination Centre (RIPE NCC), que atende organizações europeias, do Oriente Médio e da Ásia Central.

1.1 Motivação

Em 2008, um ataque realizado por uma companhia de telecomunicações paquistanesa, a *Pakistan Telecom* (AS 17557), anunciou uma sub-rede da empresa norte-americana Youtube (AS 36561), redirecionando todo o tráfego do serviço de vídeos online para o Paquistão (RIPE, 2008). Conforme informações apuradas pelo jornalista Declan McCullagh, do jornal norte-americano CNET, um porta-voz da embaixada paquistanesa informou que a ordem para bloquear o acesso ao Youtube veio do governo paquistanês como forma de represália a um video publicada na rede com conteúdo anti-islâmico, religião de maioria no país (DECLAN, 2008). O incidente só foi neutralizado depois de 2 horas do início do evento. Um sistema autônomo que transportava as rotas da Pakistan Telecom, a PCCW Global (AS 3491), removeu os blocos anunciados pela Pakistan Telecom.

Recentemente, em julho de 2022, houve um incidente envolvendo um sistema autônomo russo. A PJSC Rostelecom (AS 12389) anunciou um prefixo que pertence ao sistema autônomo da empresa norte-americana Apple (AS 714). Devido ao fato de que o bloco não é protegido por um sistema *Route Origin Authorization* (ROA), o anúncio da rota foi propagado globalmente. Engenheiros da Apple tentaram mitigar a falha anunciando um bloco mais específico que o prefixo sequestrado pela PJSC Rostelecom. O incidente durou por volta de 12 horas até que as rotas do bloco da Apple foram desabilitadas pelo AS 12389 (SIDDIQUI, 2022).

Inclusive, um dos serviços de resolução de nomes público mais conhecidos por usuários, o Google DNS *Server* (no endereço IP 8.8.8.8), também sofreu ataque um ataque em 2014, que afetou conexões na América Latina, especificamente no Brasil e na Venezuela. Uma divisão da empresa British Telecom na América Latina, sob o sistema autônomo AS 7908, anunciou o prefixo 8.8.8.8 com máscara de rede 32, trafegando por 22 minutos milhões de requisições de resoluções de URL de brasileiros e venezuelanos (PAGANINI, 2014).

Estes são alguns dos incidentes mais notórios de ataques a sessões BGP que repercutiram mundialmente. Considerando seu impacto e a fragilidade do sistema, isso gerou estudos de caso por entidades como o RIPE NCC e a iniciativa *Mutually Agreed Norms for Routing*

Security (MANRS) para conscientizar provedores de rede, sistemas autônomos e entidades governamentais à adoção do sistema de validação de origem, o ROA.

1.2 Objetivos

Portanto, este trabalho pretende demonstrar, por meio de simulações computacionais, como ocorre um sequestro de servidor DNS por meio de um anúncio de prefixo já existente por um sistema autônomo invasor.

Utilizando uma topologia criada com base no trabalho de Rashevskiy e Shaburov (2017), e com roteadores da empresa chinesa Huawei virtualizados através do software de simulação da mesma companhia, o eNSP (SIERSZEŃ, 2020), podemos estabelecer as conexões BGP entre os roteadores e servidores para os protocolos DNS e HTTP.

Com dispositivo denominado como *Cloud* no eNSP é possível estabelecer uma conexão virtual entre os roteadores do software e outras conexões do computador, sejam conexões físicas ou conexões virtuais. Acompanhado de outro software simulações de redes, o EVE-NG (OLIVEIRA, 2020), que também possui um dispositivo denominado *Cloud* que realizada a mesma função do dispositivo no software da Huawei, podemos estabelecer uma comunicação entre equipamentos virtualizados em ambos ambientes. Como o EVE-NG é idealizado para virtualizar imagens reais, pode-se instalar uma distribuição Linux de código aberto, como o Ubuntu, em versão desktop, para utilizar uma interface gráfica um navegador que possa se conectar com os servidores WEB no eNSP.

A ferramenta livre e de código aberto Wireshark (OREBAUGH; RAMIREZ; BEALE, 2006) se mostra vantajosa para o trabalho com objetivo de capturar pacotes que trafegam pelas interfaces físicas dos equipamentos virtualizados. Um dos objetivos deste trabalho é a captura de pacotes de atualizações do protocolo BGP. Com isso, esperamos demonstrar o evento de um sequestro (*hijacking*) de prefixo, tendo seu argumento AS_Path alterado.

Este trabalho também visa abordar algumas possíveis formas de neutralizar o ataque, como a disponibilização de uma resolução de nomes local, uso de filtros de rotas e o anúncio de rotas mais específicas, como o que foi realizado por engenheiros da Apple no incidente de julho de 2022 com a Rostelecom.

Capítulo 2

Fundamentação Teórica

Este capitulo apresenta os conceitos gerais para a compreensão do trabalho. Aqui, são apresentados os conceitos de roteamento pelo protocolo BGP, o protocolo de resolução de nomes DNS e outros conceitos pertinentes.

2.1 Introdução ao protocolo BGP

Seguindo a referência do protocolo pela RFC 4271 (REKHTER; HARES; LI, 2006), abordaremos alguns termos que serão utilizados neste trabalho. Entre eles estão os seguintes:

- Sistema Autônomo (AS), que são os conjuntos de roteadores administrados por uma empresa ou organização.
- BGP *Speaker*, Origem, também conhecido como roteador de borda, pois estabelece conexão direta com o *backbone* (ligação central da rede), o dispositivo onde será implementado o protocolo de roteamento BGP.
- *internal Border Gateway Protocol* (iBGP), que são as rotas internas de um AS, aprendidas através de outros procolos, como o OSPF.
- *external Border Gateway Protocol* (eBGP), são as rotas externas a um AS. Por exemplo, o AS 1 tem rotas presentes na sua tabela de roteamento que fazem parte de rotas anunciadas de outro AS, estas rotas são externas do AS 1.
- *AS_Path* que apresenta a sequências de sistemas autônomos, a partir de um BGP *Speaker*, até o AS que anuncia uma rede de endereços IP.

- O Próximo Salto que se refere ao próximo endereço IP para o qual deve ser transmitido um pacote para alcançar um endereço externo.

Seguindo a RFC 6996 (MITCHELL, 2013), que determina a faixa de números de sistemas autônomos reservados para uso privado (interno), para sistemas em que o número segue o padrão de 16 bits, é reservada a faixa de números 64512 até 65534 para utilização privada. Este trabalho utilizará apenas de valores neste intervalo para identificação dos sistemas autônomos.

Agora podemos definir como um par de sistemas autônomos realizam a conexão para roteamento via BGP. A Figura 2.1 mostra como ocorre o estabelecimento da conexão entre dois roteadores de borda de diferentes sistemas autônomos.

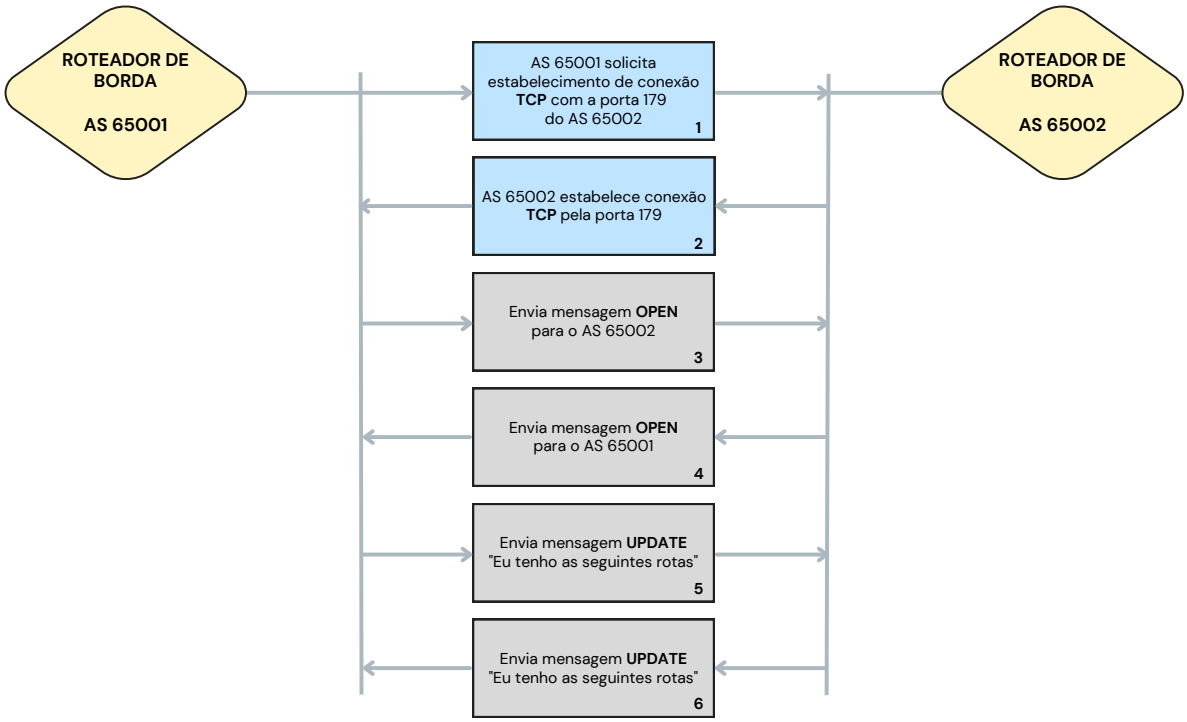

Figura 2.1: Estabelecimento de conexão BGP. Fonte: Adaptado de Rekhter, Hares e Li (2006).

Assim, o roteador de borda do AS 65001 solicita inicialmente o estabelecimento de uma conexão do protocolo *Transmission Control Protocol* (TCP) na porta 179 do endereço de *gateway* do roteador de borda do AS 65002. A RFC 793 (POSTEL, 1981), que inicialmente apresenta o protocolo TCP, estabelece que a comunicação deve seguir o processo chamado de "aperto de mãos em três-vias" para estabelecer a conexão.

Nesse processo são trocados pacotes de sincronização e reconhecimento entre os dispositivos, os pacotes SYN e ACK do protocolo. Após a finalização do processo de "aperto de

mãos", a conexão é estabelecida e os pares podem trocar dados, como aqueles do protocolo BGP e assim transmitirem as mensagens iniciais do BGP. A Figura 2.2 descreve esse processo.

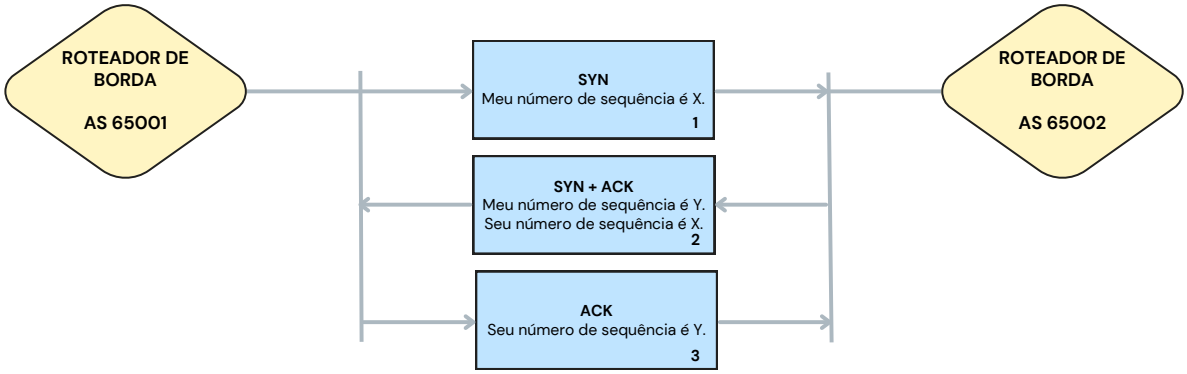

Figura 2.2: Estabelecimento de conexão TCP entre os roteadores de borda. Fonte: Adaptado de Postel (1981).

Como mostrado na Figura 2.1, ambos os dispositivos enviam uma mensagem de abertura de comunicação, – pacote OPEN –, que transmite informações como o número do AS e a versão do protocolo. Após o recebimento mútuo do pacote OPEN, os dispositivos transmitem o pacote UPDATE. Nesse pacote são enviadas informações para a atualização da tabela de roteamento e contém dados como blocos de endereços IPs roteáveis, seus respectivos números de AS e próximos saltos, informações de inserção ou remoção de rotas.

Para manter a conexão ativa entre os pares, o protocolo BGP envia, a cada intervalo de tempo, um pacote KEEPALIVE, onde informa que os pares continuam ativos. Caso um dos dispositivos não receba o pacote KEEPALIVE de sua adjacência, ele aguarda um intervalo três vezes maior que o tempo de espera do KEEPALIVE para enviar um pacote de NOTIFICATION. Esse pacote informa que a sessão está sendo encerrada, pois seu par não respondeu a atualizações. Dispositivos de empresas como a Huawei e a Cisco utilizam, por padrão, o intervalo de 60 segundos para o KEEPALIVE e 180 segundos para envio da mensagem NOTIFICATION de encerramento da sessão.

2.2 Classificação de ataques BGP

Nos trabalhos de Rashevskiy e Shaburov (2017) e Cho et al. (2019), algumas vulnerabilidades do BGP e seus riscos foram classificados. Dentre elas estão as seguintes:

- Quebra de confidencialidade: Os dados de roteamento trafegam sem encriptação, suscetível a interceptação dos pacotes.

- Especificação de prefixo: Anúncio de rotas com prefixos específicos, ou seja, uma rede com máscara de 25 no IPv4 é mais específica do que uma rede com máscara de 24. O algoritmo de decisão do protocolo BGP utiliza o comprimento da máscara de rede para a escolha do caminho. No trabalho de Rekhter, Hares e Li (2006) essa ocorrência é descrita como *Overlapping Routes*.

- Mudança de origem ou prefixo falso: um anúncio de rotas de um prefixo que não pertence ao sistema pode fazer com que sistemas próximos tentem trafegar pela rede do invasor, pois o *AS_Path* é menor.

- Manipulação do *AS_Path*: um sistema autônomo invasor pode manipular o parâmetro *AS_Path*, inserindo ou removendo outros sistemas autônomos de uma rota.

2.3 Introdução ao protocolo DNS

O protocolo de resolução de nomes, o DNS, foi introduzido pela RFC 1034 (MOCKAPETRIS, 1987a) e RFC 1035 (MOCKAPETRIS, 1987b), como uma forma de simplificar a navegação na internet aos usuários, permitindo acessem *sites* por meio de uma URL, como o "`www.example.com`". Esta URL, "`www.example.com`", é um dos endereços disponibilizados pela *Internet Assigned Numbers Authority* (IANA) – entidade responsável pela coordenação de servidores raiz de DNS, endereçamento IP e outros serviços – para a utilização em exemplos em documentos e trabalhos acadêmicos sem requisição prévia para autorização de seu uso. Este *site* será utilizado como base neste trabalho, a URL como o código-fonte do *site*. Mais detalhes são apresentados no Capítulo 4.

Na Figura 2.3 temos um processo de requisição do endereço IP da URL "`www.example.com`", solicitada por um usuário e direcionada a um servidor DNS recursivo local. O servidor recursivo realiza as requisições aos demais servidores. Assim, ao receber uma requisição de resolução, esse servidor consulta a sua base interna, a *cache*, verificando se há algum registro armazenado do endereço "`www.example.com`". Caso não tenha, o processo de requisição continua recursivamente em outros servidores semelhantes.

O servidor DNS solicita a resolução de um endereço um servidor raiz, que retorna a solicitação ao servidor local para que essa seja direcionada a um servidor *Top-Level Domain* (TLD). O servidor raiz decide, a partir do sufixo da URL – por exemplo, `.com` e `.net` – para qual servidor TLD a requisição deve ser enviada. O servidor TLD do sufixo `.com` recebe a

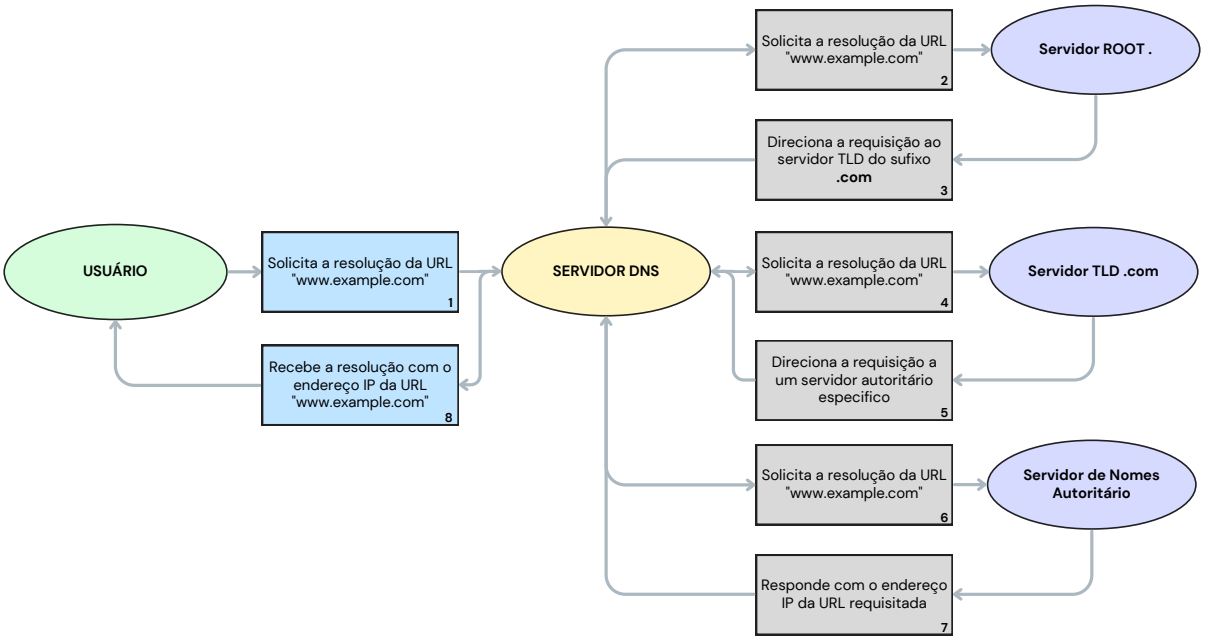

Figura 2.3: Requisição de resolução DNS. Fonte: Adaptado de Liska, Stowe e Gallo (2016).

requisição e retorna ao servidor recursivo a informação de qual servidor autoritário responde pela URL. Em seguida, o DNS solicita ao servidor autoritário que retorna o endereço IP da URL. Assim, o servidor local informa o endereço IP ao usuário que solicitava a resolução de URL, para que possa ser realizada a conexão via porta 80, usando o protocolo *Hypertext Transfer Protocol* (HTTP), sobre o protocolo TCP.

2.4 Classificação de ataques DNS

Há diversas publicações tratando sobre a classificação e mitigação de diversos tipos de ataques ao protocolo DNS. Alguns autores, como Liska, Stowe e Gallo (2016) e Grimes (2020), trazem algumas definições dos possíveis ataques ao DNS. Eis alguns exemplos:

- DNS *Spoofing*, onde há falsificação de registro em um servidor para que as requisições sejam direcionadas a um *site* falso.
- DNS *Pharming*, semelhante ao ataque *spoofing*. No entanto, o *site* ao qual o usuário é direcionado coleta informações inseridas, como senhas, informações pessoais e bancárias.
- Alteração de *Cache*, onde um invasor altera registros na *cache* de um servidor recursivo local para que requisições sejam direcionadas a *sites* maliciosos, antes mesmo que

possam ser consultados servidores autoritários, que são os servidores que contém a resposta para a requisição, que teve como passo anterior o servidor TLD.

- Tunelamento por DNS, onde um atacante consegue encapsular tráfego de outros protocolos pelo tráfego real de um computador de usuário invadido.

- Reflexão e amplificação de requisições, em que é considerado um ataque de negação de serviço (*Denial of Sevice* – DoS), pois um usuário recebe um grande volume de tráfego de requisições DNS. Esse tráfego foi requisitado por invasor externo a múltiplos servidores públicos de DNS e utilizando o endereço IP de origem do pacote como o endereço do usuário que será afetado (NEVES; SILVA DAMAS, 2008; MACFARLAND; SHUE; KALAFUT, 2015).

2.5 Filtragem e Manipulação de Rotas

Apresentadas como uma *Best Current Practice* (BCP) na implementação do BGP, a RFC 7454 publicada por Durand, Pepelnjak e Döring (2015) traz técnicas de filtragem de rotas que podem ser utilizadas para controlar como trafegam os pacotes de entrada e saída. Eis alguns exemplos de filtros:

- Filtro de Prefixo, no qual é possível definir um intervalo da máscara de um endereço de rede e executar uma ação, por exemplo:
  - Negar a rede `192.168.0.0` com prefixo maior ou menor que 24.
  - Aceitar rede `192.168.0.0` com prefixo menor ou maior que 24.

- Filtro de *AS_Path*, neste filtro é realizada uma comparação do atributo *AS_Path* nos pacotes UPDATE recebidos em uma sessão BGP, por exemplo:
  - Aceitar rede caso contenha o AS 65002 no *AS_Path*.
  - Negar rede caso contenha o AS 65003 no *AS_Path*.

Além dos filtros apresentados, também é possível manipular as rotas aprendidas na tabela de roteamento por meio da alteração de parâmetros como os valores de preferência. Os valores padrões são definidos pelos fabricantes dos dispositivos.

A manipulação do parâmetro *AS_Path* também é plausível e pode ser realizado com a técnica *Path Prepending*, que está no trabalho de McBride et al. (2023). A técnica consiste em realizar a inserção de múltiplas entradas de um sistema autônomo em uma rota aprendida que influenciará a escolha no processo de seleção do BGP. Uma rota com *Path Prepending* terá uma distância maior que a rota original. Esta técnica é utilizada quando ocorre o sequestro de rotas com o mesmo prefixo.

Utilizar uma comunidade BGP, como a BLACKHOLE (KING et al., 2016), servirá de grande utilidade também na realização da engenharia de tráfego. Afim de descartar transmissões a rotas afetadas, de maneira temporária, é possível definir uma politica de roteamento na qual rotas marcadas com esta comunidade são direcionadas a um próximo salto inválido, descartando todos pacotes direcionados a rede.

2.6 Considerações Finais

Neste capítulo descrevemos o funcionamento do protocolo de roteamento BGP e as principais mensagens enviadas entre os pares que possuem uma comunicação BGP ativa. Também introduzimos o protocolo de resolução de nomes e ilustramos como é realizada a requisição de uma URL de um *site*. A compreensão desses conceitos é importante para os experimentos práticos que serão realizados neste trabalho, apresentados no Capítulo 4.

Além disso, também abordamos as vulnerabilidades e ataques a esses protocolos. Conforme descrevemos na Seção 1.2, o objetivo deste trabalho é explorar a vulnerabilidade de especificação de prefixo e realizar o *Spoofing* de DNS, com o intuito de afetar um usuário final.

Por outro lado, neste capítulo também apresentamos técnicas que podem auxiliar na mitigação desses cenários. O uso de filtros e manipulação de rotas influenciam em como os pacotes serão transmitidos pela rede.

Capítulo 3

Revisão Bibliográfica

Neste capítulo, são apresentados pesquisas e resultados de relevantes trabalhos de temas como BGP, DNS e segurança dos protocolos. Os resultados obtidos pelos trabalhos apresentados serviram de base para este trabalho. Apesar de existir diversos trabalhos publicados que exploram as vulnerabilidades dos protocolos, BGP e DNS, não há um trabalho que explore ambas as falhas de segurança ocorrendo simultaneamente.

3.1 Ataques DNS

Os trabalhos de Hussain et al. (2016) e Tripathi, Swarnkar e Hubballi (2017) apresentam uma abordagem teórica sobre como os ataques ao serviço de Resolução de Nomes são realizados. No caso do artigo de Tripathi, Swarnkar e Hubballi (2017), também é apresentada uma abordagem prática do DNS *Spoofing* em uma rede local. Os autores, por meio de algoritmos escritos em linguagem de programação C, realizaram ataques que afetaram os demais usuários da rede local, redirecionando-os para páginas falsas com a URL desejada pelo usuário da rede. Com base na abordagem prática desse artigo, foi possível desenvolver uma metodologia semelhante, abordada na Seção 4.5.

O trabalho de Tripathi, Swarnkar e Hubballi (2017) captura as requisições por meio de um de seus algoritmos. Esse algoritmo específico realiza o ataque de ARP *sniffing*, um protocolo que funciona de maneira semelhante ao DNS, mas que realiza a resolução de endereços em redes locais, requisitando os endereços *Media Access Control* (MAC) dos endereços IP do bloco pertencente. A proposta deste trabalho, conforme abordado na Seção 1.2, é receber as

requisições devido ao redirecionamento causado pelo sequestro da rota do protocolo BGP, sem a necessidade de realizar o ARP *sniffing*.

3.2 Segurança do BGP

A RFC 4272, publicada por Murphy (2006), é uma extensão da RFC 4271 e investiga as vulnerabilidades de segurança do protocolo BGP. Nesse trabalho são abordados diversos pontos do protocolo que estão passíveis de ataques, como a interceptação de pacotes contendo informações de roteamento que não são criptografados, inserção de pacotes OPEN, UPDATE e NOTIFICATION modificados e ataques de negação de serviço.

No entanto, essas vulnerabilidades estão presentes devido ao protocolo de comunicação TCP e podem ser solucionadas com a implementação da autenticação por meio do TCP MD5, solução inicialmente introduzida pela RFC 2385 (HEFFERNAN, 1998). Porém, como também citado na RFC 4272, esses mecanismos não protegem contra ataques externos, como o sequestro de rotas, as quais são brevemente mencionadas na RFC como uma vulnerabilidade do atributo de caminho na mensagem UPDATE do protocolo.

O sequestro de sessões BGP também é apresentado de forma teórica em artigos, principalmente classificando-os em diferentes tipos de ataques, como no artigo de Cho et al. (2019). Por sua vez, o trabalho de Rashevskiy e Shaburov (2017) apresenta a parte prática que aborda as falhas do protocolo. Os autores abordam o ataque realizando o anúncio de um bloco de endereços conhecido – que já foi anunciado por outro sistema autônomo –, e sistemas com menos saltos, ou seja, sistemas mais próximos, para alcançar o endereço desejado. Assim, acabam direcionando o tráfego para o sistema autônomo falso.

Para este trabalho, decidimos abordar o sequestro de sessões BGP por meio do anúncio de uma rota mais específica, conforme classificado nos tipos de ataques no capítulo anterior. A topologia da rede será apresentada no Capítulo 4.

Noutra frente, em 2015, foi publicada a RFC 7454 (DURAND; PEPELNJAK; DÖRING, 2015), onde foram definidas as melhores práticas atuais de implementação e manutenção do protocolo BGP e medidas de segurança. O trabalho apresenta formas de implementação de segurança de sessões BGP, autenticação de sessões TCP e técnicas de filtragem de rotas. As técnicas de filtragem de rotas incluem filtragem por prefixo de rede, filtragem por comprimento da máscara de rede, filtragem pelo atributo `AS_Path` da rota e o uso de comunidades, que foram

inicialmente introduzidas por meio da RFC 1997 (LI; CHANDRA; TRAINA, 1996). Esses são atributos adicionais das políticas de roteamento, como não exportação de rotas e não anunciar a rota a outros pares. Essas práticas apresentadas na RFC 1997 são utilizadas na engenharia de tráfego, pois com elas podemos controlar como os dados serão transmitidos e como devemos tratar os pacotes recebidos.

As comunidades BGP, Li, Chandra e Traina (1996), compõem um grande papel na engenharia de tráfego, uma vez que ela podem ser transitadas através dos pacotes UPDATE entre as sessões BGP e serem ativadas através das politicas de roteamento dos roteadores de borda. Existem algumas comunidades padrões, definidas pela RFC 1997, que são implementadas por padrão nos sistemas operacionais dos roteadores como a NO_EXPORT que define que rotas recebidas marcadas com essa comunidade não devem ser exportadas a outras sessões BGP, porém também é desenvolver comunidades próprias e compartilha-las com as demais organizações que se comunicam seu sistema autônomo, um exemplo são as comunidades do IX.br como a comunidade `65000:AS` que não anunciará rotas recebidas com essa comunidade para o sistema autônomo "AS"no sufixo, ou também `65001:AS` que anuncia as rotas exclusivamente para o sistema autônomo "AS"(IX.BR, s.d.).

Uma outra comunidade fundamental foi definida através da King et al. (2016), a comunidade BLACKHOLE é utilizada para descartar qualquer tráfego direcionado as rotas marcadas com esta comunidade. Esta comunidade pode ser utilizada como uma politica de roteamento interna do sistema autônomo ou exporta-las também aos demais sistemas, porém, ao receber uma rota com esta informação, deve ser inclusa a comunidade NO_EXPORT ou a NO_ADVERTISE para não propagar a rota.

A RFC 7454 também traz como sugestão a implementação da infraestrutura *Secure Inter-Domain Routing* (SIDR), introduzido pela RFC 6480 publicada por Lepinski e Kent (2012), Essa é uma arquitetura desenvolvida para aperfeiçoar a segurança no roteamento pelo protocolo BGP.

O SIDR disponibiliza dois modos de operação para sistemas. O primeiro serve para a validação de origem do prefixo, apresentada pela RFC 6811 (MOHAPATRA et al., 2013). A validação de origem de prefixo verificará se o sistema autônomo é autorizado a anunciar a rede. Essa verificação é realizada por um servidor validador que, com a informação do sistema autônomo e o endereço de rede, realiza uma busca em bancos de dados das entidades de Registo Regional da Internet (RRI). Esses bancos de dados contêm registros como um

certificado digital, conhecidos como RPKI, introduzidos também pela RFC 6480, e este certificado assina a *Route Origin Authorization*.

A operação do método de validação de origem apresenta os seguintes ações após a verificação realizada:

- Se um ROA válido é encontrado, então o prefixo deve ser aceito e fará parte da tabela de roteamento.
- Se um ROA inválido é encontrado, então o prefixo deve ser descartado e a rede descartará também pacotes destinados a essa rede.
- Se um ROA não é encontrado, o prefixo deve ser aceito. Porém, receberá atributos de preferência baixos, ou seja, a rota será utilizada em última instância.

O outro modo de operação apresentado pela RFC 6480 é a validação de caminho, ou *PATHSEC*, onde o roteador de borda verifica se o *AS_Path* representa a sequência de sistemas autônomos que a mensagem *UPDATE* trafegou.

A organização MANRS disponibiliza, desde 2021, uma ferramenta de livre acesso, com dados atualizados diariamente, para consultar o atual estado da implantação da validação por RPKI no mundo (STUCCHI, 2021). A ferramenta exibe a rota anunciada, número do sistema autônomo que anuncia e o estado do anúncio, se é válida, inválida ou se o ROA não foi encontrado na busca. Esses dados podem ser filtrados por país ou por AS. A Tabela 3.1 contém dados referentes à implementação do RPKI em alguns dos países com maior número de rotas anunciadas, os dados foram coletados em setembro de 2023.

Tabela 3.1: Estado da Implantação do RPKI pelo Mundo. Adaptado de MANRS (2023a).

País	Rotas Anunciadas	Rotas Válidas	Rotas Inválidas	(%) de Uso
Estados Unidos	281319	85020	446	30,38
Brasil	**87412**	**24967**	**146**	**28,73**
Índia	53420	35614	802	68,17
Rússia	41391	16820	217	41,16
China	28744	19849	125	69,49
Alemanha	22379	14337	104	64,53
Reino Unido	21405	11143	278	53,36

A plataforma também informa a percentual total de utilização no mundo, que no momento encontra-se em 46,27% dos blocos IPv4 anunciados e 53,57% dos blocos de

endereços IPv6 anunciados. A partir da Tabela 3.1, com algum dos principais países, podemos aferir que a implementação da validação de origem de rotas nos países com maior número de rotas sendo anunciadas, Estados Unidos e Brasil, tem um percentual de uso do RPKI inferior à média mundial. Juntos, os países representam aproximadamente 33% do total de rotas anunciadas.

Além da validação de origem de rotas, outras soluções foram propostas a fim de aprimorar a segurança de redes do protocolo BGP, como o *Automatic and Real-Time Detection and Mitigation System* (ARTEMIS) (SERMPEZIS; KOTRONIS; GIGIS et al., 2018), *Hijacking Event Analysis Program* (HEAP) (SCHLAMP et al., 2016), entre outras ferramentas.

O trabalho onde a solução ARTEMIS foi proposta (SERMPEZIS; KOTRONIS; GIGIS et al., 2018), traz dados importantes, além dos seus resultados, pois também foi realizada uma pesquisa entre 75 operadores de rede. A pesquisa foi publicada posteriormente no artigo de Sermpezis, Kotronis, Dainotti et al. (2018). Essa pesquisa revelou que operadores de rede relutam em implementar soluções de defesa proativas, pois eles oferecem uma proteção limitada, como o RPKI que será completamente eficiente quando for implementado uma escala global. Porém, conforme a Tabela 3.1, ainda em 2023, não se encontra em uma operação global.

O uso de ferramentas terceirizadas para detecção de eventos de sequestro de rotas por parte dos responsáveis pelos sistemas autônomos é um dos motivos para a demora na mitigação dos ataques. Essas ferramentas podem emitir falsos positivos e falsos negativos, onde alarmes reportados podem informar eventos de maneira errada, sendo necessária uma análise profunda do evento após a notificação.

O ARTEMIS também utiliza de dados obtidos por meio de plataformas externas de detecção em tempo real. Porém, conta com uma base de dados de diversos tipos de ataque para decidir se o evento é um ataque legitimo ou falso positivo. A cada pacote BGP UPDATE recebido pelos monitores em tempo real, o ARTEMIS extrai o campo `AS_Path` e compara com um registro prévio. Se o `AS_Path` não contiver informações do AS inicial, isso gerará um alarme informando o sequestro.

O software proposto também traz uma automação que realiza, de forma autônoma, as configurações no protocolo BGP do AS para neutralizar o ataque, dependendo do cenário alertado anteriormente. Por conta da automação presente, o ARTEMIS alcançou resultados onde a mitigação completa do evento se deu em um minuto.

Por sua vez, o HEAP, introduzido por meio da publicação de Schlamp et al. (2016), trata-se de uma ferramenta de detecção, que recebe também dados de fontes externas, que avalia o evento a fim de diminuir a taxa de alarmes falsos em incidentes de BGP. Os autores partem da suposição que um invasor consegue sequestrar as rotas. Porém, não pode alterar dados externos contendo informações de roteamento por órgãos registradores.

A ferramenta se utiliza dos dados presentes nas *Internet Routing Registries* (IRR) para verificar se há legitimidade na conexão. O IRR é um banco de dados onde os sistemas autônomos divulgam suas políticas de roteamento, contendo bloco anunciado, contato com o operador de rede responsável, regras de roteamento (CORAZZA, 2019).

Após a verificação do IRR, o HEAP faz uma análise topológica, a fim de descartar eventos de redes causadas por práticas operacionais de roteamento, or exemplo, uma organização menor recebendo um prefixo IP de uma companhia maior (SCHLAMP et al., 2016). A análise consiste em comparar o `AS_Path` recebido no pacote UPDATE, semelhante ao realizador pelo ARTEMIS (SERMPEZIS; KOTRONIS; GIGIS et al., 2018).

Por último, há um filtro final em que são comparadas as chaves criptográficas SSL/TLS. A verificação é feita por meio da análise da chave pública de encriptação, observando se elas são idênticas antes e durante o evento suspeito.

Os autores apresentaram resultados após um mês de coleta de dados e realizaram também uma checagem dos dados com outra plataforma de detecção e reporte de alarmes, a BGPmon.net. De 85 alarmes reportados pela ferramenta, apenas sete no total foram falsos positivos.

3.3 Considerações Finais

Neste capítulo, abordamos trabalhos relevantes relacionados à segurança dos protocolos DNS e BGP. Por não haver trabalhos até o momento que explorem ataques ao DNS através do sequestro de rotas BGP, este trabalho poderá ser utilizado como referência bibliográfica.

A Seção 3.1 introduz brevemente dois trabalhos sobre ataques DNS *Spoofing* e mostra que é possível simular uma rede local e conduzir ataques DNS locais. Com base nesses trabalhos foi desenvolvida uma metodologia de ataque ao protocolo DNS, sem utilizar linguagens de programação e ARP *sniffing* como em (TRIPATHI; SWARNKAR; HUBBALLI, 2017), apresentado na Seção 4.5.

Por sua vez, a Seção 3.2 aborda artigos e referenciais técnicos sobre a vulnerabilidade do protocolo e ataques de manipulações de rotas do protocolo BGP, medidas de mitigação e trabalhos que introduzem novas ferramentas com intuito de aprimorarem a segurança do roteamento. Nessa seção, destaca-se a RFC 4272 (MURPHY, 2006) com uma extensão da RFC 4271, em que é introduzida a versão 4 do protocolo BGP, contendo uma análise sobre as vulnerabilidades presentes no protocolo. A seção também comenta sobre a RFC 7454 (DURAND; PEPELNJAK; DÖRING, 2015) que traz medidas práticas de implementação de quesitos de segurança apresentados na RFC 4272. Neste capítulo, discutimos como implementar as recomendações no cenário desenvolvido para a execução deste trabalho.

Capítulo 4

Metodologia

Neste capítulo, apresentamos a metodologia utilizada para execução dos objetivos propostos neste trabalho. Aqui descrevemos o software, os dispositivos virtuais e a topologia que usamos para demonstrar os experimentos.

4.1 Simuladores de Redes

Os equipamentos de rede, como roteadores, *switches* e servidores DNS e web, são disponibilizados para simulações através do software oficial da empresa Huawei, chamado *Enterprise Network Simulation Platform* (eNSP), disponibilizado gratuitamente. O simulador é amplamente utilizado por estudantes e profissionais da área de redes, devido à sua biblioteca contendo os principais roteadores, *switches* e estações finais para simulações, possibilitando o uso para treinamento e provas de certificações da empresa, nos níveis associado e profissional.

Para obtermos a perspectiva do usuário final, por meio de um terminal, é necessário utilizar dois simuladores distintos, de modo que ambos se comuniquem por meio de interfaces lógicas de um computador. O software *Emulated Virtual Environment – Next Generation* (EVE-NG), também disponibilizado de forma gratuita para uso não comercial, nos permite a virtualização de sistemas operacionais, servidores e dispositivos de rede, como *firewalls*, mediante instaladores oficiais do equipamento ou sistema operacional desejado.

A intercomunicação entre os simuladores é realizada através do dispositivo *Cloud* no eNSP. Esse dispositivo possibilita o mapeamento entre outras *Clouds* em uma topologia, a comunicação com outros programas por meio de portas do *User Datagram Protocol* (UDP)

abertas e a comunicação com as interfaces de rede do computador. O EVE-NG também possui um dispositivo com as mesmas funções. A Figura 4.1 apresenta a configuração necessária para interligar o eNSP com a interface de rede do computador onde o EVE-NG está virtualizado.

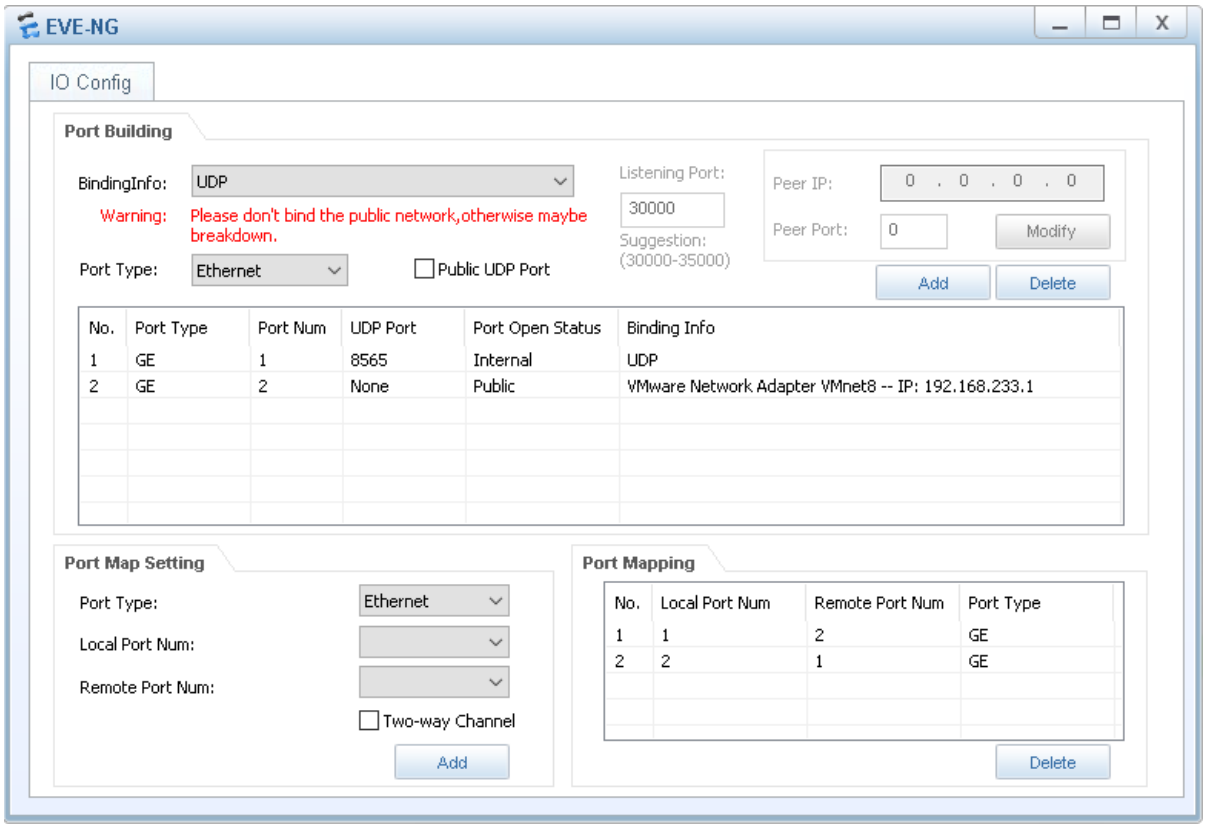

Figura 4.1: Dispositivo *Cloud* no eNSP. Fonte: Elaborado pelo Autor (2023).

4.2 Topologia

A topologia da rede desenvolvida para execução prática do trabalho está ilustrada na Figura 4.2. Essa topologia é composta por roteadores interligados por meio de um Ponto de Troca de Trafego (PTT), o *switch* denominado PTT na topologia, um computador representando o usuário final que será afetado pelos ataques, e servidores que serão utilizados para habilitação dos serviços de DNS e web para execução. Em tom alaranjado, está representada a rede sob o domínio do sistema autônomo 65003, que realizará os ataques a fim de afetar os serviços do AS 65002.

O PTT, como é chamado, representa um ponto de acesso, por meio de uma rede local, de *Data Centers*, provedores de internet e provedores de trânsito IP. No Brasil, há 36 pontos

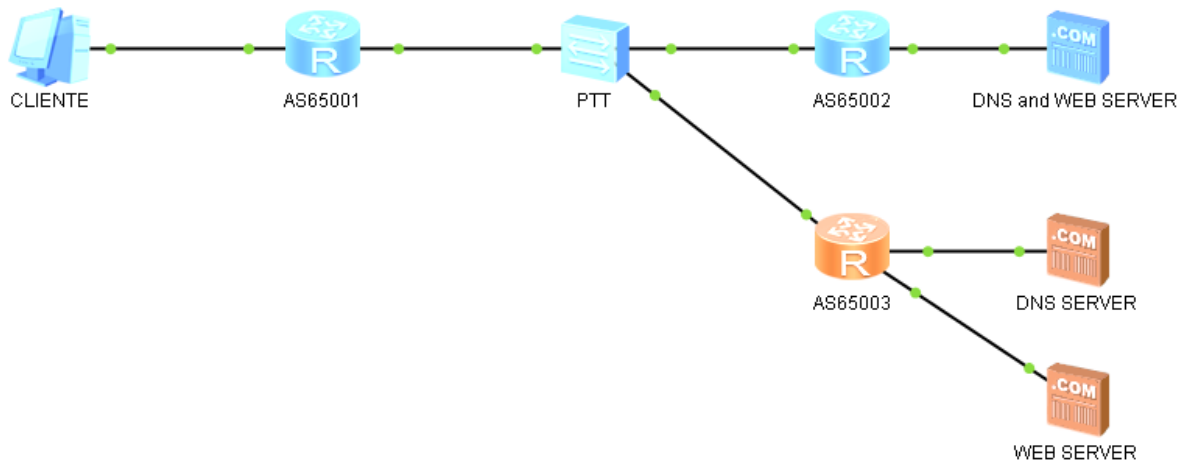

Figura 4.2: Topologia da rede. Fonte: Elaborado pelo Autor (2023).

espalhados pelo país nas principais localidades como capitais e regiões metropolitanas. O principal ponto é o PTT São Paulo que hoje conta com 2595 sistemas autônomos participantes e, através de contratos de serviços, estabelecem comunicação BGP através de seus endereços de borda, ou seja, os endereços acessíveis através da rede local no PTT.

Em Julho de 2023, o agregado do tráfego dos participantes do ponto de São Paulo alcançou um novo recorde de 31 Terabits por segundo, conforme divulgado pelo site IX.br (SHANDWICK, 2023). Como comparação. o ponto de acesso em Amsterdã, nos Países Baixos, do *Amsterdam Internet Exchange* (AMS-IX), alcançou em Outubro de 2022 o recorde de pouco mais de 11 Terabits por segundo, segundo dados divulgados em (AMS-IX, 2022); e o ponto de acesso em Nova Iorque, nos Estados Unidos, alcançou recorde de 1,5 Terabit por segundo, conforme noticiado pelo *Deutscher Commercial Internet Exchange* (DE-CIX) em (DE-CIX, 2023).

4.3 Dispositivos e Sistemas Operacionais

No eNSP há diversos roteadores e *switches* de camada 3, em referência ao modelo OSI, onde a camada 3 representa protocolos de roteamento IP, que podem ser utilizados na criação de uma topologia de rede de roteamento do protocolo BGP. Neste trabalho, utilizamos roteadores da série AR2000, que possuem baixo consumo computacional em relação aos dispositivos de grande porte, como o NE40, NE5000e e NE9000, que também estão presentes no simulador.

Com os referenciais técnicos de configuração disponíveis na página da Huawei (2023a), podemos realizar a configuração das interfaces, endereçamento de interfaces e habilitação de protocolos nos roteadores.

Os servidores necessários para a execução do trabalho estão disponíveis no eNSP, dispensando a instalação de um sistema operacional de servidor, como uma distribuição Linux para servidores, por exemplo, o Ubuntu *Server*. Neste dispositivo, por meio da interface gráfica exibida na Figura 4.3, podemos habilitar serviços como servidor HTTP, DNS e *File Transfer Protocol* (FTP) de forma simplificada, direcionando as requisições para um diretório do computador que está simulando os dispositivos.

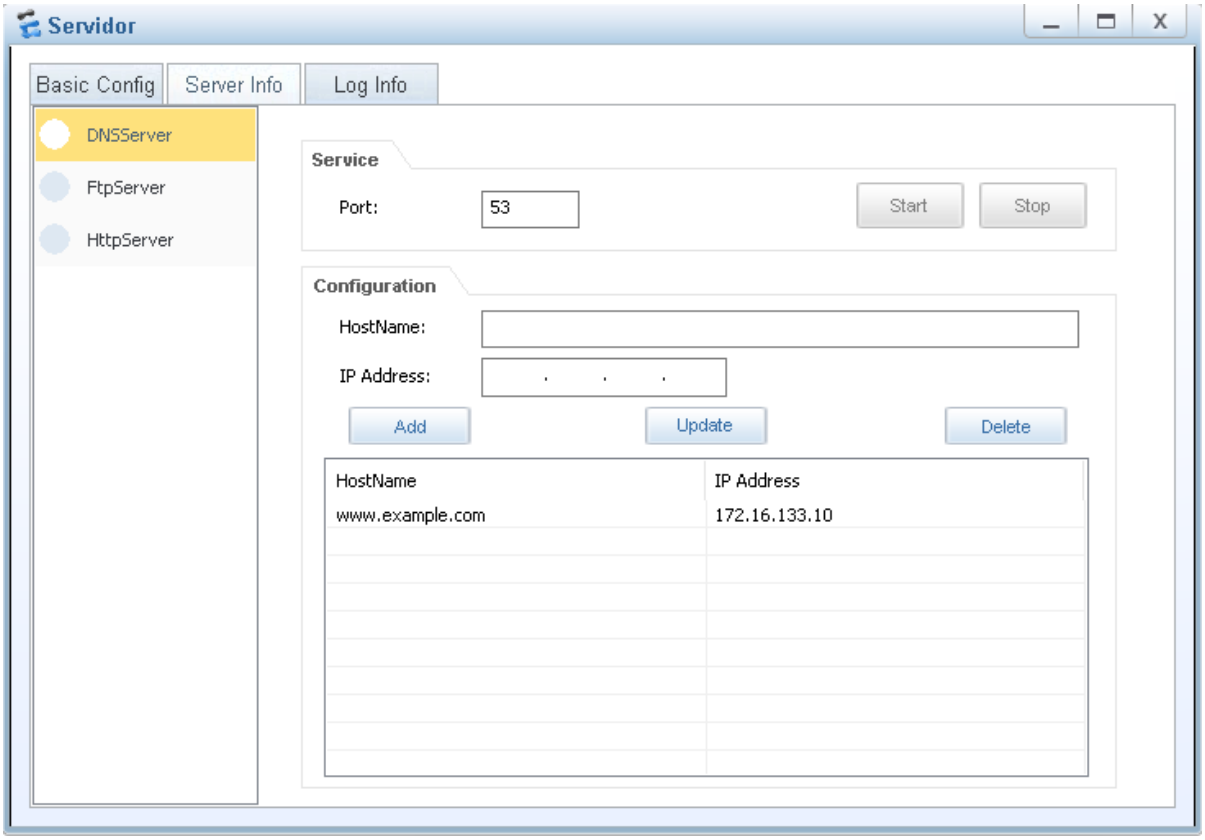

Figura 4.3: Interface gráfica do servidor. Fonte: Elaborado pelo Autor (2023).

Para a perspectiva do usuário, utilizando o EVE-NG, podemos instalar uma distribuição Linux para terminal, como o Ubuntu Desktop. A versão Desktop 20.04 do Ubuntu, lançada em abril de 2020, foi utilizada neste trabalho, pois se encontra em seu período operacional e ainda recebe atualizações de segurança.

4.4 Analisador de Pacotes

Um elemento fundamental para o desenvolvimento deste trabalho é a utilização de um analisador de pacotes, que realiza desde a captura até a desfragmentação dos pacotes trafegados em uma interface selecionada. O software de código aberto e uso gratuito Wireshark, como apresentado por Orebaugh, Ramirez e Beale (2006), pode ser utilizado, pois há integração com ambos os simuladores apresentados neste capítulo.

Ao selecionarmos a interface do dispositivo nos simuladores, realizamos a captura dos pacotes, que são desfragmentados, e obtemos todas as informações contidas no pacote, como endereços de origem e destino, protocolo e mensagens do protocolo utilizado. Protocolos não criptografados, como o HTTP e BGP, são exibidos no analisador de forma íntegra.

4.5 Cenário de Ataque

Em um cenário inicial, sem intervenção do invasor, aguardamos uma captura de pacotes que segue o fluxograma da Figura 4.4.

Na Figura 4.4, um usuário localizado na rede local do sistema autônomo 65001 solicita uma conexão e, através de um navegador, tenta acessar a URL `www.example.com`. O servidor DNS utilizado pelo usuário segue o endereço IP 172.16.133.10, pertencente ao sistema autônomo 65002, que retorna a solicitação de resolução da URL para seu próprio endereço IP, o qual é também o servidor HTTP do sistema 65002. Após receber a requisição de resolução, o usuário estabelece a sessão TCP com o servidor e inicia a comunicação do protocolo HTTP, conforme explicado na Seção 2.1 e ilustrado na Figura 2.2.

Conforme abordado na Seção 2.2, um invasor com acesso a um roteador de borda de um sistema autônomo pode manipular o tráfego de sistemas externos realizando o anúncio de um bloco de endereços mais específicos. Isso caracteriza um sequestro de sessão BGP. O AS 65002 anuncia o bloco de endereços de rede `172.16.133.0` com máscara 24, ou seja, anuncia 254 endereços de `172.16.133.1` a `172.16.133.254`. Por meio de um roteador de borda do sistema autônomo 65003, que também estabelece uma sessão BGP com a rede requerente dos serviços, AS65001, é possível anunciar o bloco de endereços `172.16.133.0` com máscara 25, que inclui endereços de `172.16.133.1` a `172.16.133.126`, redirecionando assim requisições DNS do servidor localizado no AS 65002 para sua rede interna.

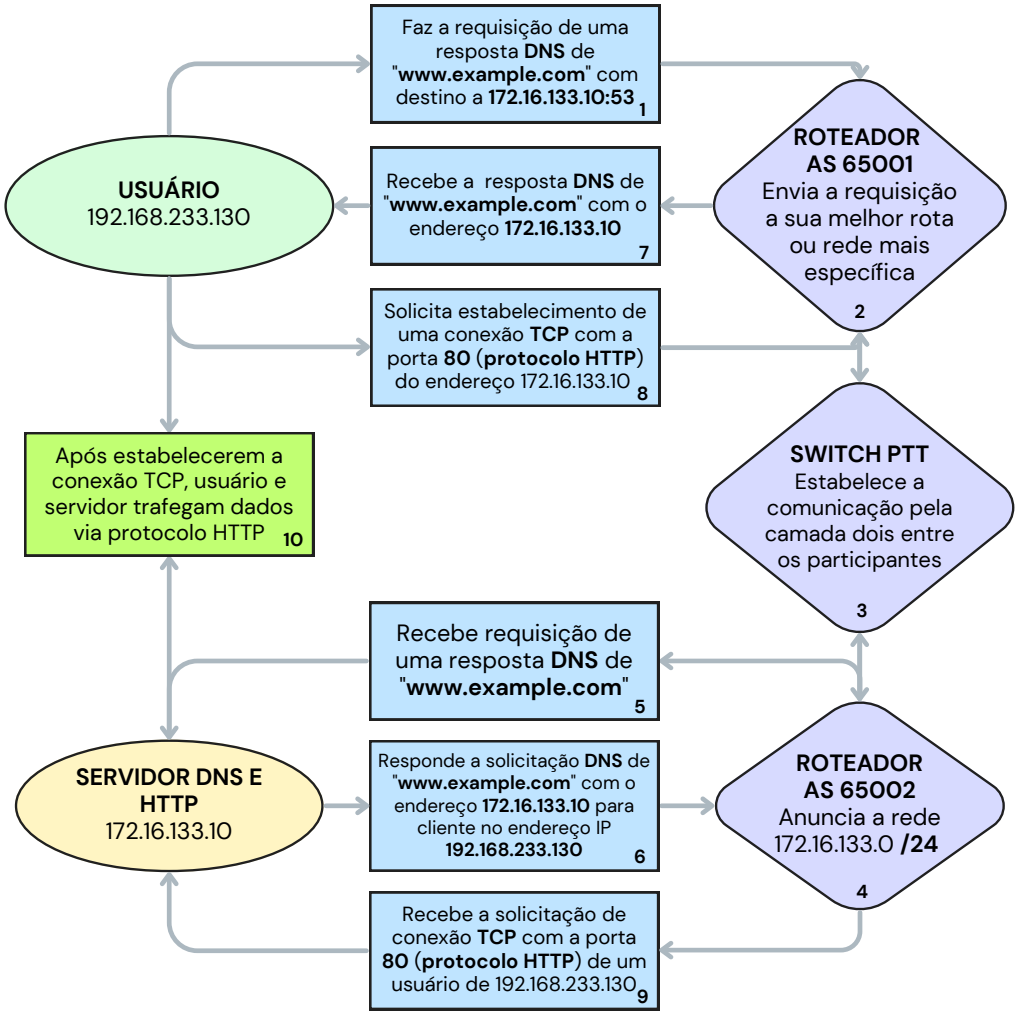

Figura 4.4: Cenário inicial. Fonte: Adaptado de Liska, Stowe e Gallo (2016).

Para realizar o ataque de *spoofing* de DNS, conforme abordado na Seção 2.4, um invasor sob o comando de um servidor DNS que está recebendo tráfego de requisições redirecionadas devido ao sequestro do bloco, deve alterar a resposta das solicitações de resolução da URL `www.example.com` para outro endereço IP. Esse endereço deve estar no bloco de endereços também anunciado pelo sistema que está atacando. O fluxograma apresentado na Figura 4.5 apresenta o ciclo de requisições e direcionamentos do usuário aos servidores ao tentar realizar a conexão no site *www.example.com*, comprometido inicialmente pelo sequestro.

A escolha do método de sequestro de rota, realizando o anúncio de um prefixo mais específico, se dá através da topologia da rede desenvolvida para o experimento, apresentada na Figura 4.2. O anúncio do bloco com o mesmo prefixo, que foi anunciado pelo AS 65002, não surtirá o efeito de desvio de tráfego desejado, pois o número de saltos necessários a partir do AS 65001 para alcançar endereços IPs no bloco `172.16.133.0` é definido por meio de quantos sistemas autônomos o pacote trafegará até seu destino final.

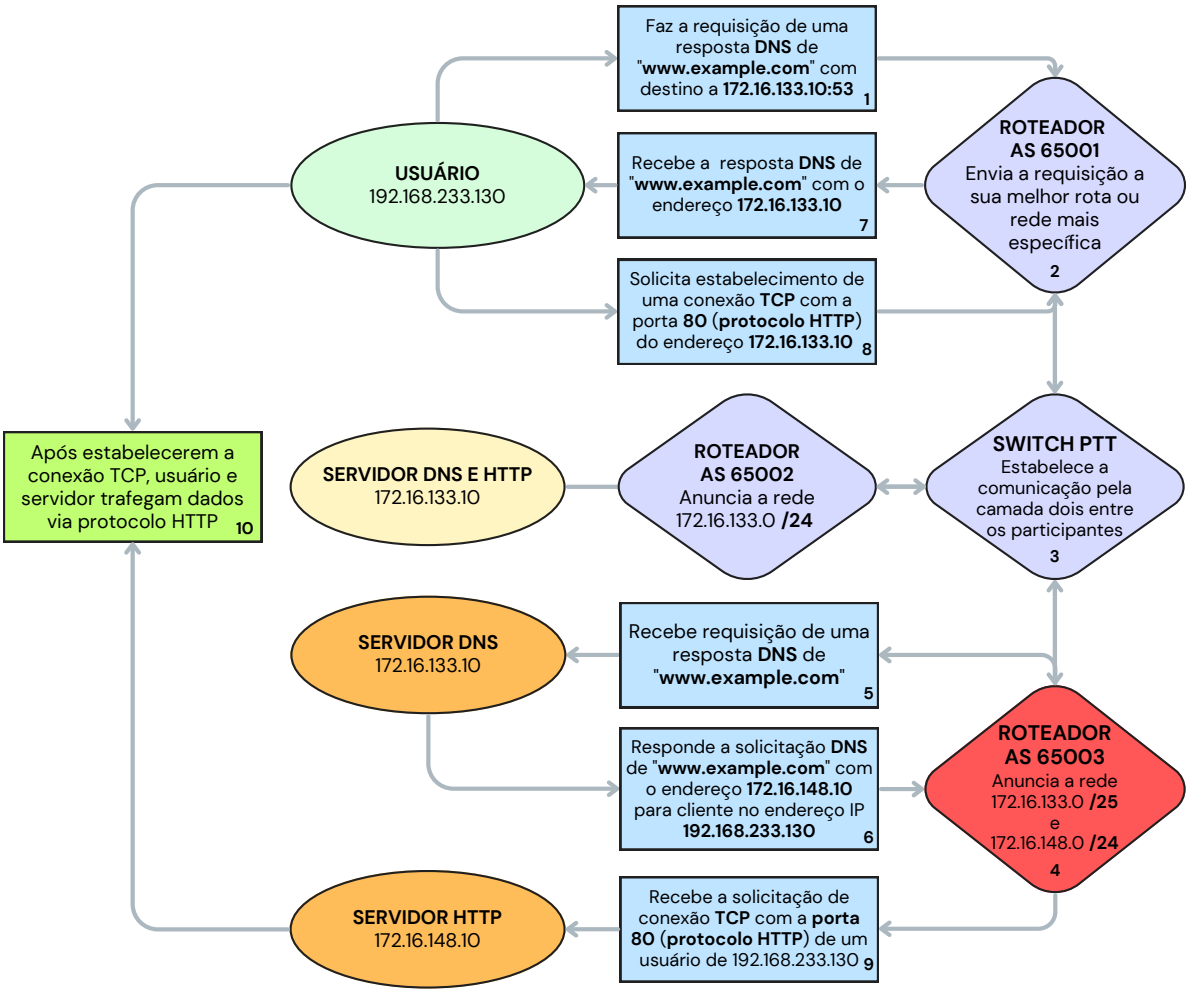

Figura 4.5: Cenário comprometido. Fonte: Elaborado pelo Autor (2023).

Além dos pacotes dos fluxogramas anteriores, espera-se capturar um pacote BGP UPDATE no momento em que o roteador do AS 65003 anunciar a rota mais específica. Esse momento será definido como o início da invasão, que durará até a tomada de medidas de mitigação que restabeleçam a comunicação do cenário inicial, conforme apresentado na Figura 4.4.

4.6 Medidas de Mitigação

Conforme introduzido no Capítulo 2, é possível realizar a manipulação do tráfego através de filtros de rotas, manipulação de rota e preferência de rota. Diante do cenário comprometido, apresentado na Seção 4.5 pela Figura 4.5, podemos implementar as seguintes medidas de mitigação, visando redirecionar o usuário ao *site* legítimo e também bloquear o tráfego para a rede que está realizando o ataque.

- Adicionar um registro local de DNS: Ao registrar localmente o endereço `www.example.com` e seu respectivo endereço IP (*172.16.133.10*), as requisições DNS ao endereço já serão respondidas pelo roteador local do usuário. Neste caso, o roteador do AS 65001, ao receber uma requisição de resolução do endereço `www.example.com`, retornará ao usuário o endereço IP do domínio registrado pelo AS65002, com base na informação DNS inserida manualmente.

- Filtro de prefixo: Bloqueando a entrada dos prefixos mais específicos, anunciados pelo sistema autônomo 65003, espera-se que o tráfego seja transmitido ao destino correto, uma vez que a rota não estará mais presente na tabela de roteamento. Através do roteador do sistema 65001, pode-se criar uma lista de endereços de rede e o intervalo de prefixos, e informar se essa rede deve ser negada ou aceita ao receber um pacote BGP UPDATE. Esta lista deve ser utilizada como parâmetro de estabelecimento de comunicação entre pares BGP. Além disso, são utilizadas para verificações de rotas importadas de uma sessão BGP ou rotas que serão exportadas na sessão, determinando se o sistema autônomo vizinho recebe ou não algumas rotas.

- Filtro de AS: Semelhante à filtragem de prefixos, pode-se bloquear a entrada de rotas vindas do sistema 65003 e também bloquear a transmissão de rotas ao AS. Desta forma, impede-se que o sistema invasor tenha conhecimento da rota para os usuários. Esta última medida tem um caráter maior de exclusão, pois é possível impedir que quaisquer rotas que passem por um ou outro sistema autônomo específico sejam registradas na tabela de roteamento.

- Comunidade BLACKHOLE: Utilizando de uma politica de roteamento, é possível encaminhar o tráfego destinado ao sistema autônomo 65003 a uma interface inválida, descartando o trafego destinado a rede comprometida.

O estudo conduzido pelos pesquisadores Sermpezis, Kotronis, Dainotti et al. (2018), mostra que 71% dos operadores de redes que responderam à pesquisa, responsáveis na atuação em incidentes, não utilizavam técnicas de mitigação de validação de origem, como o ROA. Porém, técnicas de engenharia de tráfego, como anúncio de rotas mais específicas, habilitam sessões BGP com mais vizinhos a fim de reduzir o impacto, e principalmente, 58% dos operadores que não utilizam ROA, realizam a filtragem de prefixos e `AS_Path`.

No entanto, apesar da importância de se demonstrar o funcionamento do sistema RPKI, não encontramos métodos de simulação da validação de origem compatíveis com os *softwares* e métodos definidos para a execução do trabalho neste capítulo. O trabalho de Ando, Okada e Kanaoka (2017), que simula validação de origem de incidentes de sequestro de rotas, utilizou algoritmo para reproduzir o método de seleção de caminho do protocolo BGP e posteriormente introduziu métodos matemáticos no algoritmo para simular a validação de origem. Por outro lado, o *software* `KathBGPBuilder`, introduzido por Spadaccino et al. (2023), utilizou um contêiner `Docker` para emular roteadores com suporte ao validador RPKI-RTR. Ambos os trabalhos conseguiram validar o método de validação de origem. Porém, não são compatíveis com a metodologia introduzida nesse capítulo.

4.7 Considerações Finais

Neste capítulo, apresentamos a metodologia que será utilizada para a execução dos experimentos a fim de comprovar os objetivos da Seção 1.2. Descrevemos os softwares de simulações de redes utilizados, os equipamentos virtualizados e o analisador de tráfego, que realizará a captura de pacotes que serão essenciais para a análise do evento e a afetação no cliente.

Capítulo 5

Resultados Experimentais

Neste capítulo, apresentamos os resultados obtidos através da simulação de sequestro da rota e os resultados obtidos após serem realizadas as medidas mitigatórias. Inclusive, apresentamos uma discussão neste capítulo acerca dos resultados obtidos através dos experimentos e os efeitos que cada medida mitigadora causou no cenário.

5.1 Identificando o Sequestro

Seguindo a metodologia apresentada no Capítulo 4, inicialmente, após estabelecer a comunicação entre os roteadores e criar sessões BGP, habilitamos os serviços de DNS e HTTP do servidor do sistema AS 65002. Para testar o funcionamento do serviço DNS, utilizamos o comando `dig www.example.com` no terminal de comandos do computador virtualizado do usuário, que realiza a requisição da resolução da URL e retorna a resposta bruta do protocolo. O processo está ilustrado na Figura 5.1 a seguir.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23140
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        86400   IN      A       172.16.133.10

;; Query time: 440 msec
;; SERVER: 172.16.133.10#53(172.16.133.10)
```

Figura 5.1: Resposta da Requisição DNS Inicial. Fonte: Elaborado pelo Autor (2023).

Utilizando o navegador *web* Mozilla Firefox, ao conectarmos à URL `www.example.com/home.html`, o *site* desejado é exibido, como pode ser visto na Figura 5.2 a seguir.

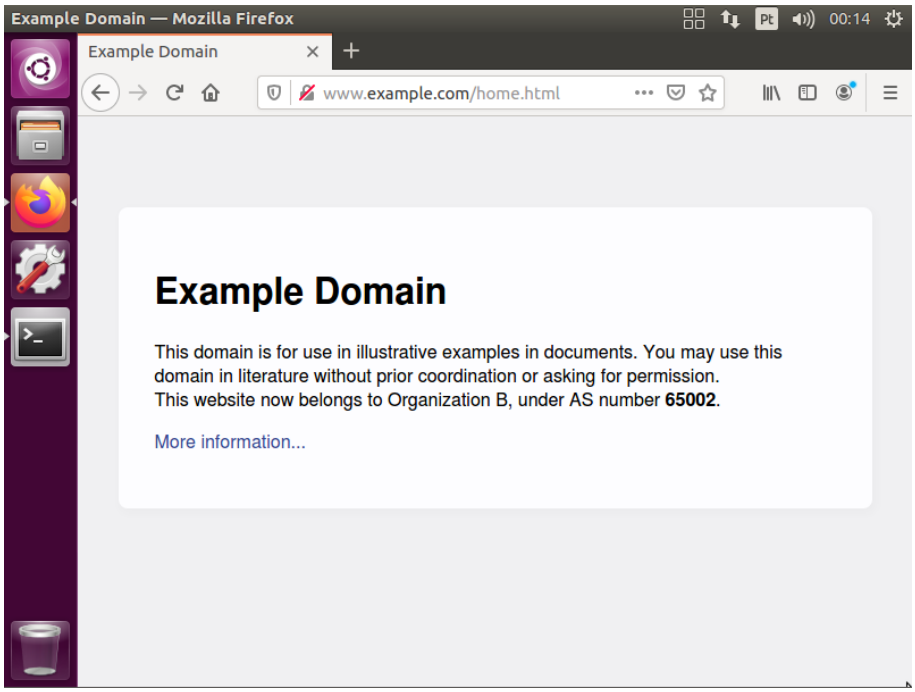

Figura 5.2: Conexão com o *site* oficial. Fonte: Elaborado pelo Autor (2023).

Com acesso ao roteador de borda do sistema autônomo 65003, realizamos o anúncio da rota `172.16.133.0` com o prefixo de rede 25, com a intenção de desviar o tráfego do AS 65002. Com auxílio do software Wireshark, capturamos os pacotes na interface do roteador de borda do AS 65001 que está conectado diretamente ao PTT. Dentre os pacotes recebidos, está uma mensagem do tipo UPDATE do protocolo BGP. Nesse pacote, havia informações sobre a nova rota inserida na tabela de roteamento, tais como `AS_PATH = 65003`. Em outras palavras, para alcançar a rede com prefixo 25, temos uma rota direta, estabelecida através da sessão entre o AS 65001 e o AS 65003.

Como pode ser visto na Figura 5.3, esse pacote contém a informação de que uma nova rota foi recebida pelo AS 65001, vindo do endereço IP `10.0.123.3` (AS 65003). No instante em que é recebida a mensagem BGP UPDATE e atualizada a tabela de roteamento do sistema, iniciou-se o sequestro dos endereços de rede `172.16.133.0`, originalmente anunciados pelo sistema autônomo 65002 e agora interceptados pelo AS 65003.

Novamente executando o comando `dig www.example.com` pelo terminal do usuário para validar o novo cenário, houve o retorno de um endereço IP diferente do exibido na

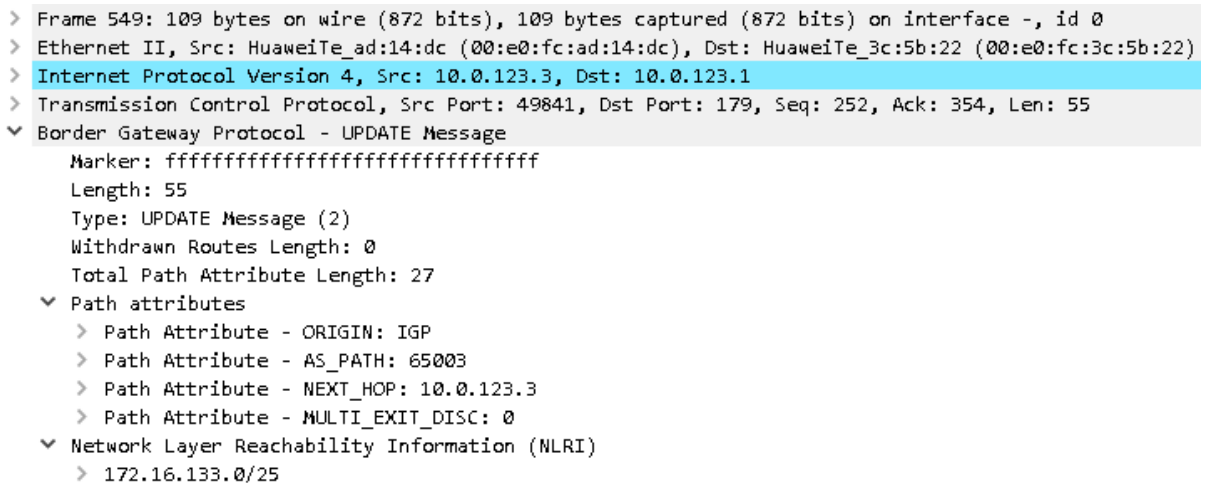

Figura 5.3: Pacote capturado do sequestro. Fonte: Elaborado pelo Autor (2023).

Figura 5.1. Com isto, confirmamos o cenário de DNS *Spoofing* também. De acordo com a Figura 5.4, para o usuário, não há indícios de que houve mudança de servidor DNS. Por isso, é transparente ao usuário final que inicialmente houve um incidente ao nível de rotas conhecidas pelo seu provedor. Somente realizando uma nova requisição de conexão através do navegador, o usuário poderá ter algum indício de que o acesso site desejado, `www.example.com`, foi comprometido.

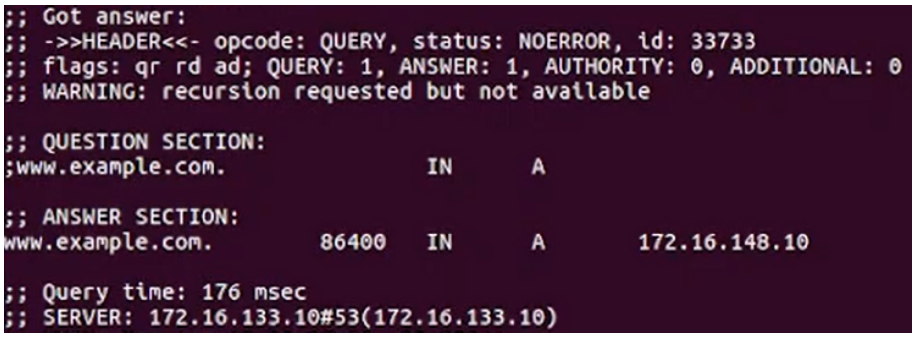

Figura 5.4: Pacote capturado do sequestro. Fonte: Elaborado pelo Autor (2023).

Analisando os dados coletados através do experimento inicial, é possível constatar a possibilidade de realizar um ataque DNS *Spoofing* em um ambiente simulado. Esse ataque é viabilizado através de um ataque de sequestro de rotas do protocolo BGP. Esse resultado positivo possibilita que a exploração de diferentes tipos de ataques a um usuário final, que fogem do escopo deste trabalho. Um exemplo simples foi a modificação do código-fonte da página *web* do site `www.example.com`. Assim, o usuário final, dentro da rede do AS 65001, conecta-se agora nessa página distinta exibida na Figura 5.5, através do Mozilla Firefox.

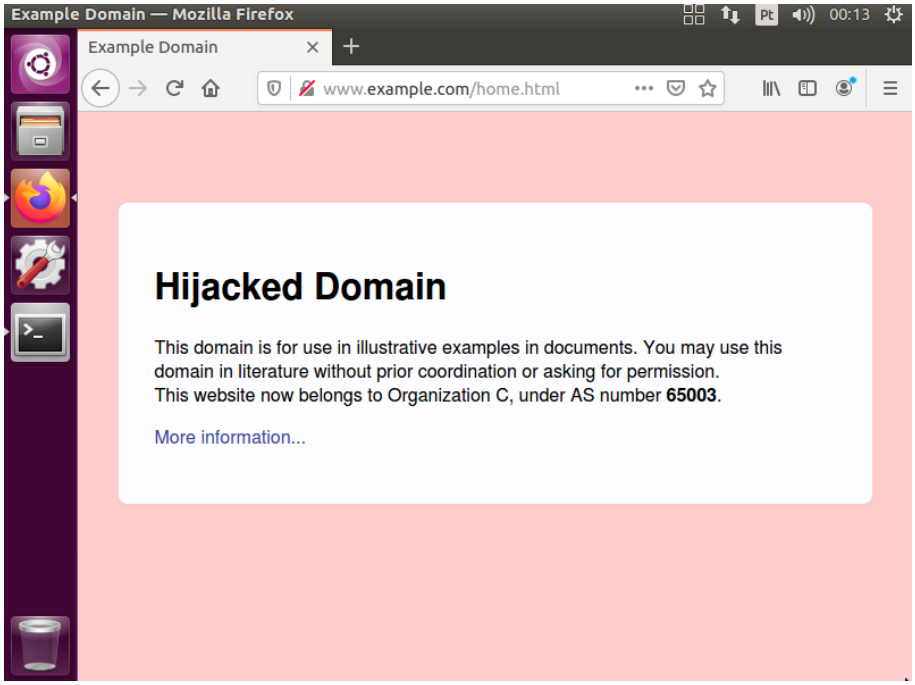

Figura 5.5: Conexão com o *site* não oficial. Fonte: Elaborado pelo Autor (2023).

5.2 Mitigando o Sequestro

Diante do resultado apresentado na Seção 5.1, comprovando a viabilidade da execução de um ataque DNS *Spoofing* através de um sequestro de rota BGP, podemos entrar com medidas mitigatórias a fim de neutralizarmos o ataque. As medidas de contra-ataque foram apresentadas na Seção 2.5.

5.2.1 Registro Local de DNS

Em uma rede local, como o cenário do AS 65001, com o auxílio do protocolo *Dynamic Host Configuration Protocol* (DHCP), introduzido para a comunidade por meio da RFC 2131 (DROMS, 1997), que distribui parâmetros de configuração, como endereço IP e servidor DNS, para computadores de forma dinâmica é possível utilizarmos o método de registro local no roteador da rede.

Com o roteador da Huawei, modelo AR 2200, utilizado neste trabalho, é possível permitir, através do serviço de DHCP, que o usuário da rede receba o endereço do próprio roteador como servidor de DNS para que as requisições de resolução sejam solicitadas ao roteador. Seguindo os referenciais técnicos disponibilizados pela fabricante, podemos configurar o equipamento para fornecer um endereço de servidor DNS pelo DHCP (HUAWEI, 2023c) e habilitar o roteador para responder às requisições de resolução de endereços (HUAWEI, 2023b). No entanto, ainda

se faz necessário registrar localmente a URL de destino e seu IP no dispositivo através do comando "`ip host www.example.com 172.16.133.10`".

Na Figura 5.6, temos uma nova captura de dados através do software Wireshark. Nela, podemos observar que o cliente, identificado pelo endereço IP `192.168.233.11` solicita a resolução do endereço para o seu *gateway*, o roteador do AS 65001, que responde conforme o registro em sua memória.

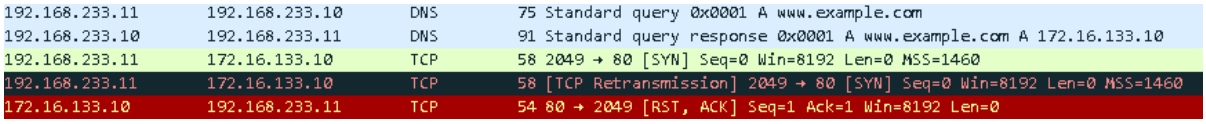

Figura 5.6: Resolução local de DNS e comunicação TCP falha com o destino. Fonte: Elaborado pelo Autor (2023).

Também na Figura 5.6, podemos observar que o cliente envia um pacote SYN para o endereço `172.16.133.10`, a fim de estabelecer uma conexão TCP com a porta 80 (protocolo HTTP). Após não receber um ACK desejado do servidor, o cliente envia novamente a mensagem SYN para a porta 80 como uma retransmissão no protocolo. Dessa forma, notifica o servidor que não houve o recebimento do ACK e solicita uma resposta que, por sua vez, responde com um pacote contendo as mensagens RST e ACK.

Conforme documentado na RFC 793 (POSTEL, 1981), a mensagem RST é enviada quando um pacote recebido não é destinado a uma conexão atual. Nesse caso uma porta aberta, a mensagem é enviada para o cliente encerrar a tentativa de estabelecer comunicação pelo protocolo TCP. Nesse cenário, o servidor `172.16.133.10` não permite a conexão. pois a porta 80, referente ao serviço HTTP, não está disponível, indicando que o servidor não é um servidor web.

Na Figura 5.7, executamos comando `traceroute` a partir do roteador do AS 65001 que. através das mensagens ECHO do protocolo *Internet Control Message Protocol* (ICMP), obtém o caminho que uma mensagem trafegou no sentido cliente para servidor. Notamos que o endereço IP do AS 65003, `10.0.123.3`, apareceu na resposta do comando, indicando que o tráfego segue destinado à rede indesejada.

Essa abordagem mostrou-se positiva para a neutralização do DNS *Spoofing*, pois a requisição a URL retorna ao cliente o endereço IP correto do servidor. Porém, não houve mudanças no quesito do roteamento aprendido pelo AS 65001.

```
[BORDA-AS65001]tracert www.example.com

traceroute to  172.16.133.10(www.example.com)
max hops: 30 ,packet length: 40,press CTRL_C to break

1 10.0.123.3 60 ms  40 ms  30 ms

2 172.16.133.10 < AS=65003 > 40 ms  40 ms  50 ms
```

Figura 5.7: Comando `tracert` rastreando o pacote até o AS65003. Fonte: Elaborado pelo Autor (2023).

5.2.2 Filtragem de Prefixos

Esta abordagem, segundo apresentado na Seção 2.5, consiste em negar a recepção ou a transmissão de rotas, com base no seu endereço de rede e o intervalo de prefixos, através da mensagem BGP UPDATE. Pela topologia da Figura 4.5, há dois cenários de atuação através do AS 65001. São eles:

- Não transmitir a rede local, `192.168.233.0/24`, para a sessão BGP com o AS 65003.
- Não aceitar um endereço de rede recebido através da mensagem UPDATE ou uma rede mais específica, negando a rede `172.16.133.0` com mascará 25 ou até o prefixo 32, porém aceitando os qualquer outra rede anunciada pelo AS vizinho.

O primeiro item causa apenas o efeito na tabela de roteamento do AS 65003. Assim, o roteador do sistema autônomo 65001 segue com a informação da rota incorreta em sua tabela, e pacotes são transmitidos para a rede de 65003. Porém, sem resposta, pois a rede não contém a informação sobre rota para o endereço do pacote que foi recebido. Portanto, a segunda forma apresenta-se mais adequada para o cenário, pois o filtro irá descartar a rede indesejada, e o AS 65001 ira ter em sua tabela de roteamento a rota para `172.16.133.0/24` anunciada pelo AS 65002 e nenhuma outra mais específica.

O site do MANRS (2023b) disponibiliza exemplos de configurações baseadas nas melhores práticas de operação e manutenção do procolo BGP, conforme a RFC 7454, de diversos fabricantes de roteadores e switches que fazem parte e apoiam essa iniciativa. A Huawei é uma delas e há exemplos de configurações de filtros que podem ser utilizados no roteador AR 2200. O primeiro índice do filtro nega o prefixo de rede `172.16.133.0` de 25 até 32; enquanto o segundo índice utiliza o IP padrão `0.0.0.0/0` para indicar que aceita as demais rotas. Pela Figura 5.8, que foi obtida após a aplicação do filtro com os parâmetros indicados, podemos observar a nova tabela de roteamento conhecida pelo AS 65001. Essa tabela contém apenas duas rotas: uma pertencente ao AS 65002 e outra pertencente ao AS 65003.

```
[BORDA-AS65001-bgp]display bgp routing-table

 BGP Local router ID is 10.0.123.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 2
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   172.16.133.0/24    10.0.123.2      0                      0      65002i
 *>   172.16.148.0/24    10.0.123.3      0                      0      65003i
```

Figura 5.8: Tabela de roteamento do AS65001 após filtragem. Fonte: Elaborado pelo Autor (2023).

Com o auxílio do Wireshark, capturamos um pacote contendo a mensagem BGP UPDATE que informa aos seus pares que realizam conexão BGP, que a rota *172.16.133.0/25* foi removida de sua tabela de roteamento. A Figura 5.9 ilustra a captura desse pacote.

```
> Frame 806: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface -, id 0
> Ethernet II, Src: HuaweiTe_3c:5b:22 (00:e0:fc:3c:5b:22), Dst: HuaweiTe_ad:14:dc (00:e0:fc:ad:14:dc)
> Internet Protocol Version 4, Src: 10.0.123.1, Dst: 10.0.123.3
> Transmission Control Protocol, Src Port: 179, Dst Port: 49864, Seq: 838, Ack: 827, Len: 28
v Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 28
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 5
  v Withdrawn Routes
    v 172.16.133.0/25
        Withdrawn route prefix length: 25
        Withdrawn prefix: 172.16.133.0
    Total Path Attribute Length: 0
```

Figura 5.9: Pacote capturado com a remoção de rotas. Fonte: Elaborado pelo Autor (2023).

Executando novamente o comando `traceroute` com destino ao site `www.example.com`, pode-se comprovar que o tráfego foi direcionado corretamente à rede na qual o serviço original estava hospedado. Com esta confirmação, podemos assegurar que a medida empregada – mitigar o sequestro por meio de implantação de filtros que bloqueiam o recebimento de rotas indesejadas – é de grande eficácia para um cenário de sequestro de rotas BGP por especificação de prefixo.

5.2.3 Filtragem de *AS_Path*

Conforme comentamos na Seção 2.5, semelhante à filtragem na recepção e transmissão de prefixos, é possível filtrar as rotas com o número do sistema autônomo presente no parâmetro

AS_Path. Esse tipo de filtragem é mais excludente, pois excluirá da tabela de roteamento qualquer rota que tenha algum número da tabela de roteamento presente no filtro negador.

Configuramos dois filtros no roteador – um que rejeita o AS 65003 e outro que rejeita o AS 65001 – aplicados respectivamente na importação e na exportação de rotas. Aplicando esses filtros na sessão com o endereço 10.0.123.3, endereço do AS 65003 no PTT, podemos constatar, por meio da Figura 5.10, que ambos roteadores não possuem rotas anunciadas pelo outro em suas tabelas de roteamento.

```
[BORDA-AS65001]display bgp routing-table
Total Number of Routes: 2
     Network            NextHop         MED        LocPrf    PrefVal Path/Ogn

*>   172.16.133.0/24    10.0.123.2       0                      0      65002i
*>   192.168.233.0      0.0.0.0          0                      0      i
[BORDA-AS65003]display bgp routing-table
Total Number of Routes: 2
     Network            NextHop         MED        LocPrf    PrefVal Path/Ogn

*>   172.16.133.0/25    0.0.0.0          0                      0      i
*>   172.16.148.0/24    0.0.0.0          0                      0      i
```

Figura 5.10: Tabela de roteamento do AS 65001 e AS65003 após filtragem. Fonte: Elaborado pelo Autor (2023).

Nessa topologia, a utilização da metodologia de filtragem pode ser aplicada devido à menor dimensão da rede. No entanto, a propagação de um filtro excludente pode causar interrupções de rotas globalmente.

O uso da técnica deve ser empregado com precaução pelo responsável pelo roteamento em um sistema autônomo, pois ainda é uma ferramenta que se apresentou muito útil na engenharia de tráfego. O filtro de AS pode estar no acordo mútuo entre os pares para que determinadas rotas não sejam transmitidas para as demais sessões que o sistema realiza.

5.2.4 Comunidade *BLACKHOLE*

Como apresentado na Seção 2.5, para descartar transmissões destinadas à rota afetada, deve-se inserir um próximo salto com uma interface de saída inválida. Configuramos no roteador da Huawei que o endereço 10.0.66.66/32, um endereço de uso privado, será utilizado como o BLACKHOLE e registrado na interface NULL 0. Trata-se de interface virtual utilizada apenas para o descarte de pacotes.

Com uma política de roteamento criada no equipamento pode-se estabelecer que, caso a rota contenha a comunidade – definida com um o número 65003:666, em que o sufixo 666

é definido através da RFC 7999 (KING et al., 2016) –, será aplicado o próximo salto para a interface de descarte. A Figura 5.11 apresenta criação da regra e suas definições.

```
[BORDA-AS65001]display route-policy DESCARTA
Route-policy : DESCARTA
  permit : 10 (matched counts: 0)
  description : Regra de descarte de pacotes
    Match clauses :
      if-match community-filter 65003:666
    Apply clauses :
      apply ip-address next-hop 10.0.66.66
```

Figura 5.11: Política de roteamento com a comunidade. Fonte: Elaborado pelo Autor (2023).

Ao aplicar essa regra de roteamento, é possível observar, através da tabela de roteamento do roteador de borda, a mudança do parâmetro *NextHop* da Figura 5.12. Isso indica que a nova política de roteamento com o descarte de rotas foi aplicada com sucesso.

```
[BORDA-AS65001]display bgp routing-table

BGP Local router ID is 10.0.123.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


Total Number of Routes: 4
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   172.16.133.0/24    10.0.123.2     0                    0       65002i
*>   172.16.133.0/25    10.0.66.66     0                    0       65003i
*>   172.16.148.0/24    10.0.66.66     0                    0       65003i
*>   192.168.233.0      0.0.0.0        0                    0       i
```

Figura 5.12: Tabela de roteamento após aplicação do BLACKHOLE. Fonte: Elaborado pelo Autor (2023).

Ao testar, através do comando `ping`, a comunicação com o *site*, inicialmente recebemos uma resposta informando erro de comunicação, devido à não resolução do endereço pelo protocolo DNS. Como não há a comunicação com o endereço IP `172.16.133.10`, não é possível realizar a resolução do endereço pelo DNS.

Utilizando o registro local de DNS, apresentado na Seção 5.2.1, e testando novamente a comunicação com o *site*, é possível ver, através da Figura 5.13, o resultado desejado. Assim, os pacotes são transmitidos. Porém, não há retorno de nenhum pacote, indicando que foram transmitidos a uma interface que os descartou.

Essa abordagem mostra-se útil em cenários no quais é necessário impedir, imediatamente, o acesso indevido dos usuários a um domínio ou endereço IP de um serviço comprometido.

```
[BORDA-AS65001]ping www.example.com
Error: Unknown host www.example.com.
[BORDA-AS65001]ip host www.example.com 172.16.133.10
[BORDA-AS65001]ping www.example.com
  PING www.example.com (172.16.133.10): 56  data bytes
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- www.example.com ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Figura 5.13: Teste de comunicação após aplicação do BLACKHOLE. Fonte: Elaborado pelo Autor (2023).

5.3 Considerações Finais

Neste capítulo apresentamos os resultados obtidos através dos experimentos realizados através do simulador de redes eNSP, da Huawei, EVE-NG e o analisador de tráfego Wireshark. Os experimentos realizados, introduzidos no Capítulo 4, alcançaram os resultados esperados para cumprimento dos objetivos especificados na Seção 1.2.

A abordagem da utilização do filtro de prefixo e o registro de local de resolução de nomes foi observada como melhor abordagem, pois o cliente estaria recebendo a requisição de resolução DNS diretamente do seu roteador. Assim, não fica dependendo de um servidor DNS externo. Enquanto o registro local neutraliza o efeito de DNS *Spoofing*, o descarte de rotas filtradas neutraliza o sequestro da rota BGP.

Foi discutido também a utilização de uma política de roteamento para descarte de tráfego utilizando uma comunidade BGP.

Capítulo 6

Conclusões

Este trabalho utilizou dados obtidos através de captura de pacotes para comprovar a viabilidade da execução de um ataque DNS *Spoofing*. O experimento realizado foi um sequestro de rotas do protocolo BGP, em um cenário simulado de um ponto de troca de tráfego e sistemas autônomos representando provedores de serviços web e provedores de internet.

Para alcançar esse objetivo, foi realizado primeiramente um levantamento bibliográfico de artigos científicos que abordam os temas de ataques de DNS e segurança de roteamento do protocolo BGP. Durante a pesquisa, não encontramos nenhum artigo que abordasse o tema ataques de DNS através de desvios de rotas por BGP, apesar de ter casos reais de ataques em cenário semelhante.

O estudo dos referenciais técnicos para padrões da Internet, as RFCs, foram de grande importância para a monografia, pois por meio delas foi possível compreender os protocolos de redes utilizados no desenvolvimento do trabalho. As RFCs abordam, além da introdução ao protocolo e sua operação, os estudos de vulnerabilidades e medidas de segurança dos protocolos.

A partir de uma topologia estabelecida – em que três sistemas autônomos fazem parte de membros de um ponto de troca de tráfego – e utilizando o simulador de redes da companhia chinesa Huawei, o eNSP, foram executados os ataques de desvio de rota e posteriormente, o redirecionamento do acesso de um usuário final a um *site* comprometido. O trabalho também tinha como objetivo estabelecer uma medida de mitigação dos ataques, neutralizando não somente o sequestro de rotas anunciadas pelo BGP como o direcionamento correto do usuário final ao *site* de destino.

Os resultados foram obtidos por meio das simulações executadas no software eNSP, com emulação de uma máquina virtual de um usuário final utilizando um navegador web e com a análise de pacotes de rede capturados pelo software Wireshark. Com os resultados, constatamos que o cenário proposto é vulnerável a este tipo de ataque.

Durante a análise, foi possível identificar os dados enviados pelo protocolo BGP, a partir dos roteadores. Esses dados contêm o anúncio de uma rota por AS e o descarte da rede após as medidas de contenção surtirem efeito e neutralizarem os ataques.

As medidas de defesa implementadas neste trabalho, apesar de surtirem o efeito desejado protegendo a rede, não são uma técnica escalável. Isso devido à complexidade em se implementar múltiplos filtros em uma sessão ativa e a necessidade de um planejamento prévio, a fim de não realizar filtro em um endereço distinto e causar um novo incidente BGP.

O método de mitigação por meio de uma comunidade do tipo BLACKHOLE, que destina todos pacotes a uma interface inválida para descarta-los, se mostra eficiente para uma medida inicial em que seja necessário impedir o tráfego dos usuários a um endereço ou serviço comprometido afim de presarmos pela segurança, no entanto, esta medida não soluciona o sequestro da rota e os usuários não tem seu serviço reestabelecido enquanto outras medidas não forem aplicadas, como a filtragem de prefixos e AS_Path. As comunidades BGP podem ser utilizadas não apenas com o fim de descarte de tráfego, porém também como a engenharia de tráfego, influenciando parâmetros como a exportação de rotas a determinados sistemas autônomos, aplicação de valores de preferência em rotas entre outros.

A organização MANRS e a RFC 7454 recomendam o uso de filtros IP e de AS_Path para os chamados *bogons*. Esses são endereços IP e números de sistemas de uso privado, pois são considerados não roteáveis e o anúncio desses endereços pode causar conflitos em redes locais onde é comum o uso desses endereços.

O uso da validação de origem através do sistema RPKI é a principal recomendação de implementação atualmente, devido à sua escalabilidade, à automatização e à confiabilidade em sua filtragem, pois os validadores consultam diversas bases de dados de órgãos regionais de registradores de domínios.

6.1 Trabalhos Futuros

Esta monografia e seus resultados podem ser estendidos a outras pesquisas cujos objetivos fogem do escopo inicial deste trabalho. Como exemplo, é possível simular o impacto em serviços reais caso um incidente desse nível ocorra. Além disso, uma estimativa prévia de impacto pode ser realizada a fim demostrar a importância da implementação de medidas de segurança antes que ocorra um incidente.

O sequestro de rotas também pode ser utilizado para estudar ataques do tipo *man-in-the-middle*, onde ocorre a intercepção da comunicação por um invasor com o propósito de obter informações sensíveis como senhas e dados bancários, entre outros. Um atacante pode se aproveitar de um incidente de rotas e utilizar técnicas de IP *Sniffing*, interceptando os pacotes destinados a um endereço IP para análise e desfragmentação. Depois, retransmitir as informações ao destinatário correto. Desta forma, o usuário final não teria indicativos que estaria sofrendo um ataque.

O mesmo cenário deste trabalho pode ser utilizado para explorar técnicas de ataques via páginas web, coletando dados de usuários que acreditam trafegar em um *site* legitimo. A técnica também pode ser estendida para estudar medidas de mitigação desses ataques web, como os provedores do serviço oficial implementarem medidas de proteção e autenticidade dos seus *sites*.

Referências Bibliográficas

AMS-IX. New Peak traffic record in Amsterdam: 11 Tbps. **Ams-IX**, Amsterdam, 2022. Disponível em: <https://www.ams-ix.net/ams/news/new-peak-traffic-record-in-amsterdam-11-tbps>. Acesso em: 7 set. 2023.

ANDO, M.; OKADA, M.; KANAOKA, A. Simulation Study of BGP Origin Validation Effect against Mis-Origination with Internet Topology. In: 2017 12th Asia Joint Conference on Information Security (AsiaJCIS). Seoul: IEEE, ago. 2017. P. 75–82. ISBN 978-1-5386-2132-5. DOI: 10.1109/AsiaJCIS.2017.17. Disponível em: <https://ieeexplore.ieee.org/document/8026044/>.

CHO, S. et al. BGP hijacking classification. In: 2019 Network Traffic Measurement and Analysis Conference (TMA). Paris, France: IEEE, jun. 2019. P. 25–32. ISBN 978-3-903176-17-1. DOI: 10.23919/TMA.2019.8784511.

CISCO SYSTEMS. **An Introduction to IGRP**. Ago. 2005. Disponível em: <https://www.cisco.com/c/en/us/support/docs/ip/interior-gateway-routing-protocol-igrp/26825-5.html>. Acesso em: 7 set. 2023.

DE-CIX. Summer Traffic Peak Report. **DE-CIX**, ago. 2023. Disponível em: <https://www.de-cix.net/en/about-de-cix/news/summer-traffic-peak-report>.

CORAZZA, J. **O Minimo que você precisa saber sobre IRR Wiki BPF**. [S.l.: s.n.], dez. 2019. Disponível em: <https://wiki.brasilpeeringforum.org/w/O_Minimo_que_Voce_precisa_saber_sobre_IRR>. Acesso em: 25 set. 2023.

DECLAN, M. **How Pakistan knocked YouTube offline (and how to make sure it never happens again)**. Fev. 2008. Disponível em: <https://www.cnet.com/culture/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/>. Acesso em: 7 set. 2023.

DROMS, R. **Dynamic Host Configuration Protocol**. [S.l.]: RFC Editor, mar. 1997. 45 p. RFC 2131. (Request for Comments, 2131). DOI: 10.17487/RFC2131.

DURAND, J.; PEPELNJAK, I.; DÖRING, G. **BGP Operations and Security**. [S.l.]: RFC Editor, fev. 2015. 26 p. RFC 7454. (Request for Comments, 7454). DOI: 10.17487/RFC7454.

GRIMES, R. A. **Hacking Multifactor Authentication**. Indianapolis: John Wiley e Sons, 2020. v. 1. ISBN 978-1-119-65079-9.

HEDRICK, C. **Routing Information Protocol**. [S.l.]: RFC Editor, jun. 1988. 33 p. RFC 1058. (Request for Comments, 1058). DOI: 10.17487/RFC1058.

HEFFERNAN, A. **Protection of BGP Sessions via the TCP MD5 Signature Option**. [S.l.]: RFC Editor, ago. 1998. 6 p. RFC 2385. (Request for Comments, 2385). DOI: 10.17487/RFC2385.

HUAWEI. **Example for Configuring Basic BGP Functions – AR100, AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, and AR3600 V200R010 CLI-based Configuration Guide – IP Unicast Routing - Huawei**. 2023. Disponível em: <https://support.huawei.com/enterprise/en/doc/EDOC1100034072/9a2ddc78/example-for-configuring-basic-bgp-functions>. Acesso em: 7 set. 2023.

HUAWEI. **Example for Configuring DNS Proxy - AR100, AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, and AR3600 V200R010 CLI-based Configuration Guide - IP Service - Huawei**. 2023. Disponível em: <https://support.huawei.com/enterprise/en/doc/EDOC1100034071/886932a2/example-for-configuring-dns-proxy>. Acesso em: 7 set. 2023.

HUAWEI. **Example for Configuring the Device as a DHCP Server (Based on the Interface Address Pool) - AR100, AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, and AR3600 V200R010 CLI-based Configuration Guide - IP Service - Huawei**. 2023. Disponível em: <https://support.huawei.com/enterprise/en/doc/EDOC1100034071/f02ffa43/example-for-configuring-the-device-as-a-dhcp-server-based-on-the-interface-address-pool>. Acesso em: 7 set. 2023.

HUSSAIN, M. A. et al. DNS Protection against Spoofing and Poisoning Attacks. In: 2016 3rd International Conference on Information Science and Control Engineering (ICISCE). Beijing: IEEE, 2016. P. 1308–1312. DOI: 10.1109/ICISCE.2016.279.

IX.BR. **Serviço de Route-Server do IX.br**. [S.l.: s.n.]. Disponível em: <https://ix.br/route-server-and-commmunities>.

K. LOUGHEED, Y. R. **Border Gateway Protocol (BGP)**. [S.l.]: RFC Editor, jun. 1989. 17 p. RFC 1105. (Request for Comments, 1105). DOI: 10.17487/RFC1105.

KING, T. et al. **BLACKHOLE Community**. [S.l.: s.n.], out. 2016. DOI: 10.17487/RFC7999. Disponível em: <https://datatracker.ietf.org/doc/rfc7999>.

LEPINSKI, M.; KENT, S. **An Infrastructure to Support Secure Internet Routing**. [S.l.]: RFC Editor, fev. 2012. 24 p. RFC 6480. (Request for Comments, 6480). DOI: 10.17487/RFC6480.

LI, T.; CHANDRA, R.; TRAINA, P. S. **BGP Communities Attribute**. [S.l.]: RFC Editor, ago. 1996. 5 p. RFC 1997. (Request for Comments, 1997). DOI: 10.17487/RFC1997.

LISKA, A.; STOWE, G.; GALLO, T. **DNS security**: defending the Domain Name System. Amsterdam: Elsevier Syngress Media Inc, 2016. v. 1. ISBN 978-0-12-803306-7. DOI: 10.1016/c2014-0-04564-9.

LYSTRUP, O. **BGP Stream: The Emergency Alert System for the Internet**. [S.l.: s.n.], jul. 2015. Disponível em: <https://umbrella.cisco.com/blog/bgp-stream-the-emergency-alert-system-for-the-internet>.

MACFARLAND, D. C.; SHUE, C. A.; KALAFUT, A. J. Characterizing Optimal DNS Amplification Attacks and Effective Mitigation. **Passive and Active Measurement**, Springer International Publishing, v. 1, p. 15–27, 2015. DOI: 10.1007/978-3-319-15509-8_2.

MANRS. **MANRS ROA Stats Tool - Search by Country**. [S.l.: s.n.]. Disponível em: <https://roa-stats.manrs.org/country>. Acesso em: 25 set. 2023.

MANRS. **Mutually Agreed Norms for Routing Security**. 2023. Disponível em: <https://www.manrs.org/participant/85/>. Acesso em: 7 set. 2023.

MCBRIDE, M. et al. **AS Path Prepending**. [S.l.], jun. 2023. 12 p. Work in Progress. Disponível em: <https://datatracker.ietf.org/doc/draft-ietf-grow-as-path-prepending/08/>. Acesso em: 7 set. 2023.

MITCHELL, J. **Autonomous System (AS) Reservation for Private Use**. [S.l.]: RFC Editor, jul. 2013. 4 p. Internet Requests for Comments. (Request for Comments, 6996). DOI: 10.17487/RFC6996.

MOCKAPETRIS, P. **Domain Names – Concepts and Facilities**. [S.l.]: RFC Editor, nov. 1987. 55 p. RFC 1034. (Request for Comments, 1034). DOI: 10.17487/RFC1034.

MOCKAPETRIS, P. **Domain Names – Implementation and Specification**. [S.l.]: RFC Editor, nov. 1987. 55 p. RFC 1035. (Request for Comments, 1035). DOI: 10.17487/RFC1035.

MOHAPATRA, P. et al. **BGP Prefix Origin Validation**. [S.l.]: RFC Editor, jan. 2013. 10 p. RFC 6811. (Request for Comments, 6811). DOI: 10.17487/RFC6811.

MURPHY, S. L. **BGP Security Vulnerabilities Analysis**. [S.l.]: RFC Editor, jan. 2006. 22 p. RFC 4272. (Request for Comments, 4272). DOI: 10.17487/RFC4272.

NEVES, F.; SILVA DAMAS, J. da. **Preventing Use of Recursive Nameservers in Reflector Attacks**. [S.l.]: RFC Editor, out. 2008. 7 p. RFC 5358. (Request for Comments, 5358). DOI: 10.17487/RFC5358. Disponível em: <https://www.rfc-editor.org/info/rfc5358>.

OLIVEIRA, V. C. Simulador Eve-NG em projetos de redes heterogêneas: um estudo sobre a importância da simulação em redes de computadores. **Research, Society and Development**, Research, Society e Development, v. 9, n. 11, e1199119562, nov. 2020. DOI: 10.33448/rsd-v9i11.9562.

ORAN, D. **OSI IS-IS Intra-domain Routing Protocol**. [S.l.], fev. 1990. 517 p. (Request for Comments, 1142). DOI: 10.17487/RFC1142.

OREBAUGH, A.; RAMIREZ, G.; BEALE, J. **Wireshark & Ethereal network protocol analyzer toolkit**. Amsterdam: Elsevier, 2006. ISBN 978-1-59749-073-3. DOI: 10.1016/B978-1-59749-073-3.X5000-3.

PAGANINI, P. **Google Public DNS Server Traffic Hijacked, Millions users impacted**. Mar. 2014. Disponível em: <https://securityaffairs.com/23150/cyber-crime/google-public-dns-server-traffic-hijacked-millions-users-impacted.html>. Acesso em: 7 set. 2023.

POSTEL, J. **Transmission Control Protocol**. [S.l.]: RFC Editor, set. 1981. 91 p. RFC 793. (Request for Comments, 793). DOI: 10.17487/RFC0793.

RASHEVSKIY, R. B.; SHABUROV, A. S. BGP-hijacking attacks: Theoretical basis and practical scenarios. **2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)**, p. 208–212, 2017. DOI: 10.1109/EIConRus.2017.7910530.

REKHTER, Y.; HARES, S.; LI, T. **A Border Gateway Protocol 4 (BGP-4)**. [S.l.]: RFC Editor, jan. 2006. 104 p. RFC 4271. (Request for Comments, 4271). DOI: 10.17487/RFC4271.

RIPE, N. **Youtube Hijacking: A RIPE NCC RIS case study**. Mar. 2008. Disponível em: <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>. Acesso em: 7 set. 2023.

SCHLAMP, J. et al. HEAP: Reliable Assessment of BGP Hijacking Attacks. **IEEE Journal on Selected Areas in Communications**, v. 34, n. 6, p. 1849–1861, jun. 2016. ISSN 0733-8716. DOI: 10.1109/JSAC.2016.2558978.

SERMPEZIS, P.; KOTRONIS, V.; DAINOTTI, A.; DIMITROPOULOS, X. A Survey among Network Operators on BGP Prefix Hijacking. **ACM SIGCOMM Computer Communication Review**, v. 48, n. 1, p. 64–69, abr. 2018. ISSN 0146-4833. DOI: 10.1145/3211852.3211862.

SERMPEZIS, P.; KOTRONIS, V.; GIGIS, P. et al. ARTEMIS: Neutralizing BGP Hijacking Within a Minute. **IEEE/ACM Transactions on Networking**, v. 26, n. 6, p. 2471–2486, dez. 2018. ISSN 1063-6692, 1558-2566. DOI: 10.1109/TNET.2018.2869798.

SHANDWICK, W. In a New Record, IX.br surpasses 31 Tbits of peak. **IX.br**, 2023. Disponível em: <https://ix.br/noticia/releases/in-a-new-record-ix-br-surpasses-31-tbit-s-of-peak-internet-traffic-exchange>. Acesso em: 7 set. 2023.

SIDDIQUI, A. **For 12 Hours, Was Part of Apple Engineering's Network Hijacked by Russia's Rostelecom?** Jul. 2022. Disponível em: <https://www.manrs.org/2022/07/for-12-hours-was-part-of-apple-engineerings-network-hijacked-by-russias-rostelecom/>. Acesso em: 7 set. 2023.

SIERSZEŃ, A. Huawei eNSP environment for e-learning of corporate network configuration and maintenance. In: PROCEEDINGS of 12th International Conference on Education and New Learning Technologies. online: IATED, jul. 2020. P. 7464–7470. ISBN 978-84-09-17979-4. DOI: 10.21125/edulearn.2020.1895.

SPADACCINO, P.; BRUZZESE, S.; CUOMO, F.; LUCIANI, F. Analysis and emulation of BGP hijacking events. In: NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium. [S.l.: s.n.], mai. 2023. P. 1–4. DOI: 10.1109/NOMS56928.2023.10154437.

STUCCHI, M. **Introducing MANRS ROA Stats Tool**. [S.l.: s.n.], jul. 2021. Disponível em: <https://www.manrs.org/2021/07/introducing-manrs-roa-stats-tool/>.

TRIPATHI, N.; SWARNKAR, M.; HUBBALLI, N. DNS spoofing in local networks made easy. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). Bhubaneswar: IEEE, dez. 2017. P. 1–6. DOI: 10.1109/ANTS.2017.8384122.