Alison da Cruz

Identificação de Chamadas Maliciosas em PABX IP

São José – SC

Fevereiro / 2019

Alison da Cruz

Identificação de Chamadas Maliciosas em PABX IP

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador: Prof. Dr. Marcelo Maia Sobral

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC

Fevereiro / 2019

Monografia sob o título "*Identificação de Chamadas Maliciosas em PABX IP*" defendida por Alison da Cruz e aprovada em 19 de fevereiro de 2019, São José, Santa Catarina, pela banca avaliadora assim constituída:

_____

Prof. Marcelo Maia Sobral, Dr.
Orientador

_____

Prof. Ederson Torresini, Me.
IFSC

_____

Prof. Odilson Tadeu Valle, Dr.
IFSC

RESUMO

Inúmeros são os benefícios em se utilizar a telefonia IP, comprovado pelo elevado índice de convergência de telefonia digital e analógica para cenários que utilizam o Voip. Em contrapartida é preciso que haja uma preocupação relacionada com a integridade, confiabilidade e segurança dos ambientes que usam essa tecnologia. Nos últimos anos as tentativas de ataques e invasões aos PABX IP estão se tornando mais frequentes. Os invasores buscam tornar indisponível a infraestrutura existente ou até mesmo utilizá-la para efetuar chamadas, acarretando assim prejuízos para as empresas e operadoras de telefonia IP.

Existe a necessidade de reforçar a segurança dos sistemas de telefonia VOIP para prevenir as tentativas de invasão e ataques. Ações eficazes devem ser tomadas, pois, caso contrário, essas incursões maliciosas podem acarretar prejuízos para as empresas. Para identificar suas causas e propor soluções que previnam os ataques é preciso identificar os padrões utilizados por esses invasores.

Este trabalho caracteriza ataques baseados no protocolo SIP realizados a PABXIP. Os ataques foram classificados por meio da análise de mensagens SIP recebidas por um PABX IP, em que se identificaram sequências de mensagens e informações contidas em seus cabeçalhos. Com base nessa classificação foram propostas contramedidas com objetivo de inibir ou dificultar o acesso ao PABX IP por usuários mal-intencionados.

Palavras-chaves: VoIP. Ataques. Padrões. Segurança.

ABSTRACT

There are countless benefits to using IP telephony, proven by the high convergence rate of digital and analog telephony for scenarios that use VoIP. On the other hand, there must be a concern regarding the integrity, reliability and security of the environments that use this technology. In recent years attempts at IP PBX attacks and intrusions are becoming more common. Invaders seek to make the existing infrastructure unavailable or even use it to make calls, thus causing losses to companies and operators of IP telephony.

There is a need to enhance the security of VOIP phone systems to minimize and prevent attempts at intrusion and attacks. Effective actions must be taken, otherwise such malicious incursions can be harmful to business. To identify its causes and propose solutions that prevent attacks, it is necessary to identify the standards used by these invaders.

This work characterizes attacks based on SIP protocol realized to IP PBX. The types of attacks were classified through the analysis of SIP messages received by an IP PBX, in which message sequences were identified and information contained in header that characterized them. With this information in hand, simulations were carried out to better understand the attack attempts and countermeasures were sought to inhibit or hinder the access of VoIP resources by malicious users.

Keywords: VoIP. Attacks. Standards. Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ATA	Adaptador de Telefone Analógico
DDOS	Distributed Denial of Service
DOS	Denial of Service
DTMF	Dual-Tone Multi-Frequency
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Detection System
MAC	Media Access Control
MITM	Man In The Middle
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NTP	Network Time Protocol
PABX	Private Automatic Branch Exchange
PC	Personal Computer
RFC	Request For Comments
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Security
SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Iniform Resource Identifier
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network

WAN Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

A telefonia tem conectado as pessoas ao redor do mundo por muitos anos. Desde a invenção do telefone foi possível a realização da comunicação entre pessoas que podem estar em cidades ou até mesmo continentes diferentes, isso tudo por meio do tráfego de voz em uma rede de telecomunicações.

Com o avanço exponencial da Internet, as inovações relacionadas a comunicação têm se expandido. A conversação pela Internet, também conhecida como *Voice Over IP* (VoIP), surgiu na década de 1990 e para o usuário final é semelhante ao tradicional serviço telefônico por comutação de circuitos. No entanto, nesse tipo de serviço, os usuários se comunicam por meio do envio de voz codificada em pacotes de dados, que são transportados através de redes IP (FERDOUS; LO CIGNO, 2014).

A telefonia IP oferece diversos benefícios e soluções de baixo custo para os usuários da telefonia, tais como: integração de voz e dados na mesma infraestrutura; mobilidade com a utilização de softphone em um computador ou até mesmo em um celular, entre outras possibilidades. Por essas razões, no decorrer dos anos, cada vez mais empresas substituem seus antigos sistemas de telefonia analógicos ou digitais por um sistema baseado em voz sobre IP.

Porém o VoIP é vulnerável a escutas, o que possibilita tentativas de invasões se sua infraestrutura não for bem protegida. A infraestrutura de uma rede de telefonia VoIP pode ser composta pela rede local, que envolve os cabeamentos estruturados, *switches* e painéis de distribuição. Também fazem parte da infraestrutura da rede VoIP os computadores pessoais ou *notebooks*, que podem ser utilizados para originar chamadas VoIP por meio de um *softphone*. Além disso, existem os telefones IP que também são utilizados para originar e receber chamadas usando essa tecnologia. Integram-se ainda à infraestrutura o PABX IP, que é responsável pela comunicação entre os ramais e também com a rede pública, além dos gateways, que convertem a

sinalização e o canal de voz para a rede IP e também podem se comunicar com a rede pública.

Os ataques ocorrem quando pessoas mal-intencionadas identificam PABX IP acessíveis desde a rede pública. Posteriormente, procuram descobrir credenciais que lhes deem acesso para então usufruir dos recursos disponíveis no PABX, geralmente realizando chamadas para outras cidades ou até mesmo outros países. Atualmente as próprias operadoras buscam orientar os clientes a reforçar a segurança da rede a fim de evitar ou minimizar essas invasões.

1.1 Objetivo geral

O objetivo geral deste trabalho de conclusão de curso é realizar um estudo de padrões anômalos e hostis de mensagens do Protocolo SIP recebidas por um PABX IP.

1.2 Objetivos específicos

Para a realização deste projeto tem-se como seguintes objetivos específicos:

- Classificar padrões de chamadas maliciosas;
- Propor contramedidas para minimizar tentativas de ataques tendo reconhecido os padrões utilizados.

1.3 Proposta de trabalho

A proposta do trabalho em questão é realizar um estudo para identificar padrões anômalos e hostis de mensagens do Protocolo SIP recebidas por um PABX IP. Para isso foram capturadas mensagens SIP de comunicações envolvendo equipamentos reais, os quais sofrem tentativas de invasão no dia a dia. Foram capturados os pacotes recebidos por PABX/Terminal IP que possui acesso à internet. Não foram informados os modelos dos telefones IP e PABX IP utilizados nos testes para não expor fragilidades do fabricante.

Tendo em mão os relatórios de captura (*log*), foi realizada a análise de mensagens SIP para identificar padrões que caracterizem ataques. A ferramenta utilizada para análise foi o *software* gratuito *Wireshark* que possibilita a coleta e especificação de filtros para futura análise de pacotes de tráfego na rede.

Por fim, foram propostas contramedidas com base nos padrões de tentativas de invasões identificados, de forma a minimizar os ataques recebidos nas redes de Telefonia IP.

2 FUNDAMENTAÇÃO TEÓRICA

Esse capítulo tem por objetivo descrever o protocolo SIP, seus métodos e suas respostas. Também são apresentados os principais tipos de ataques maliciosos em redes VoIP.

2.1 Protocolo SIP

O *Session Initiation Protocol* (SIP) é um protocolo que controla a criação, estabelecimento e término de sessões, dessa forma esse protocolo trata-se apenas de tráfego de sinalização. Esse protocolo foi desenvolvido pelo IETF em 1997, e atualmente está em sua segunda versão incorporando diversas melhorias que foram propostas em 2002.

De acordo com Kurose e Ross (2013), o protocolo SIP, definido pela RFC 3261, é um protocolo que possui a finalidade de:

- Prover mecanismos para estabelecer chamadas entre dois interlocutores por uma rede IP, permitindo que a chamada seja encerrada por um destes interlocutores e que os participantes concordem com a codificação da mídia.
- Oferecer mecanismos que permitem a quem chama determinar o endereço IP atual de quem é chamado, já que os usuários não possuem um endereço IP único, pois podem receber endereços dinamicamente da rede, além da possibilidade de ter vários equipamentos IP, cada um com um endereço IP diferente.
- Prover dispositivos de gerenciamento de chamadas, tais como adicionar novos fluxos de mídia, mudar a codificação, convidar mais interlocutores para participar da chamada, além de realizações de transferências.

Junior e Júnior (2017) listam 5 funcionalidades básicas oferecidas pelo protocolo SIP: localização de usuário; verificação de disponibilidade de usuário; descoberta das capacidades ou recursos de um usuário; estabelecimento de parâmetros de uma sessão; e por fim, gerenciamento de uma sessão. Concordando com a afirmativa acima Porter (2006) cita que além de configurar e gerenciar as

sessões, o SIP tem a função de determinar a localização, disponibilidade e compatibilidade entre os agentes usuários envolvidos na comunicação. Os principais componentes da arquitetura SIP são:

- Agente usuário (*User Agent Client*): UAC são os clientes que originam pedidos de conexão e UAS (*User Agent Server)* são servidores que recebem e respondem aos pedidos de conexão. Pode-se citar como agentes usuários equipamentos terminais como ATAs, telefones IP e *softphone*.

- Servidor proxy (*Proxy Server*): atua de forma intermediária, passando adiante requisições para o próximo servidor SIP como se fosse o originador da chamada, e quando a resposta é recebida este redireciona para quem de fato originou a requisição.

- Servidor de redirecionamento (*Redirect Server*): a função do *Redirect Server* é fornecer informações sobre a localização do servidor para que o cliente possa entrar em contato diretamente.

- Servidor de registro (*SIP Registrar):* é um tipo especial de UAS responsável por receber e aceitar pedidos apenas solicitações do tipo REGISTER, além disso armazena informações (como a localização) dos agentes usuários.

Esses componentes descritos acima são apresentados na figura 2.1.

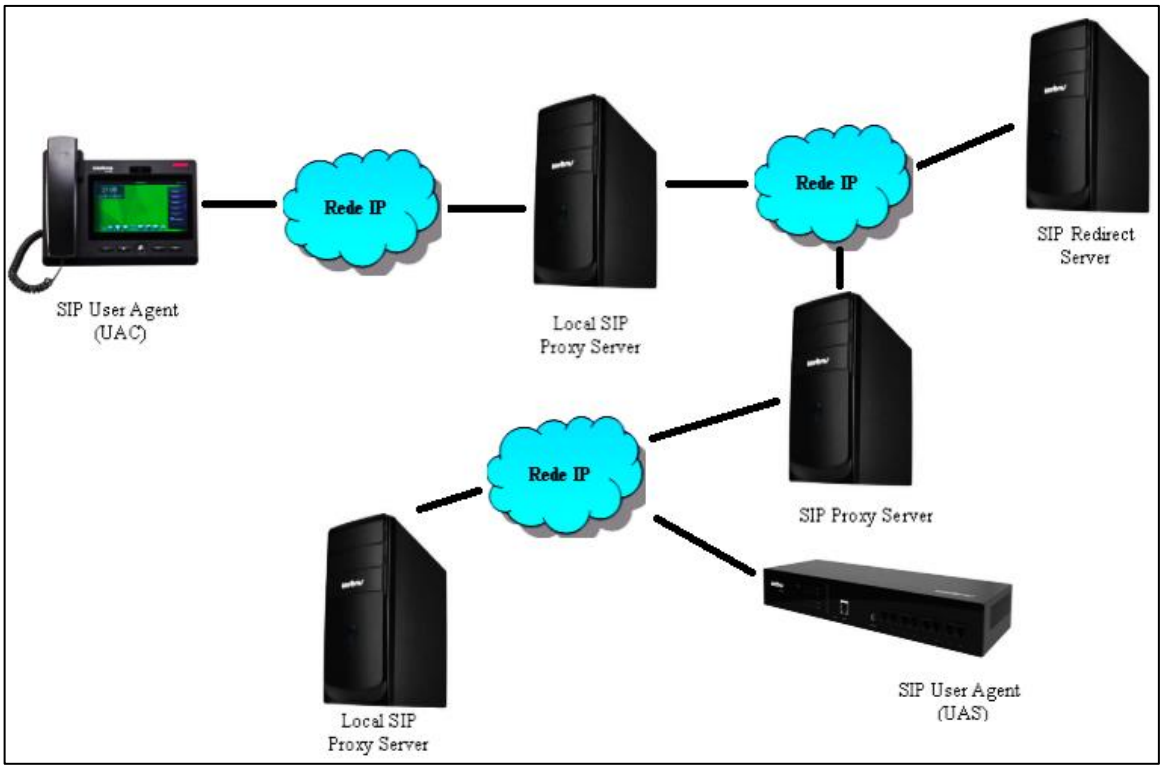


Figura 2.1 - Principais componentes da arquitetura SIP

Fonte: Elaborado pelo autor

2.1.1 Métodos SIP

O SIP se baseia no formato de requisições de texto, semelhante ao HTTP (*Hiper Text Protocol*), segundo a RFC 3261 foram definidos 6 métodos que serão apresentados e descritos resumidamente no quadro a seguir. A Tabela 1 a seguir descreve os principais métodos SIP.

Método SIP	**Descrição**
REGISTER	Usado por um agente para registrar informações de contato.
INVITE	Usado para estabelecer sessões entre dois agentes
ACK	Confirma respostas finais a requisições INVITE
BYE	Termina uma sessão previamente estabelecida
CANCEL	Encerra tentativas de chamadas
OPTIONS	Consulta um agente sobre suas capacidades

Tabela 1 – Métodos SIP
Fonte: WIKI IFSC SJ (2018)

Cada método apresenta uma ação requerida, como será apresentado mais detalhadamente abaixo.

REGISTER: tem o papel de informar a localização do usuário com as informações que o identificam. De acordo com Johnston (2009), a informação relacionada a localização está contida no campo *Contact* do cabeçalho. O servidor compara o SIP URI do campo *To* com o SIP URI do campo *Contact,* que revela a localização do UAC. É esse serviço de localização que é utilizado pelo *proxy* para rotear as chamadas para os usuários. Dependendo do uso dos campos *Contact* e *Expires*, o servidor tomará medidas diferentes. Se o campo *Expires* não for utilizado, o registro do SIP deverá ser cancelado em 3600 segundos, se o *Expires* estiver igual a zero o registro será cancelado imediatamente. O *RequestURI* contém apenas o domínio do servidor registrar (não possui o usuário). O REGISTER pode ser encaminhado por um *proxy* até chegar ao servidor registrar responsável pelo domínio. O campo *To* contém o SIP URI que será registrada no servidor. O campo *From* contém o SIP URI do originador da requisição, recomenda-se que o mesmo Call-ID seja usado para todos os registros de um usuário agente.

A figura 2.2, mostra uma troca de mensagens SIP entre Cliente e Servidor, na qual o cliente faz uma requisição de registro para o Servidor, este por sua vez aceita e o registro é estabelecido.

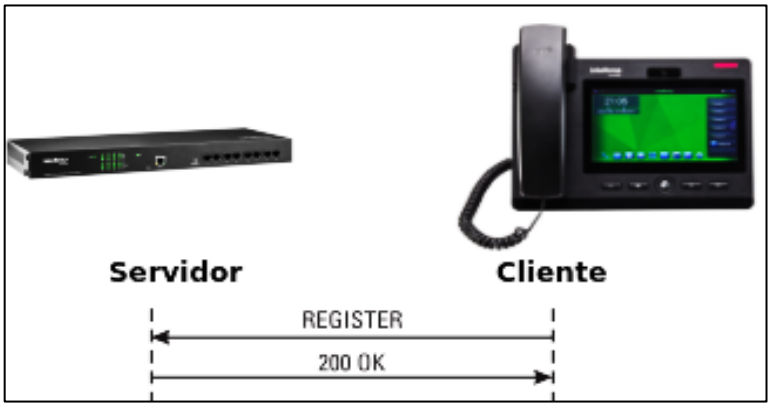


Figura 2.2 - Registro SIP

Fonte: adaptada de Johnston (2009)

No período de tempo de registro configurado no UAC, este enviará novamente uma mensagem REGISTER ao servidor para que essa sessão não seja encerrada e o cliente permaneça registrado. Alguns campos são obrigatórios no cabeçalho

REGISTER: Call-ID, Cseq, From, To, Via e Max-forwards, que podem ser vistos na figura 2.3 abaixo.

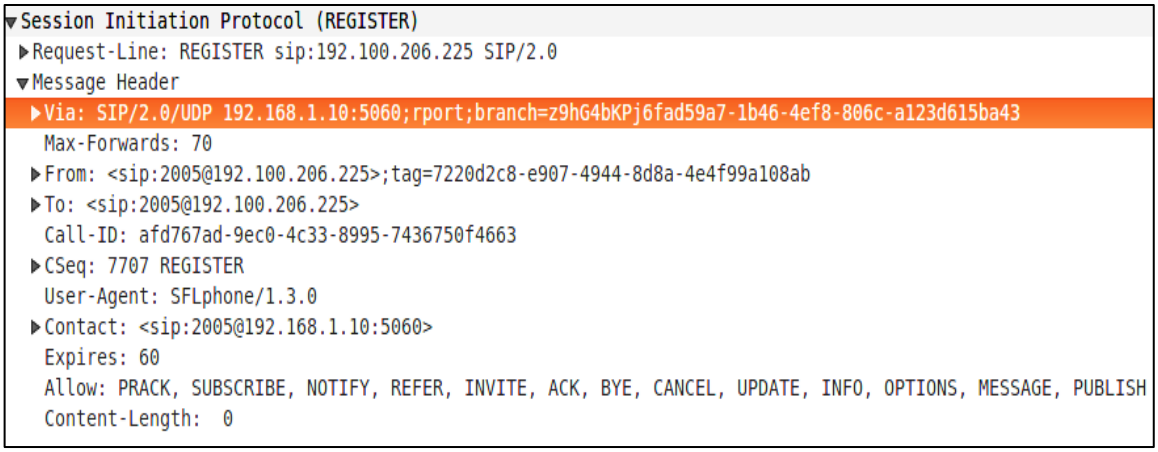


Figura 2.3 - Campos do registro SIP

Fonte: Captura de tela Wireshark

INVITE: o método *INVITE* é usado para estabelecer uma sessão de mídia entre dois agentes usuários. O *INVITE* sempre deve ser confirmado através de uma mensagem ACK. O *INVITE* possui um cabeçalho com a descrição da sessão (via protocolo SDP). Caso a descrição da sessão não seja aceita pelo agente servidor, este deverá enviar um *BYE* para terminar a sessão (JOHNSTON, 2009).

Um exemplo do fluxo do método *INVITE* é apresentado na figura 2.4.

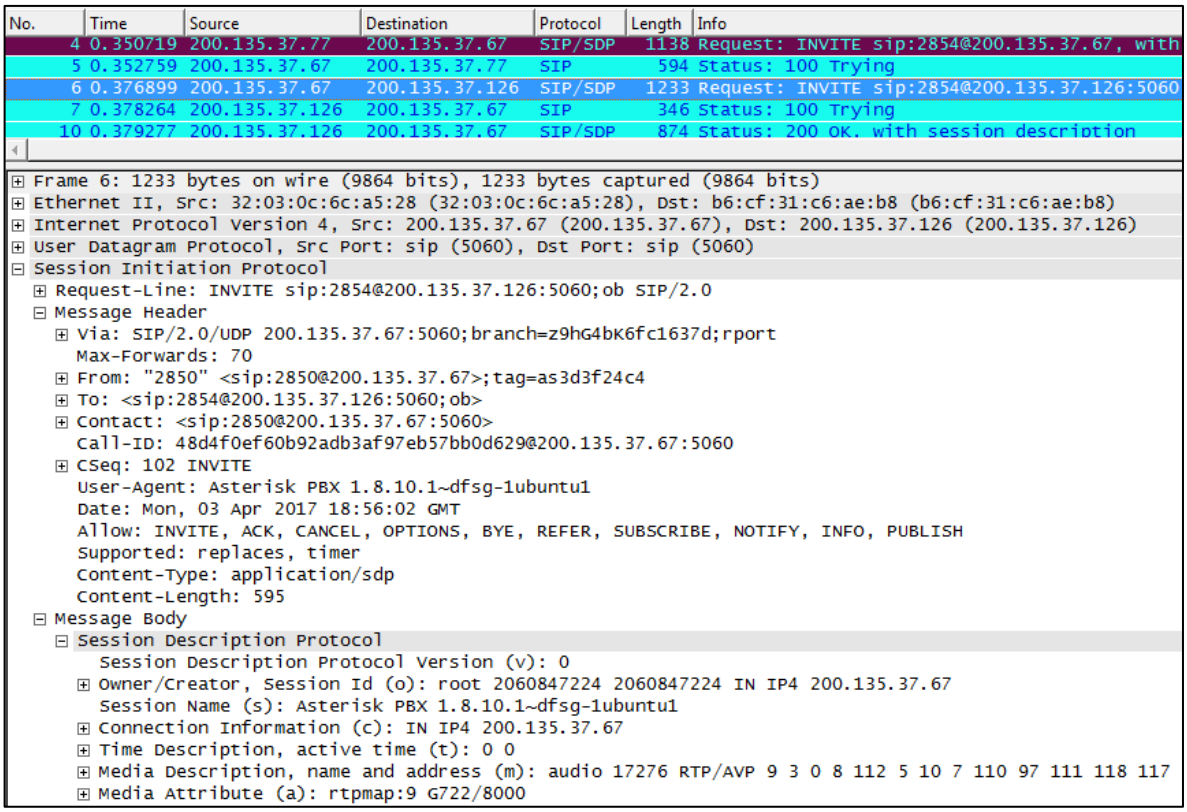


Figura 2.4 - Mensagem *INVITE*

Fonte: Captura de tela Wireshark

Ainda segundo Johnston (2009), o agente cliente (UAC) que gera o *INVITE* para estabelecer um diálogo gera juntamente um identificador chamado de Call-ID que é usado durante toda a sessão. O campo CSeq do cabeçalho é usado para numerar em ordem das mensagens. Os campos *From* e *To* servem para identificar o usuário chamador e usuário chamado. No campo *From* do *INVITE* é adicionado um parâmetro *tag* pelo UAC e no campo *To* das respostas é adicionado um parâmetro *tag* pelo agente servidor (UAS). A *tag* do campo *To* da mensagem 200 OK em resposta ao INVITE é usada no cabeçalho *To* da mensagem ACK e em todas as mensagens seguintes do diálogo. A combinação das tags do *To* e *From* e Call-ID formam um identificador único para esse diálogo. O campo Via é usado para gravar o caminho da requisição. Depois ele é usado para rotear as respostas exatamente pelo mesmo caminho no sentido inverso. Uma mensagem *INVITE* enviada em um diálogo já existente é chamado de *re-INVITE* e é usado para mudar alguma característica da mídia utilizada naquela sessão. Caso o *re-INVITE* não seja aceito, a sessão continua como antes.

ACK: segundo a RFC 3261 a mensagem *ACK* confirma que o cliente recebeu uma resposta final para uma requisição de *INVITE*. O método *ACK* funciona como a confirmação de um *INVITE*, se *o INVITE* não tiver a descrição da sessão, o *ACK* deverá possuir. O Cseq nunca é incrementado quando se envia um *ACK*, de modo que o usuário/servidor possa relacionar com o *INVITE* correspondente. A figura 2.5 abaixo mostra um exemplo de uma mensagem ACK.

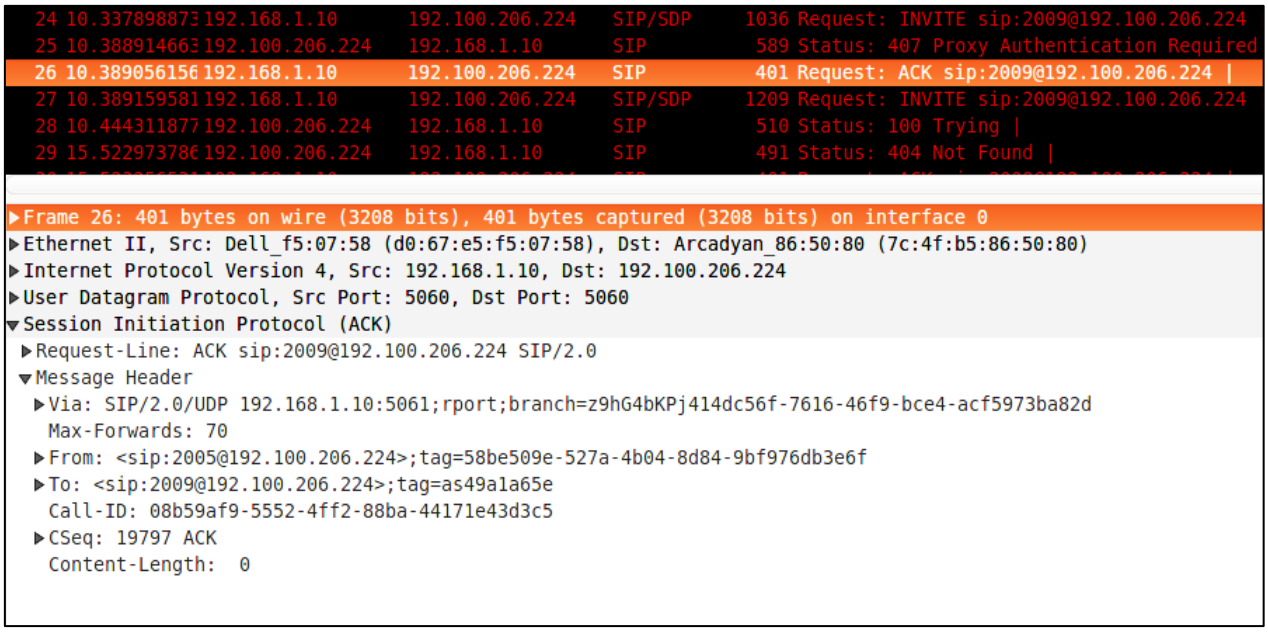


Figura 2.5 - Mensagem ACK

Fonte: Captura de tela Wireshark

Os campos de cabeçalho obrigatórios do método *ACK* são os mesmos da requisição *REGISTER.*

*BYE: c*onforme descrito na RFC 3261, o método específico para a finalização de um diálogo é o método *BYE*. Um usuário agente (UA) não deve enviar um *BYE* fora de um diálogo e quando o *BYE* é recebido dentro de uma sessão, esta deve ser encerrada. Ainda segundo a RFC 3261, quando um dos pontos envia um *BYE* essa sessão não deverá ser finalizada até que o outro ponto confirme com um ACK. A figura 2.6 demonstra a sinalização da mensagem *BYE*.

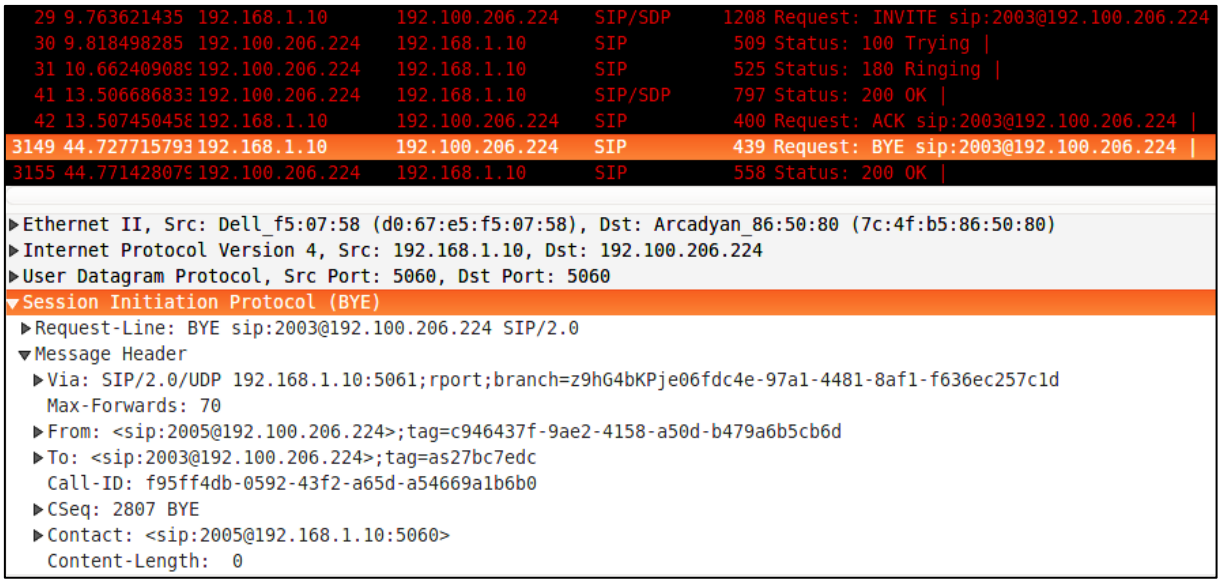


Figura 2.6 - Mensagem BYE

Fonte: Captura de tela Wireshark

A requisição *BYE* só pode ser enviada por UAs que participam da sessão e nunca por servidores proxies, ou seja, é um método fim-a-fim (JOHNSTON, 2009).

CANCEL: o método *CANCEL* é usado para encerrar sessões que ainda não foram estabelecidas ou, conforme a RFC 3261, cancela pedidos enviados que não obtiveram respostas dentro do tempo estabelecido. Um cliente ou servidor confirma o cancelamento através de uma mensagem 200 OK e responde com uma mensagem 487 *Request Terminated*, conforme figura 2.7 a seguir.

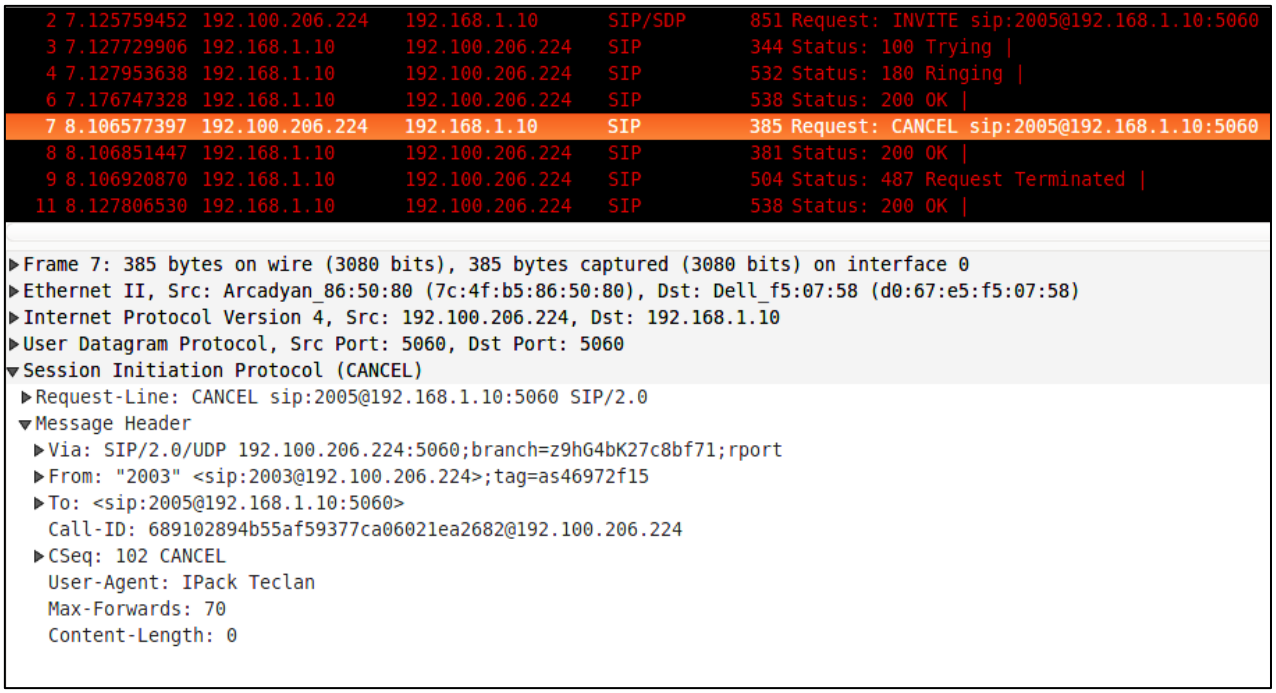


Figura 2.7 - Mensagem CANCEL

Fonte: Captura de tela Wireshark

Diferentemente do método *BYE*, o método *CANCEL* pode ser enviado tanto por UA's quanto por servidores *proxies*. Quando um *proxy* recebe uma mensagem *CANCEL* repassa essa para os mesmos *hops* de onde as mensagens *INVITE* pendentes foram encaminhadas.

OPTIONS: segundo Johnston (2009), o método *OPTIONS* é usado para questionar um usuário cliente ou servidor sobre sua disponibilidade ou capacidades. Faz uma pergunta sobre quais métodos e extensões são suportados pelo servidor e pelo usuário descrito no campo de cabeçalho. Tanenbaum (2003) descreve que geralmente o *OPTIONS* é usado antes da sessão ser iniciada, com o intuito de descobrir se a máquina suporta os recursos solicitados, a resposta contém uma listagem com métodos, extensões e *codecs* suportados. A figura 2.8 abaixo exemplifica esse método.

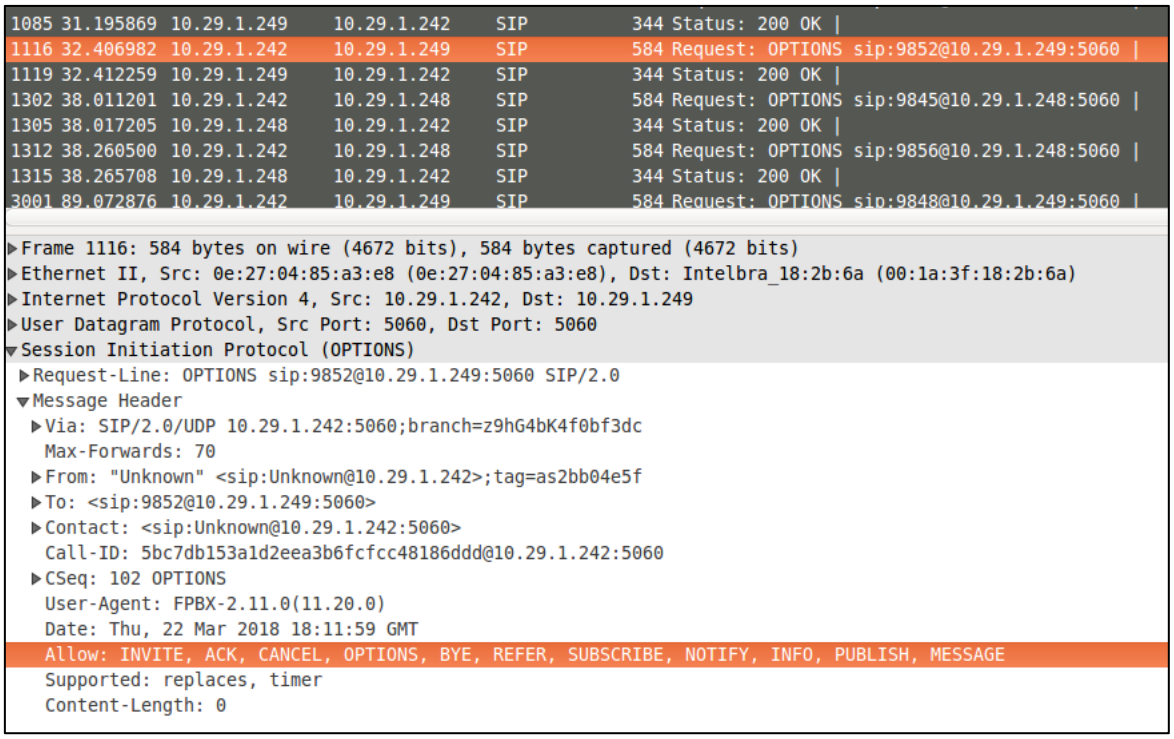


Figura 2.8 - Mensagem OPTIONS

Fonte: Captura de tela Wireshark

Os campos de cabeçalho *Allow, Accept, Accept-Encoding, AcceptLanguage* e *Supported* devem estar na mensagem *200 OK* em resposta ao *OPTIONS*.

2.1.2 Respostas SIP

De acordo com Johnston (2009), as respostas SIP geralmente são geradas por um UAS que responde a uma requisição feita por um AUC. Existem seis classes de respostas SIP que são descritas na tabela 2, junto de alguns exemplos de respostas.

Classe	**Descrição**	**Ação**
1xx	Informativo	Indica que a requisição foi recebida e que o estabelecimento da sessão está em curso. Este tipo de mensagem é fim-a-fim. 100 – Tentando 180 – Ringando 182 – Chamada colocada na fila
2xx	Bem-sucedido	Indica que a requisição foi recebida, processada e bem-sucedida. 200 – OK

3xx	Redirecionado	Indica que uma ação mais adiante precisa ser tomada para que a requisição possa ser completada, isto é, uma nova requisição deve ser gerada pelo UAC ou proxy para o(s) endereço(s) contido(s) no cabeçalho *Contact* da resposta. 300 – Múltiplas escolhas 301 – Movido temporariamente 380 – Serviço alternativo
4xx	Erro do Cliente	Indica que não foi possível executar a requisição pelo servidor do modo que foi recebida. A resposta específica do erro do cliente ou a presença de certo tipo de campo de cabeçalho deve indicar ao UAC a razão do erro e como a requisição deve ser corrigida antes de ser enviada novamente. 400 – Pedido inválido 401 – Não autorizado 403 – Proibido 404 – Não encontrado 407 – Necessária autenticação de *proxy* 408 – Tempo de pedido esgotado 480 – Temporariamente indisponível
5xx	Erro do Servidor	Indicam a incapacidade do servidor em executar uma requisição. 500 – Erro interno no servidor 502 – *Gateway* inválido 505 – Versão SIP não suportada
6xx	Falha Global	Indica que a requisição falhou. A requisição não pode ser atendida por este ou outro servidor. 603 – Declínio 604 – Não existe em nenhum lugar 606 – Não aceitável

Tabela 2 – Respostas SIP

Fonte: Adaptado de Johnston (2009)

2.2 Ataques maliciosos em redes VoIP

Os ataques têm por objetivo comprometer, de forma unitária ou conjunta, os três aspectos relacionados à segurança da informação: confiabilidade, integridade e disponibilidade (SANTOS, 2012). A confiabilidade está relacionada com a privacidade, se dá garantindo que apenas a origem e o destino tenham conhecimento do conteúdo da mensagem, ou seja, que essa informação não possa ser interceptada por partes

não autorizadas (GOMES, 2004). A integridade garante que as mensagens não sofreram alterações ao longo do caminho, ou seja, que foi preservada em sua íntegra. E por fim, a disponibilidade deve garantir que as informações e recursos estejam disponíveis para os legítimos usuários.

Da mesma forma que já acontecia nas redes de computadores, com o surgimento do VoIP surgiram também ameaças que tem como intuito comprometer a integridade, a confiabilidade ou a disponibilidade das redes baseadas em SIP. No que se refere a riscos, a própria RFC do SIP (3261) o descreve como um protocolo em que não é fácil implementar segurança. Segundo Cooney (2016), os ataques cibernéticos que utilizam o protocolo SIP têm crescido e representam mais de 51% das falhas de segurança analisadas no ano de 2016.

A seguir são apresentadas as formas mais comuns de tentativas de ataques a redes VoIP.

2.2.1 *Denial of Service* (DoS)

O ataque do tipo DoS tem por objetivo esgotar os recursos disponíveis de determinado servidor, para que os verdadeiros usuários não possam utilizá-los. Não se trata de uma invasão propriamente dita, mas sim de provocar uma indisponibilidade do serviço prestado. De acordo com Thermos e Takanen (2007), em cenários VoIP o ataque pode ser direcionado tanto para os servidores quanto para a rede em si.

Para exemplificar esse tipo de ataque pode-se citar um servidor que consiga processar 10 requisições por segundo, mas que passa a receber 30 requisições por segundo. Esse servidor pode parar de responder pelo fato de estar sobrecarregado além dos limites disponíveis. Dessa forma esse tipo de ataque objetiva comprometer a disponibilidade do serviço prestado. A figura 2.9 demonstra o PABX recebendo um ataque DoS.

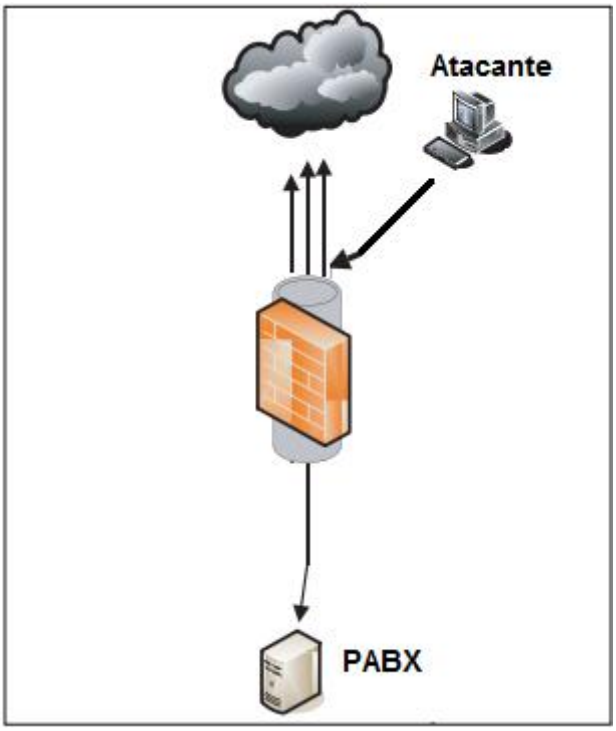


Figura 2.9 - Ataque DoS
Fonte: Adaptado de Porter (2006)

2.2.2 Distributed Denial of Service (DDoS)

O ataque de negação de serviço distribuído (DDoS) opera semelhante ao DoS e o que difere é que a origem dos ataques não é um único ponto, e sim de dezenas, ou até centenas de computadores conectados com a internet, com o intuito de alcançar o mesmo alvo e afetar sua disponibilidade. Furlan e Santos (2017) ressaltam que o impacto causado por estes ataques na maior parte das vezes se traduz em perda financeira, pois os serviços prestados pela instituição atingida não poderão ser acessados por seus usuários, podendo vir até mesmo prejudicar a imagem e a credibilidade desta instituição, uma vez que os reflexos do ataque na sua operação serão a lentidão de acesso aos recursos ou até mesmo a indisponibilidade total da infraestrutura.

A figura 2.10 demonstra que no ataque DDoS a origem é mais de uma máquina.

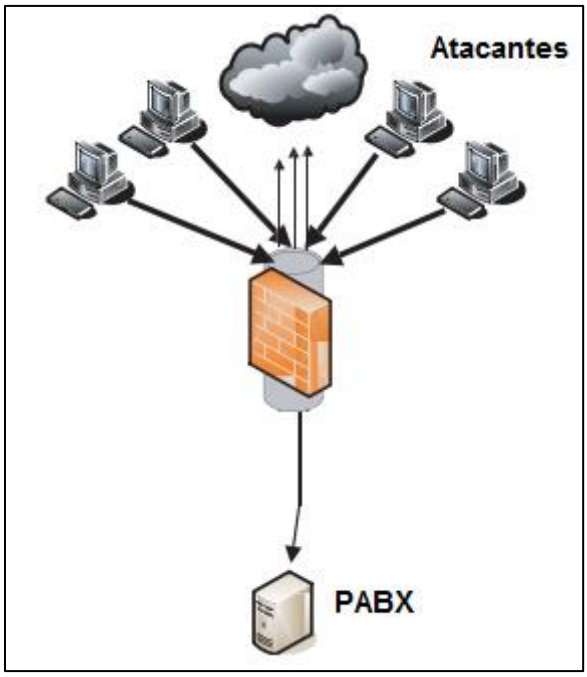


Figura 2.10 - Ataque DDoS
Fonte: Adaptado de Porter (2006)

2.2.3 SIP Flood

De acordo com Furlan e Santos (2017) em um ataque SIP *Flood* o atacante sobrecarrega o servidor *proxy* SIP com inúmeros pacotes *INVITE*. Como mencionado no item 2.1, o servidor proxy é responsável pelo processamento de todas as chamadas entre os sistemas finais e a mensagem INVITE. O grande volume de requisições a esse *proxy* causará a deterioração da rede, impossibilitando o atendimento de requisições válidas e, consequentemente, tornando o serviço indisponível. A grande maioria dos ataques utiliza a técnica de IP *Spoofing*, onde o endereço de origem das conexões é alterado para endereços inválidos fazendo com que as respostas nunca alcancem seus destinos.

2.2.4 *VoIP Packet Replay Attack*

Consiste na captura e reenvio pacotes VoIP fora de ordem para os equipamentos finais gerando assim atraso nas chamadas em curso e degradando a qualidade das ligações (Porter 2006).

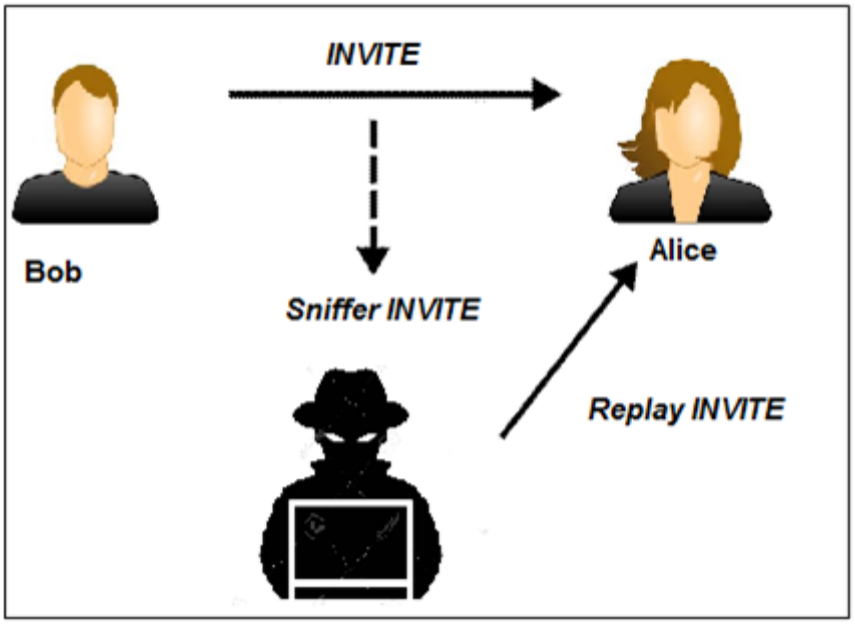


Figura 2.11 – Ataque *VoIP Packet Replay*

Fonte: Elaborada pelo autor

2.2.5 *SIP Sinalling Loop*

Segundo Thermos (2007, *apud* Antoniazzi, 2008, p.28) esse tipo de ataque afeta cenários que não possuem mecanismos de detecção de *looping*. Esse ataque resume-se a registrar dois usuários em domínios diferentes, de forma que quando o servidor proxy receber mensagens *INVITE* provindas desse ataque, acontecerá a duplicidade das mensagens nos domínios. Dentro do contato de cada registro existem dois valores, cada um direcionado para um domínio. Quando o *proxy* de um domínio recebe o *INVITE* para um desses usuários, ele irá gerar duas mensagens de *INVITE* uma para cada usuário no outro domínio. Já o SIP *Proxy* do outro domínio por sua vez, ao receber esses dois *INVITES* irá gerar quatro novas mensagens de *INVITE* para o outro domínio. Assim, as mensagens crescerão em ordem de potência, conforme a figura 2.11 abaixo, podendo assim comprometer a disponibilidade do sistema SIP.

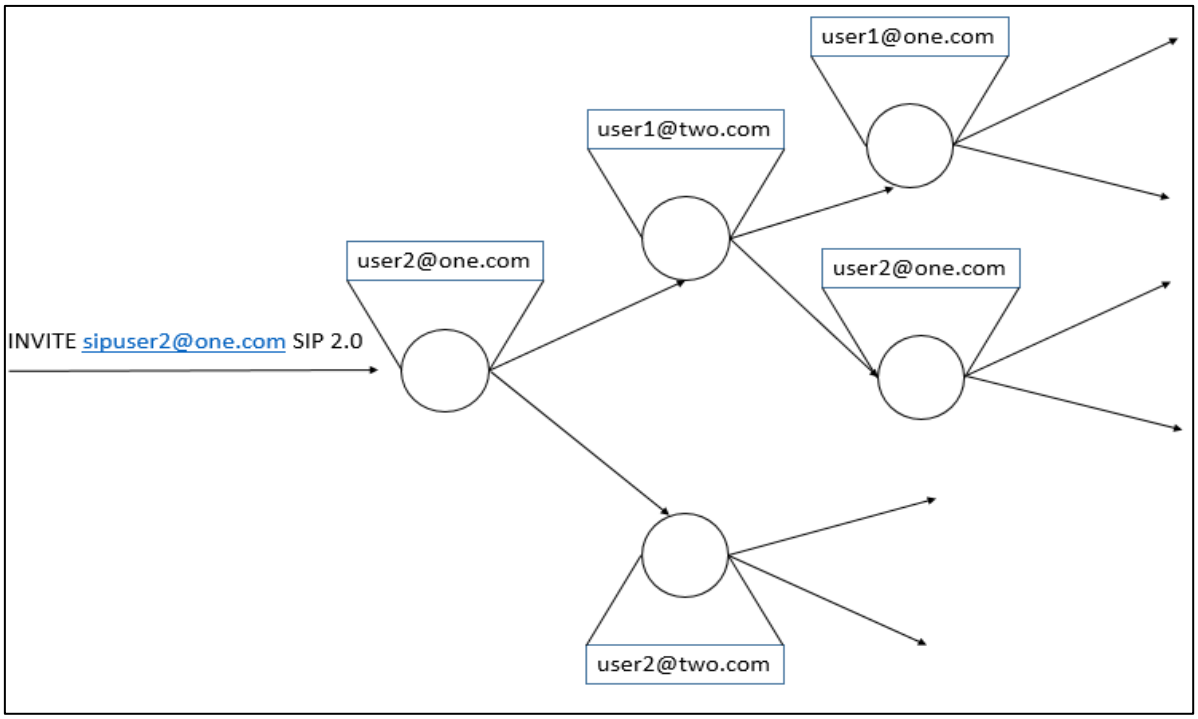


Figura 2.112 - SIP Sinalling Loop

Fonte: Adaptado de Thermos (2007)

2.2.6 *Man in the Midlle* (MITM)

Neste tipo de ataque, o invasor pode utilizar duas técnicas: clonagem do DNS, ou envenenamento da tabela ARP. Contudo, no caso da tabela ARP, só será possível se o invasor estiver fisicamente em um segmento de rede entre UAC e UAS. Dessa maneira, o interceptador não precisa obrigatoriamente conhecer usuários e senhas válidos; basta intermediar o tráfego entre servidor e cliente e agir interceptando os pacotes, impedindo assim de chegar ao seu verdadeiro destino, que é o servidor SIP. Para parecer ao cliente que a requisição de autenticação foi aceita pelo servidor, o atacante envia mensagens de sucesso a quem originou a requisição (NAKAMURA, 2007). Com posse dos pacotes trocados entre o UAC e UAS, o invasor pode decodificar o áudio e usar as informações para benefício próprio.

A figura 2.13 exemplifica um ataque do tipo MITM.

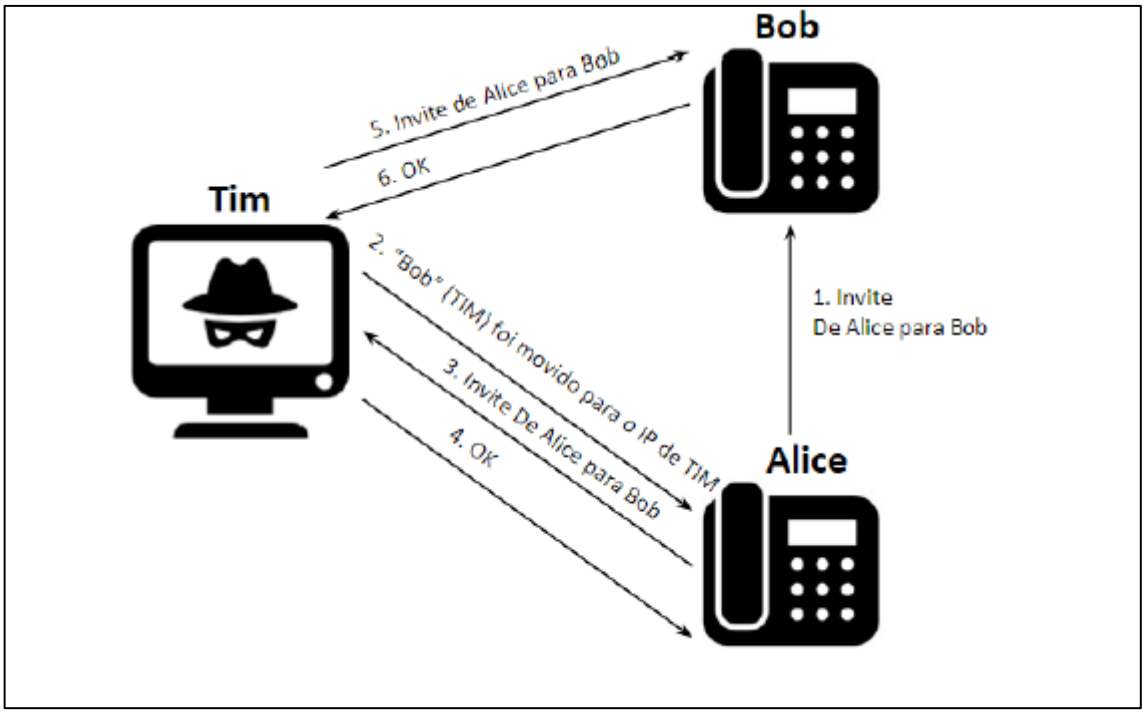


Figura 2.13 - Ataque MITM

Fonte: Nomoto e Ferreira (2016)

1. Alice envia uma mensagem *INVITE* para o Bob e esta mensagem é detectada por Tim.
2. Tim envia uma resposta para Alice com a mensagem 301 *Moved Permanently* e informa o seu próprio endereço como sendo o novo endereço IP de Bob.
3. Alice envia uma nova mensagem *INVITE* acreditando estar enviando para Bob, porém está enviando para Tim.
4. Tim responde com uma mensagem de reconhecimento *ACK* para estabelecer uma conexão entre ele e Alice.
5. Ao mesmo tempo, Tim envia uma mensagem *INVITE* para Bob como se fosse Alice.
6. Tim responde com 200 OK e a conexão entre Bob e Tim é estabelecida.

Após utilizar essa técnica de ataque, o invasor interceptou uma chamada válida do usuário e se apropriou dela após a autenticação.

2.2.7 *Registration Hijack*

O ataque *registration Hijack* ocorre quando um invasor altera a identidade de um usuário legítimo para o seu próprio endereço, dessa forma as chamadas serão encaminhadas para o atacante ao invés de serem direcionadas para o dispositivo do verdadeiro usuário. De acordo com Porter (2006), a alteração do campo *Contact* no cabeçalho SIP é feita da seguinte forma: o invasor envia uma requisição de registro semelhante à capturada em um pacote do usuário verdadeiro, porém com o campo de *IP address* de origem modificado para o seu próprio IP.

Nomoto e Ferreira (2016) descrevem detalhadamente como acontece esse tipo de ataque. No exemplo dos autores citados, Alice deseja registrar-se no servidor REGISTRAR usando protocolo SIP. A mensagem *REGISTER*, que é utilizada para este fim, é demonstrada a seguir:

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.77:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

Nesta mensagem, os campos *To* e *From* possuem a mesma informação que identifica o originador do pedido de registro através de um URI *(Uniform Resource Identifier*), que é um identificador único. O campo *Contact* contém a SIP URI que representa o seu endereço IP associado. O invasor pode construir uma mensagem REGISTER similar modificando o campo *Contact,* conforme exemplo abaixo.

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.88:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

Neste modelo, o endereço IP é modificado de 192.168.1.77 para 192.168.1.88, sendo assim, o invasor se registrará aparentemente como um usuário válido, qualquer chamada encaminhada para Alice será direcionada para o IP do invasor mal-intencionado, consequentemente Alice ficará impossibilitada de originar ou receber ligações. Souto (2008) afirma que esse tipo de ataque geralmente acaba evoluindo para um ataque do tipo MITM.

2.2.8 Quebra de senha - Ataque por dicionário

Nesse cenário o interceptador pode, através de captura de pacotes de sinalização SIP, descobrir o usuário SIP e então listar prováveis senhas (baseadas em um dicionário). Em posse dessas informações são disparadas diversas requisições *REGISTER* (ataque de força bruta) para o servidor com as possíveis senhas, até que uma funcione. Descoberta a senha, o invasor pode usufruir dos recursos disponíveis no sistema, por isso a importância de não utilizar senhas simples nos ramais e impor intervalo mínimo entre tentativas de registro, além de limite de tentativas falhas de registro.

2.2.9 *Call Eavesdropping*

Nesse método de ataque a confiabilidade é posta em risco pois nesse cenário é monitorado tanto a sinalização SIP quanto o fluxo de mídia (conversação). Através da sinalização o atacante pode descobrir usuários, senhas, contas e através da escuta da conversação pode ter acesso às informações confidenciais. O *eavesdropping* precisa ser realizado em uma rede por onde passem as mensagens da chamada, esse ataque é eficaz quando os pacotes SIP e RTP trafegam na rede sem nenhum método de proteção das informações. Para capturar a sinalização e a mídia os interceptadores utilizam de *softwares sniffers* de rede, Souto (2008) cita as seguintes ferramentas: Wireshark, Cain e Abel, Vomit, Voipong, Oreka e DTMF *decoder.*

3 IDENTIFICAÇÃO DE ATAQUES EM PABX IP

Para o desenvolvimento do trabalho em questão foram realizadas capturas de pacotes com o *software Wireshark* e analisado em 2 cenários reais com distintos fabricantes de PABX IP. Durante os primeiros testes foram expostos estes PABX IP para a internet sem qualquer tipo de proteção, na sequência foram testadas a eficácia de algumas contramedidas que visam reforçar a segurança do ambiente VoIP. Existem sites que têm por objetivo disponibilizar para consulta pública uma base de dados contendo endereços de IPs comumente conhecidos por se tratarem de tentativas de invasão. No decorrer dos testes realizados, foram consultadas essas páginas para confirmar que o pacote recebido trata-se de um ataque. Cada cenário de teste possui um IP externo (válido para Internet) diferente, o que proporcionou o recebimento e análise de pacotes distintos.

No cenário 1 o PABX IP possui o endereço IP 10.200.1.115, sua porta SIP está definida como 5060. No roteador, devido ao uso de NAT, foi configurada uma regra para redirecionar todos os pacotes provenientes da rede externa para o IP do PABX. Seu endereço IP externo é o 192.100.206.225, conforme apresentado na figura 3.1.

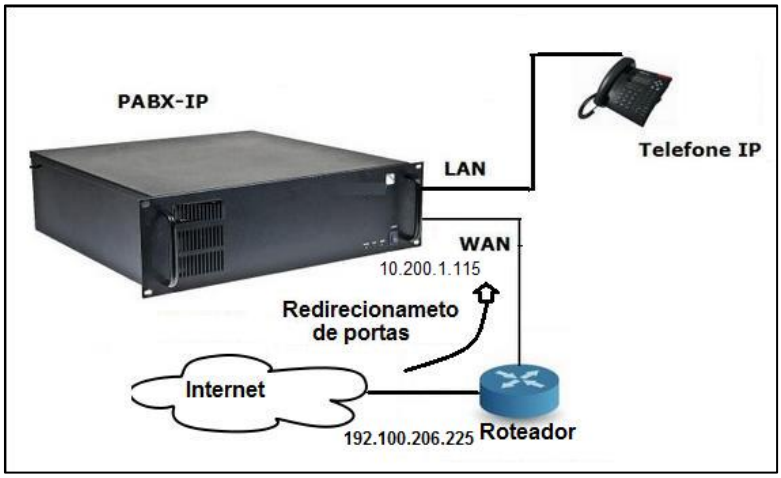


Figura 3.1 – Cenário 1

Fonte: Elaborado pelo autor

Já no cenário 2 o PABX IP está configurado com a porta SIP 5060 e possui o endereço interno 10.200.1.114, além de também utilizar NAT. Quaisquer pacotes destinados ao IP público da rede são redirecionados ao PABX IP. Conforme apresentado na figura 3.2, seu endereço IP externo é o 192.100.206.224.

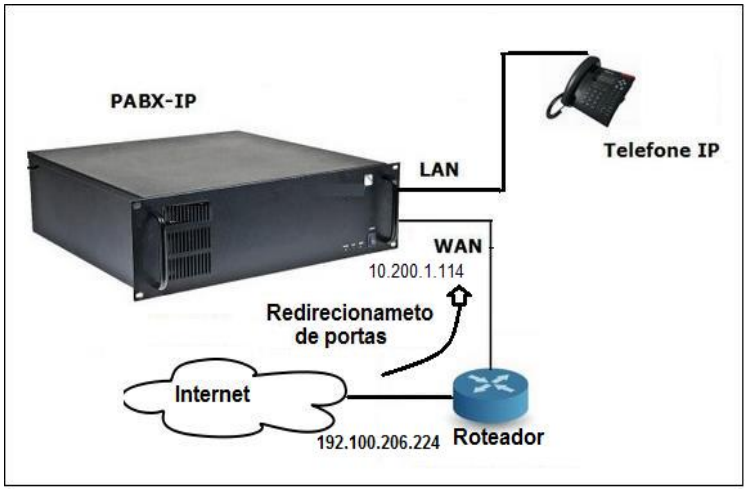


Figura 3.2 – Cenário 2

Fonte: Elaborado pelo autor

Os ataques destinados a equipamentos VoIP acarretam diversos tipos de prejuízos para o usuário final, empresas, operadoras e até mesmo para o fabricante do equipamento. Através de um *port scanner* [1] feito dentro de uma determinada faixa de rede, um equipamento VoIP pode ser identificado com o objetivo de monitorar a troca de sinalizações SIP. Durante esse monitoramento o invasor busca primeiramente coletar informações como *hosts*, *usernames* e numeração das extensões.

Também foi utilizado o programa SIPVicious para auxílio nos testes, descrito no decorrer do trabalho. Não foram informados os modelos e fabricantes dos PABX utilizados para não expor suas fragilidades.

3.1 Cenário 1

Nos testes que serão apresentados a seguir, foi realizada a captura de pacotes trafegados na interface de rede WAN do PABX, a qual possui acesso à rede externa

[1] *Port Scanner:* aplicação com o intuito de rastrear/identificar possíveis portas abertas.

(Internet) e está atrás de NAT. Poucos minutos após o início na captura, notaram-se pacotes provenientes de diferentes endereços externos. O primeiro pacote foi enviado pelo endereço 185.53.91.68 com destino a porta 3060, se trata de um pacote SIP com o método *OPTIONS*. Como esta porta não está disponível, o PABX não recebe a mensagem. Na sequência são enviadas novas mensagens OPTIONS através do mesmo endereço IP de origem com destino as portas 5080 e 5070. Novamente, o PABX não recebe as mensagens, já que estas não foram destinadas a porta 5060.

Conforme apresentado na seção 2.1 deste trabalho, esse tipo de pacote possui o objetivo de verificar quais métodos e extensões são suportadas pelo servidor (PABX). O fato de não ter sido configurado nenhum ramal na rede externa da central e dentro do cabeçalho SIP conter informações nos campos *User-Agent* e *From* totalmente desconhecidas, indicam que pode tratar-se de um usuário mal-intencionado. O PABX IP não está sendo atacado no momento, mas essa tentativa de varredura dá indícios que ataques podem ser recebidos na sequência.

Como mostra a figura 3.3 o campo *From* é apresentado como sipvicous e no *User-Agent* como *friendly-scanner*.

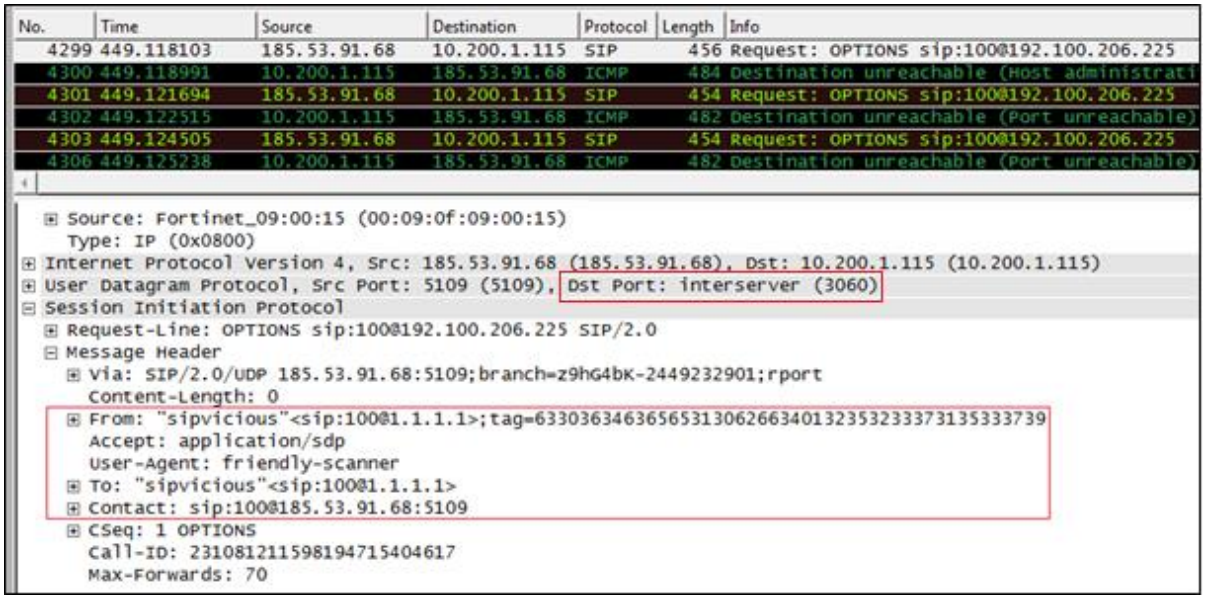


Figura 3.3 - Pacote OPTIONS (cenário 1)

Fonte: Captura de tela Wireshark

Um outro pacote TCP que o PABX recebeu, foi endereçado a porta 443 (HTTPS), o intuito é acessar a interface web de configuração do PABX. Caso o invasor tivesse sucesso nesse ataque, ele poderia ter acesso a senha dos ramais, entre outras

funções do PABX, podendo assim utilizar dessas informações para benefício próprio. A figura 3.4 mostra esse pacote sendo recebido.

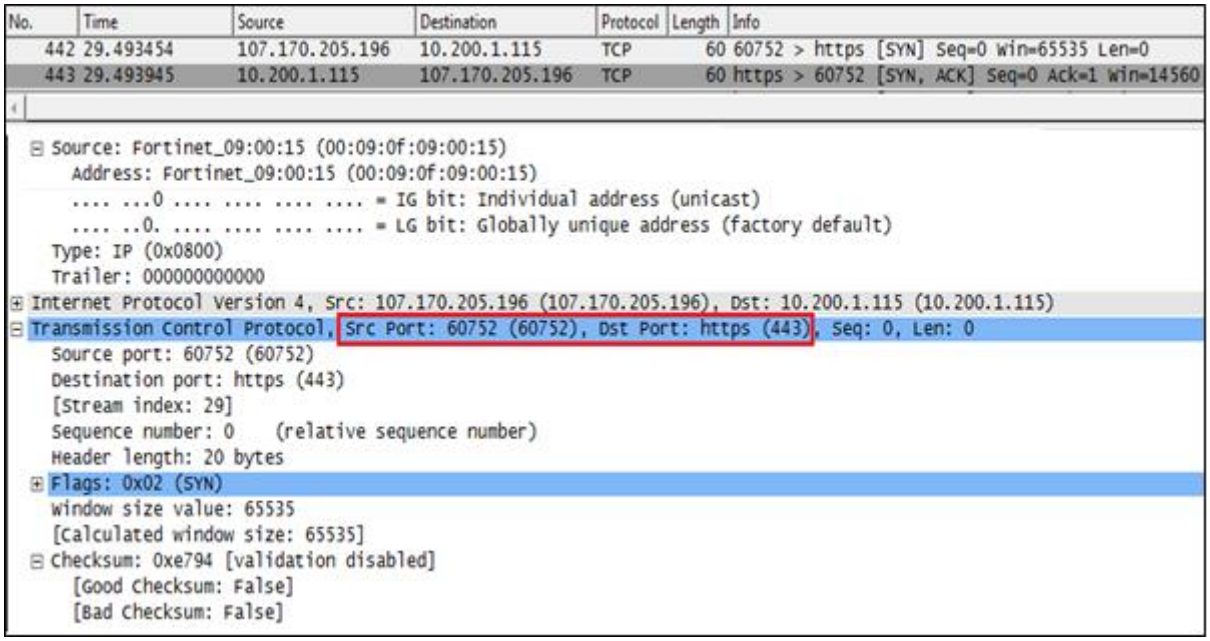


Figura 3.4 – Porta 443 TCP

Fonte: Captura de tela Wireshark

Nesse novo pacote, o atacante tenta acessar o PABX IP via *telnet* (porta 23), sem sucesso. O objetivo é acessar remotamente as configurações para poder utilizá-lo para benefício próprio, conforme a figura 3.5.

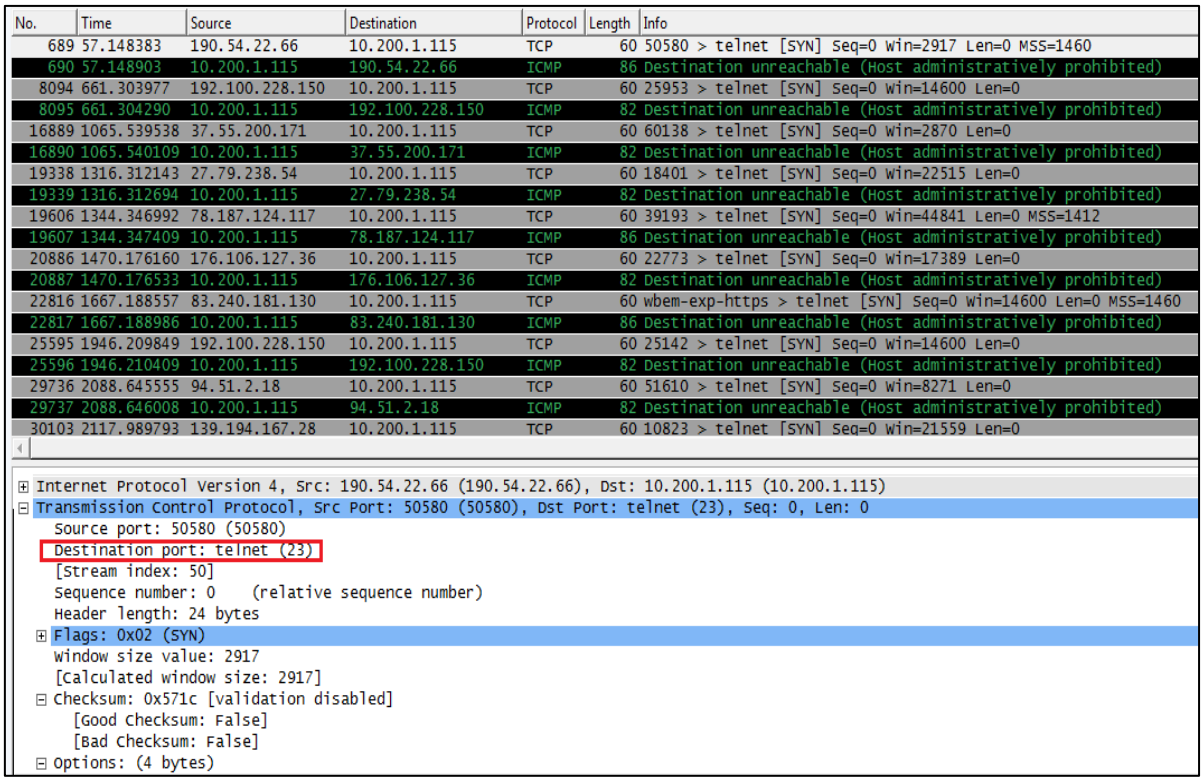


Figura 3.5 – Porta 23 TCP

Fonte: Captura de tela Wireshark

Já na figura 3.6, ocorre uma tentativa de acessar a porta TCP 1433 do dispositivo, a intenção é de ingressar no banco de dados da central. O *Wireshark* automaticamente informa no campo Info que se trata de um acesso ao SQL Server.

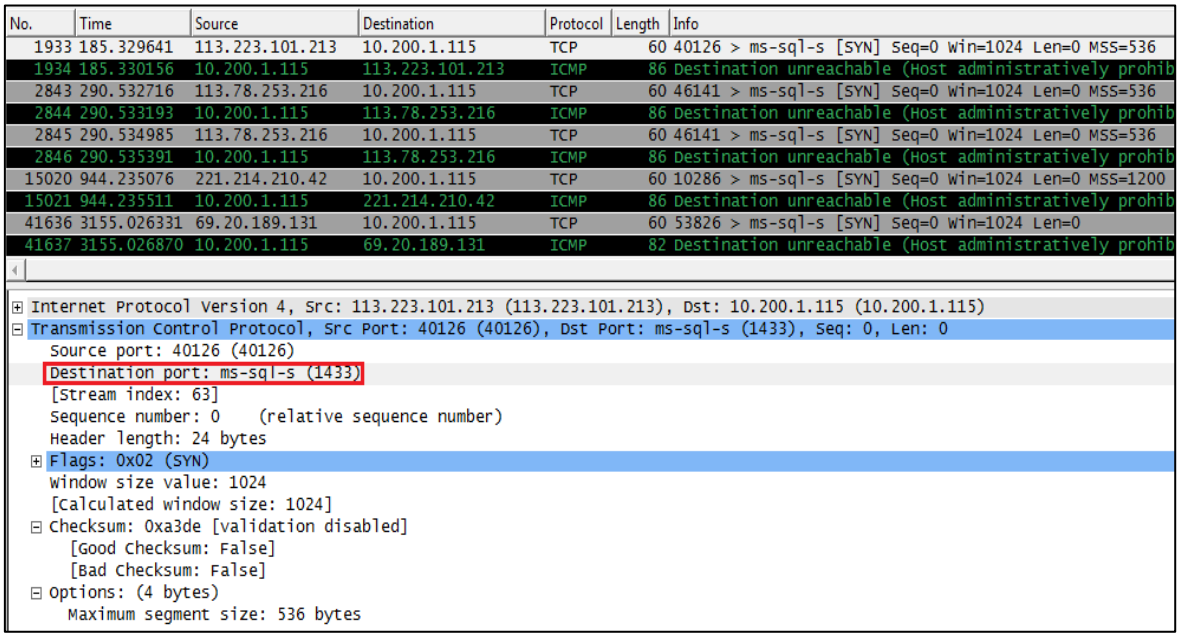


Figura 3.6 – Porta 1433 TCP

Fonte: Captura de tela Wireshark

As capturas expostas anteriormente mostram que os invasores não tentam ingressar ao PABX através apenas da porta 5060, há tentativas de acesso via Telnet, HTTPS e via SQL. Ao realizar a consulta dos endereços 185.53.91.68, 107.170.205.196, 190.54.22.66 e 113.223.101.213 na página VoipBl, todos foram apresentados como endereços já conhecidos por realizar ataques. A figura 3.7 demonstra o resultado após a consulta do endereço 190.54.22.66.

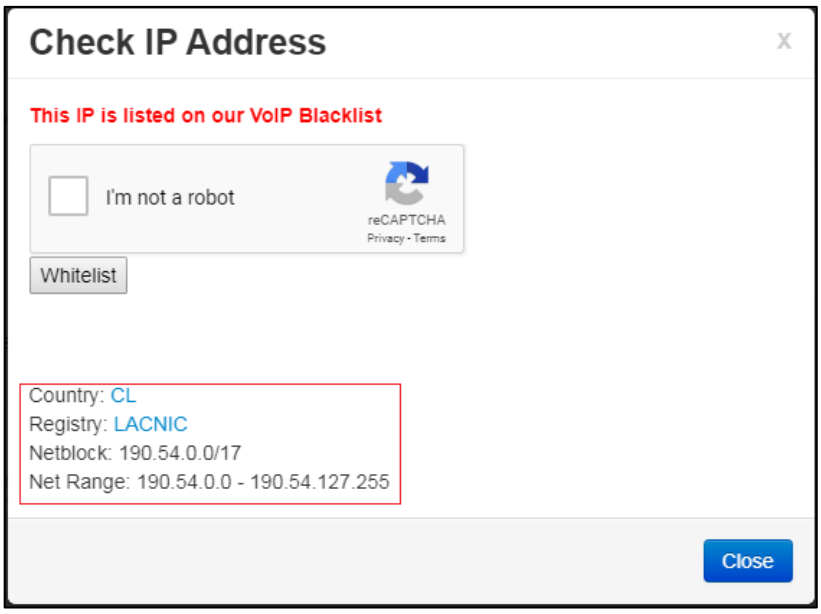


Figura 3.7 – VoipBl

Fonte: VoipBl

3.2 Cenário 2

Nesse segundo ambiente de testes, foram realizadas capturas de pacotes durante três semanas, utilizando um modelo de PABX diferente do cenário anterior. Após a coleta dos logs e análise minuciosa, os itens mais relevantes foram descritos abaixo.

No monitoramento realizado das 10h30 até às 12h40 do mesmo dia, foram recebidos 1377 INVITES, ao analisar estes pacotes foi possível identificar que eles eram oriundos de endereços IP desconhecidos pelo PABX e eram tentativas de chamadas destinadas a números internacionais, conforme apresentado na figura 3.8.

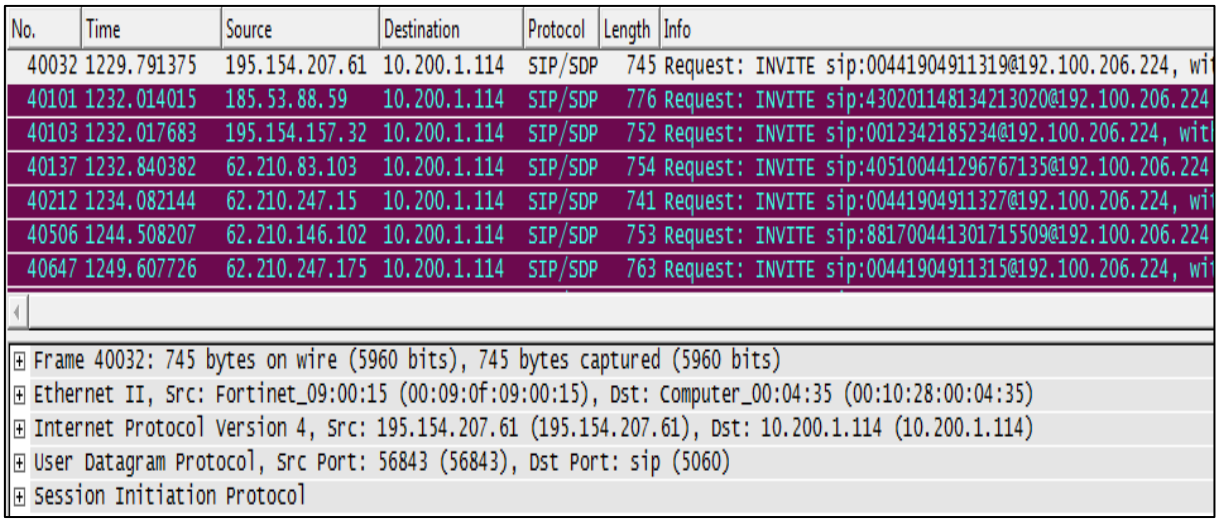


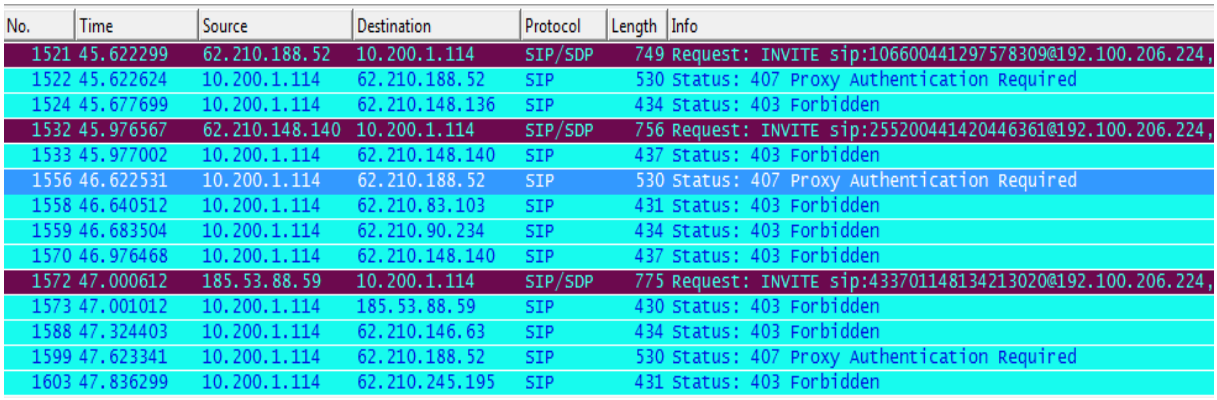
Figura 3.8 – INVITE

Fonte: Captura de tela Wireshark

No site *VoiP Blacklist* foram encontrados todos os IP's apresentados na figura 3.8. Na página *Network Systems Solutions*, que possui a mesma finalidade de listar endereços e destinos utilizados para ataques, também foram encontrados alguns dos IP's apresentados na figura acima citada.

Com base nessas informações e de acordo com item 2.2.3, temos indicações que se trata de um ataque via SIP Flood, já que ocorre uma inundação de INVITES que poderiam sobrecarregar o servidor proxy, houve momentos que foram recebidos 18 INVITES por segundo. No entanto, como não havia tráfego de chamadas dos ramais legítimos do PABX durante o recebimento dos ataques e nem todos os INVITES enviados possuíam no campo FROM o número de uma extensão SIP definida no PABX, não foram solicitadas a autenticação proxy pelo servidor para todos estes pacotes, logo, não ocorreram danos. Caso ocorresse, poderia haver atrasos nos envios de pacotes e uma interrupção total ou parcial do serviço, isso seria algo extremamente nocivo ao sistema.

Na figura 3.9 são apresentadas algumas das respostas aos INVITES recebidos.



No.	Time	Source	Destination	Protocol	Length	Info
1521	45.622299	62.210.188.52	10.200.1.114	SIP/SDP	749	Request: INVITE sip:106600441297578309@192.100.206.224,
1522	45.622624	10.200.1.114	62.210.188.52	SIP	530	Status: 407 Proxy Authentication Required
1524	45.677699	10.200.1.114	62.210.148.136	SIP	434	Status: 403 Forbidden
1532	45.976567	62.210.148.140	10.200.1.114	SIP/SDP	756	Request: INVITE sip:255200441420446361@192.100.206.224,
1533	45.977002	10.200.1.114	62.210.148.140	SIP	437	Status: 403 Forbidden
1556	46.622531	10.200.1.114	62.210.188.52	SIP	530	Status: 407 Proxy Authentication Required
1558	46.640512	10.200.1.114	62.210.83.103	SIP	431	Status: 403 Forbidden
1559	46.683504	10.200.1.114	62.210.90.234	SIP	434	Status: 403 Forbidden
1570	46.976468	10.200.1.114	62.210.148.140	SIP	437	Status: 403 Forbidden
1572	47.000612	185.53.88.59	10.200.1.114	SIP/SDP	775	Request: INVITE sip:433701148134213020@192.100.206.224,
1573	47.001012	10.200.1.114	185.53.88.59	SIP	430	Status: 403 Forbidden
1588	47.324403	10.200.1.114	62.210.146.63	SIP	434	Status: 403 Forbidden
1599	47.623341	10.200.1.114	62.210.188.52	SIP	530	Status: 407 Proxy Authentication Required
1603	47.836299	10.200.1.114	62.210.245.195	SIP	431	Status: 403 Forbidden

Figura 3.9 – SIP Flood

Fonte: Captura de tela wireshark

Ao continuar analisando os pacotes capturados, notou-se que os INVITES recebidos tinham como origem endereços IP diferentes, contudo, a mesma origem dispara dentro de um determinado intervalo de tempo novas tentativas de ataques, estas com CALL-ID diferentes. Foi percebido também que esses ataques são provenientes de endereços IP contidos em faixas de rede específicas. Cabe salientar que essas faixas de rede foram mapeadas e encontra-se disponível na blacklist em http://www.voipbl.org/.

Para facilitar o entendimento, foi criada a tabela 3 que demonstra as principais origens de ataques recebidos das redes 62.210.0.0/16, 195.154.0.0/16, 185.53.0.0/16, 37.49.0.0/16 e 163.172.0.0/16.

Endereço IP	**INVITES enviados**	**Resposta do PABX**	**Intervalo entre ataques (segundos)**
62.210.146.52	33	Forbidden	92
62.210.90.217	40	Forbidden	130
62.210.86.117	37	Forbidden	140
62.210.188.52	48	Proxy Authentication Rquired	85
62.210.146.63	60	Forbidden	75
62.210.247.15	40	Forbidden	132
195.154.133.184	43	Forbidden	123
195.154.157.32	42	Forbidden	125

185.53.88.59	266	Forbidden	20
37.49.231.87	18	Proxy Authentication Rquired	270
163.172.7.60	54	Forbidden	123

Tabela 3 – Endereços IP

Além dos INVITES recebidos, foram identificados pacotes OPTIONS durante a captura recebida pela rede 185.53.0.0/16, as mensagens são enviadas a cada aproximadamente 300 segundos. Conforme apresentado na Figura 3.10.

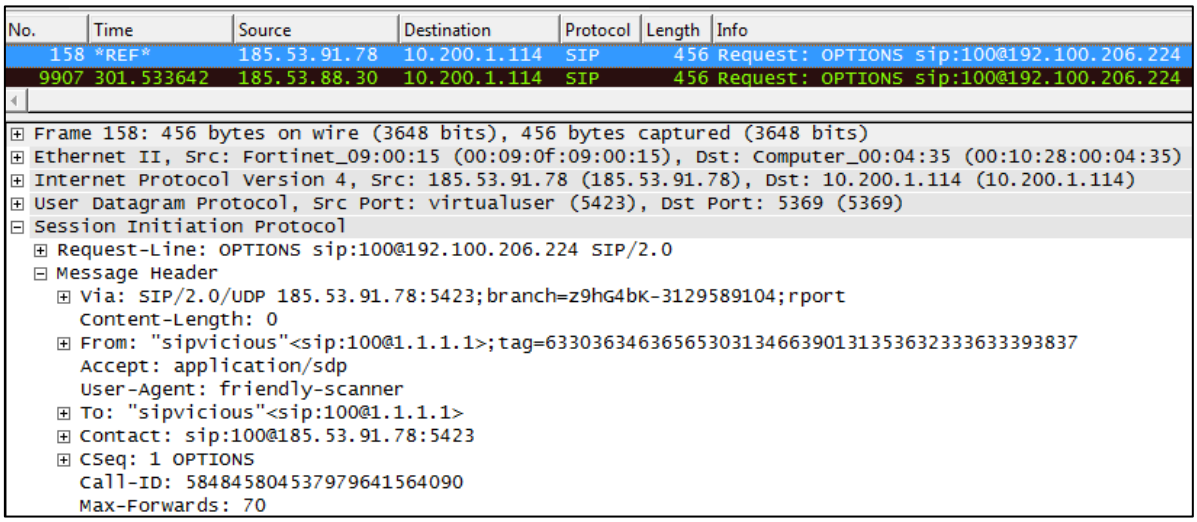


Figura 3.10 – Pacote OPTIONS (Cenário2)

Fonte: Captura de tela wireshark

Alguns dos endereços de origem apresentado anteriormente, fazem suas tentativas de ataques para o mesmo número externo, conforme figura 3.11.

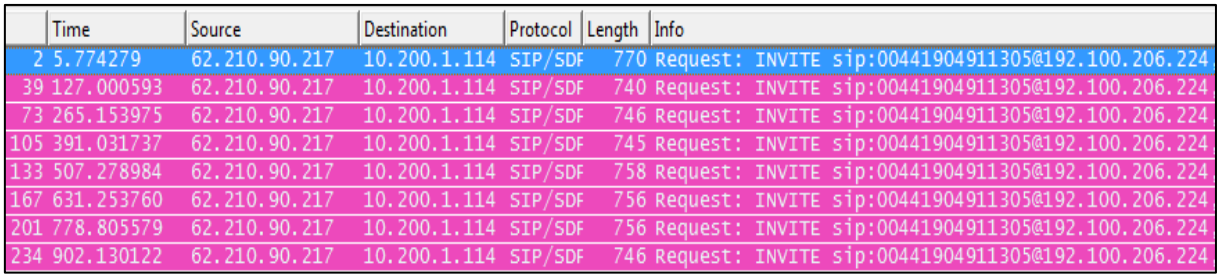


Figura 3.11 – Destino único

Fonte: Captura de tela Wireshark

No entanto, outros endereços modificam o número discado a cada INVITE enviado, conforme a figura a 3.12.

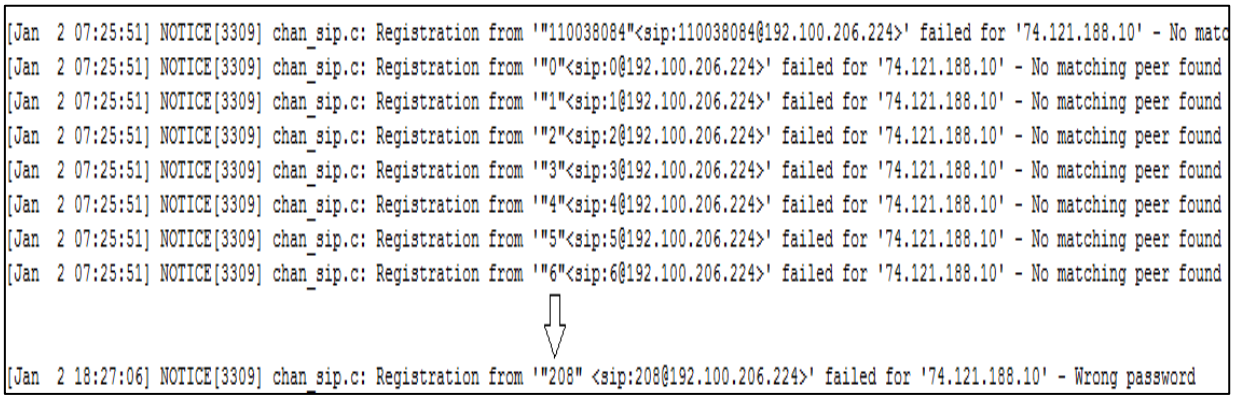
8	22.005343	62.210.146.52	10.200.1.114	SIP/SDF	753	Request: INVITE sip:142100441980874205@192.100.206.224,
32	110.467223	62.210.146.52	10.200.1.114	SIP/SDF	750	Request: INVITE sip:142200441980874205@192.100.206.224,
59	215.556463	62.210.146.52	10.200.1.114	SIP/SDF	752	Request: INVITE sip:142300441980874205@192.100.206.224,
83	307.624426	62.210.146.52	10.200.1.114	SIP/SDF	753	Request: INVITE sip:142400441980874205@192.100.206.224,
109	406.024237	62.210.146.52	10.200.1.114	SIP/SDF	753	Request: INVITE sip:142500441980874205@192.100.206.224,
132	502.445394	62.210.146.52	10.200.1.114	SIP/SDF	753	Request: INVITE sip:142600441980874205@192.100.206.224,
159	601.068869	62.210.146.52	10.200.1.114	SIP/SDF	749	Request: INVITE sip:142700441980874205@192.100.206.224,
182	689.666222	62.210.146.52	10.200.1.114	SIP/SDF	752	Request: INVITE sip:142800441980874205@192.100.206.224,
203	783.496839	62.210.146.52	10.200.1.114	SIP/SDF	754	Request: INVITE sip:142900441980874205@192.100.206.224,
228	867.537522	62.210.146.52	10.200.1.114	SIP/SDF	754	Request: INVITE sip:143000441980874205@192.100.206.224,
250	960.300630	62.210.146.52	10.200.1.114	SIP/SDF	755	Request: INVITE sip:143100441980874205@192.100.206.224,
271	1049.999609	62.210.146.52	10.200.1.114	SIP/SDF	754	Request: INVITE sip:143200441980874205@192.100.206.224,

Figura 3.12 – Destinos distintos

Fonte: Captura de tela wireshark

Se no momento do monitoramento outras chamadas estiverem em curso no PABX, é possível que esses pacotes não sejam notados pelo administrador do responsável pelo sistema, já que cada uma dessas tentativas é enviada após aproximadamente 85 segundos e são para números distintos.

Ao consultar os logs internos disponíveis pelo PABX, foi possível identificar uma quantidade abusiva de requisição de registros. No dia 02 de janeiro foram recebidos pedidos de registros oriundos do endereço IP 74.121.188.10, o primeiro pacote iniciou às 07h25 da manhã e o último enviado foi às 18h27. Houve momentos que o atacante enviava mais de 60 tentativas de registros por segundo. A figura 3.13 mostra os primeiros e últimos pacotes enviados pelo atacante.



```
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"110038084"<sip:110038084@192.100.206.224>' failed for '74.121.188.10' - No matc
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"0"<sip:0@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"1"<sip:1@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"2"<sip:2@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"3"<sip:3@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"4"<sip:4@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"5"<sip:5@192.100.206.224>' failed for '74.121.188.10' - No matching peer found
[Jan  2 07:25:51] NOTICE[3309] chan_sip.c: Registration from '"6"<sip:6@192.100.206.224>' failed for '74.121.188.10' - No matching peer found

[Jan  2 18:27:06] NOTICE[3309] chan_sip.c: Registration from '"208" <sip:208@192.100.206.224>' failed for '74.121.188.10' - Wrong password
```

Figura 3.13 – Tentativa de quebra de registro

Fonte: Logs internos PABX

Com essas informações pode-se afirmar que o PABX recebeu uma tentativa de quebra de senha. Como essas requisições de registros foram enviadas destinando-se ao ramal 0 até o ramal 208, e a faixa de ramais configurada no PABX inicia como 2000, não houveram danos. Caso esses pacotes fossem direcionados aos ramais existentes, o PABX poderia ter seus recursos comprometidos.

3.3 SIPVicious

Durante as capturas realizadas com diferentes modelos de PABX IP, notou-se um padrão de informações enviadas pelo usuário mal-intencionado, os pacotes *OPTIONS* e *INVITES* enviados por este, continham informações semelhantes em alguns parâmetros do cabeçalho. Na maioria dos casos o campo *User-Agent* apresentava-se como *friendly-scanner* e a origem desse pacote como “sipvicious”, conforme a figura 3.14.

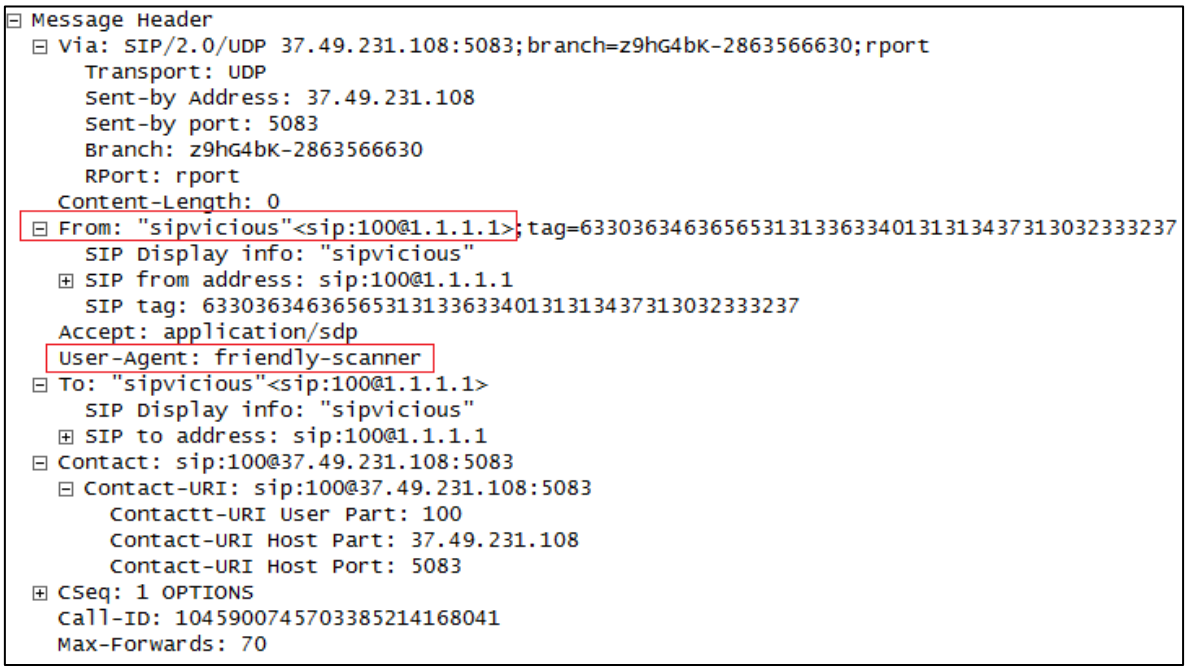


Figura 3.14 – Sipvicious

Fonte: Captura de tela Wireshark

A aplicação SIPVicious é uma ferramenta gratuita que tem por objetivo simular tentativas de ataques direcionadas a equipamentos VoIP, visando testar possíveis fragilidades. Da mesma forma que a ferramenta pode ser usada para descobrir brechas e assim implementar melhorias, há quem se aposse dela para realizar

ataques mal-intencionados. Como pode ser observado na figura 3.14, a captura de pacotes provindos da aplicação SIPVicious tem o *User-Agent* denominado '*friendly-scanner'*. A disponibilidade do pacote de instalação no blog SIPVicious permitiu ao autor deste documento simular os cenários descritos abaixo.

Através da aplicação SIPVicious foram realizados testes seguindo o procedimento feito pelo um invasor. Inicialmente foi realizado o escaneamento da rede através do svmap[2]. Ao utilizar esse comando, o programa envia pacotes SIP com o método *OPTIONS* para o IP ou faixa de IP definidas. O intuito é identificar as portas abertas em um dispositivo de rede e saber quais serviços esse equipamento utiliza. A figura 3.15 demonstra o escaneamento na interface de rede do IP 10.1.43.46, sendo possível identificar informações do equipamento de rede que está nesse endereço.

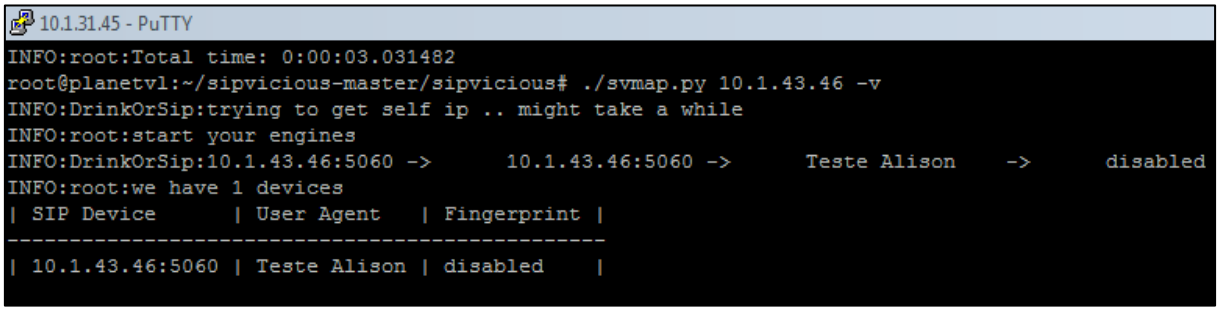


Figura 3.15 – svmap

Fonte: Captura de tela Putty

Monitorando esse pacote com o *Wireshark* na interface de rede do PABX de teste, é possível identificar a mensagem *OPTIONS* do usuário mal-intencionado e a resposta do PABX, conforme apresentado na figura 3.16 abaixo.

[2] `Svmap:` lista os dispositivos SIP encontrados em uma determinada faixa de IP.

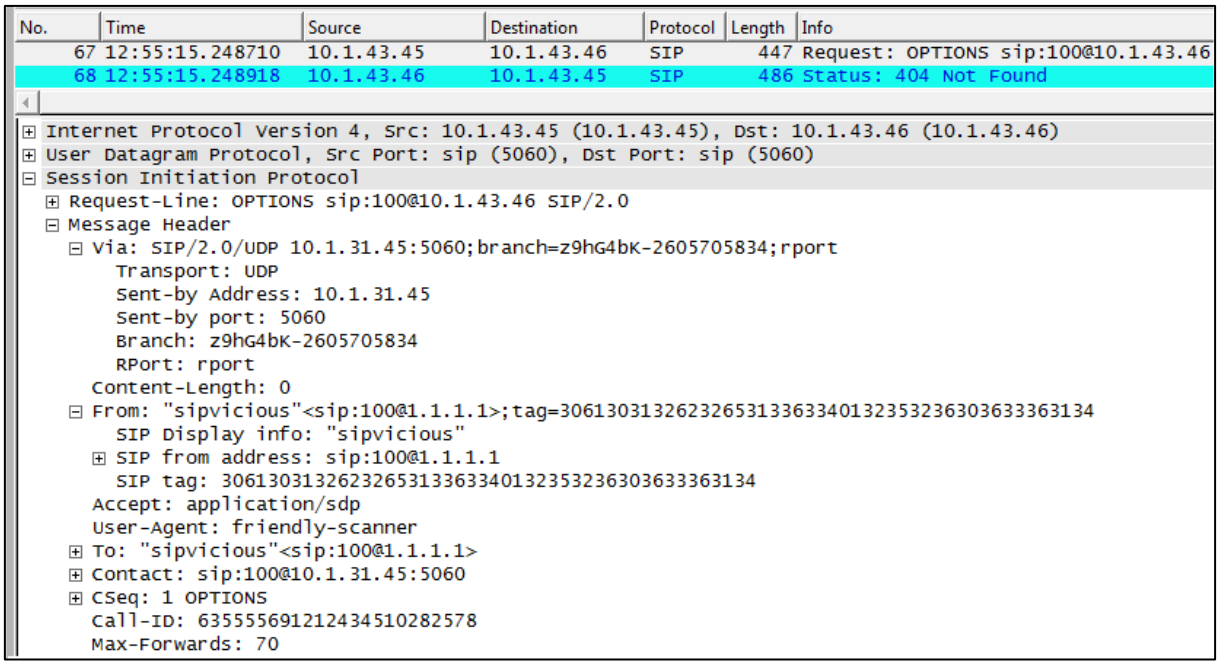


Figura 3.16 – OPTIONS (SIPVicious)

Fonte: Captura de tela Wireshark

Mesmo com o PABX respondendo o pacote *OPTIONS* com 404 (*NOT FOUND*), são enviadas informações para o atacante que indicam que naquele endereço IP há um equipamento VoIP com o endereço 10.1.43.46, utilizando a porta SIP padrão (5060) e o *User-Agent* do PABX é Teste Alison, conforme a figura 3.17.

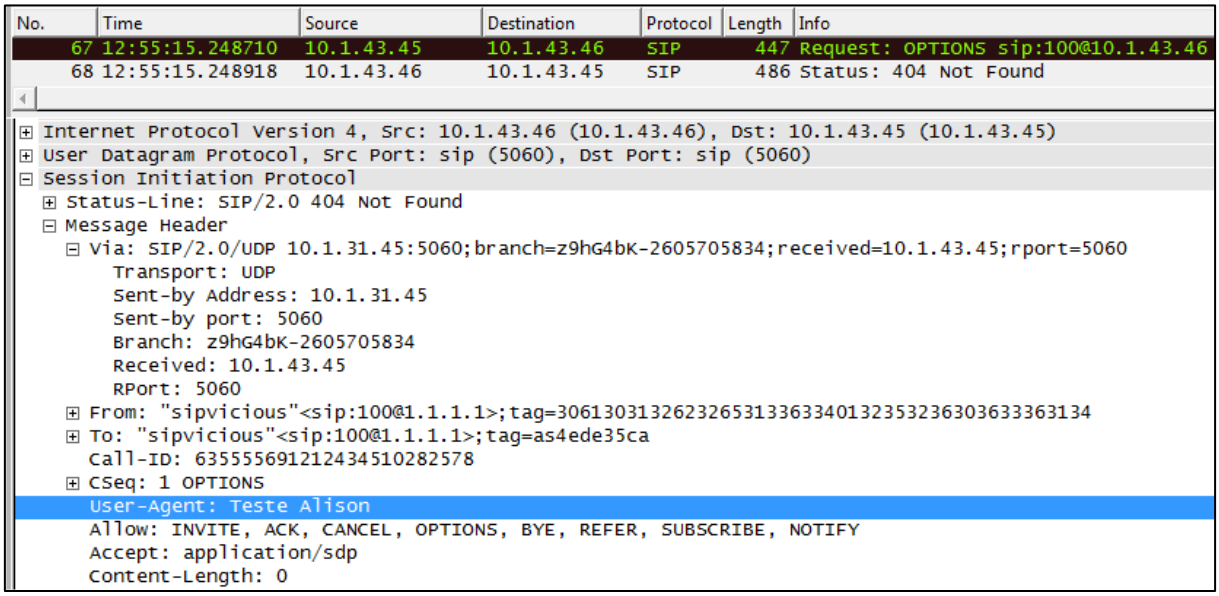


Figura 3.17 – Teste Alison

Fonte: Captura de tela Wireshark

Após a descoberta do PABX, foi utilizado a aplicação svwar[3] que tem por objetivo tentar identificar quais ramais existem no PABX 10.1.43.46. No teste demonstrado na figura 3.18, procurou-se ramais da faixa de 2000 até 2010, conforme a resposta referente aos *INVITES* enviados, foi possível identificar que os ramais 2000 e 2010 existem nesse PABX e eles necessitam de autenticação.

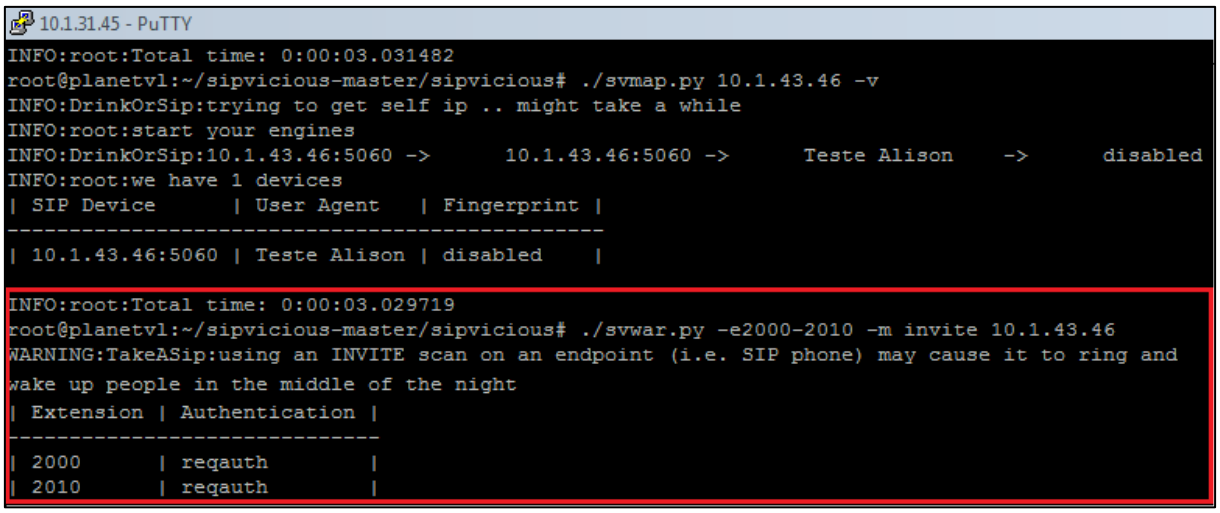
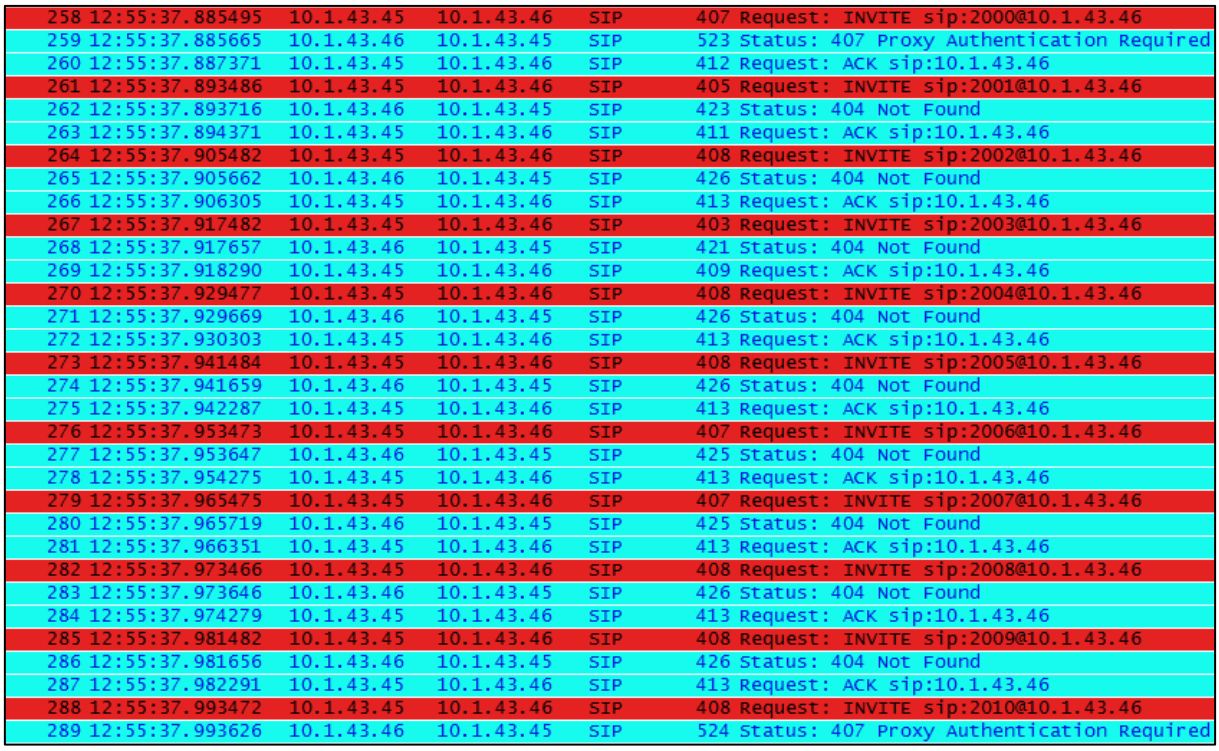


Figura 3.18 – Svwar

Fonte: Captura de tela Putty

Monitorando a interface de rede do PABX, notou-se o envio de *INVITES* para a faixa de ramais definida pelo atacante, conforme a figura 3.19.

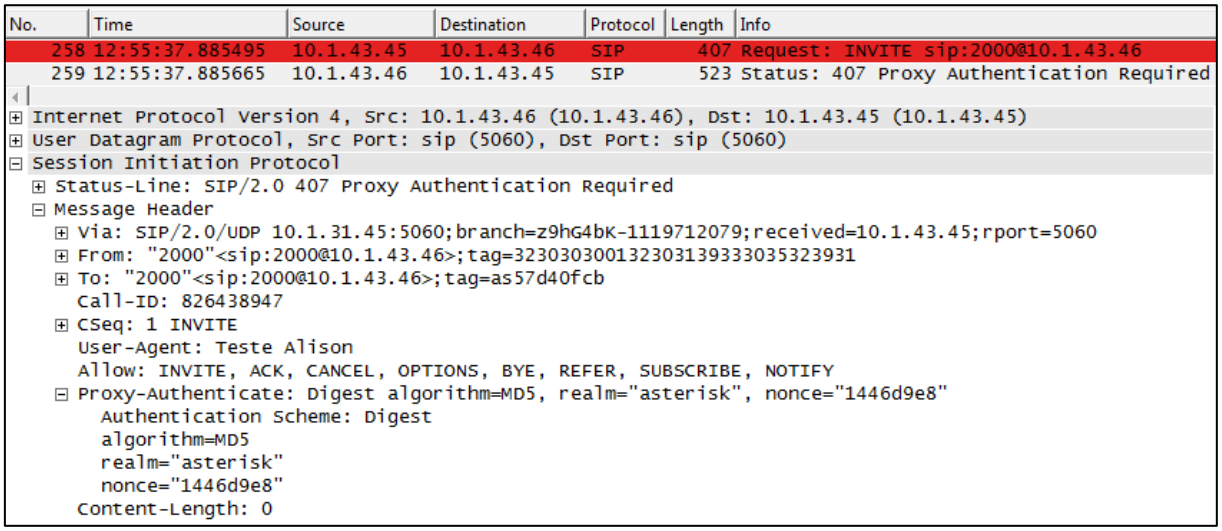
[3] Svwar: identifica ramais ativos de um PABX IP.



No.	Time	Source	Destination	Protocol	Length	Info
258	12:55:37.885495	10.1.43.45	10.1.43.46	SIP	407	Request: INVITE sip:2000@10.1.43.46
259	12:55:37.885665	10.1.43.46	10.1.43.45	SIP	523	Status: 407 Proxy Authentication Required
260	12:55:37.887371	10.1.43.45	10.1.43.46	SIP	412	Request: ACK sip:10.1.43.46
261	12:55:37.893486	10.1.43.45	10.1.43.46	SIP	405	Request: INVITE sip:2001@10.1.43.46
262	12:55:37.893716	10.1.43.46	10.1.43.45	SIP	423	Status: 404 Not Found
263	12:55:37.894371	10.1.43.45	10.1.43.46	SIP	411	Request: ACK sip:10.1.43.46
264	12:55:37.905482	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2002@10.1.43.46
265	12:55:37.905662	10.1.43.46	10.1.43.45	SIP	426	Status: 404 Not Found
266	12:55:37.906305	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
267	12:55:37.917482	10.1.43.45	10.1.43.46	SIP	403	Request: INVITE sip:2003@10.1.43.46
268	12:55:37.917657	10.1.43.46	10.1.43.45	SIP	421	Status: 404 Not Found
269	12:55:37.918290	10.1.43.45	10.1.43.46	SIP	409	Request: ACK sip:10.1.43.46
270	12:55:37.929477	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2004@10.1.43.46
271	12:55:37.929669	10.1.43.46	10.1.43.45	SIP	426	Status: 404 Not Found
272	12:55:37.930303	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
273	12:55:37.941484	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2005@10.1.43.46
274	12:55:37.941659	10.1.43.46	10.1.43.45	SIP	426	Status: 404 Not Found
275	12:55:37.942287	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
276	12:55:37.953473	10.1.43.45	10.1.43.46	SIP	407	Request: INVITE sip:2006@10.1.43.46
277	12:55:37.953647	10.1.43.46	10.1.43.45	SIP	425	Status: 404 Not Found
278	12:55:37.954275	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
279	12:55:37.965475	10.1.43.45	10.1.43.46	SIP	407	Request: INVITE sip:2007@10.1.43.46
280	12:55:37.965719	10.1.43.46	10.1.43.45	SIP	425	Status: 404 Not Found
281	12:55:37.966351	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
282	12:55:37.973466	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2008@10.1.43.46
283	12:55:37.973646	10.1.43.46	10.1.43.45	SIP	426	Status: 404 Not Found
284	12:55:37.974279	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
285	12:55:37.981482	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2009@10.1.43.46
286	12:55:37.981656	10.1.43.46	10.1.43.45	SIP	426	Status: 404 Not Found
287	12:55:37.982291	10.1.43.45	10.1.43.46	SIP	413	Request: ACK sip:10.1.43.46
288	12:55:37.993472	10.1.43.45	10.1.43.46	SIP	408	Request: INVITE sip:2010@10.1.43.46
289	12:55:37.993626	10.1.43.46	10.1.43.45	SIP	524	Status: 407 Proxy Authentication Required

Figura 3.19 – INVITE (SIPVicious)
Captura de tela Wireshark

Quando os pacotes são direcionados a ramais, é solicitada uma autenticação Proxy por parte do PABX, informação essa que é satisfatória para o atacante confirmar que esse ramal de fato existe no PABX. A figura 3.20 demonstra a autenticação *proxy* enviada do PABX ao atacante.



No.	Time	Source	Destination	Protocol	Length	Info
258	12:55:37.885495	10.1.43.45	10.1.43.46	SIP	407	Request: INVITE sip:2000@10.1.43.46
259	12:55:37.885665	10.1.43.46	10.1.43.45	SIP	523	Status: 407 Proxy Authentication Required

```
⊞ Internet Protocol Version 4, Src: 10.1.43.46 (10.1.43.46), Dst: 10.1.43.45 (10.1.43.45)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 407 Proxy Authentication Required
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 10.1.31.45:5060;branch=z9hG4bK-1119712079;received=10.1.43.45;rport=5060
    ⊞ From: "2000"<sip:2000@10.1.43.46>;tag=32303030013230313933333035323931
    ⊞ To: "2000"<sip:2000@10.1.43.46>;tag=as57d40fcb
      Call-ID: 826438947
    ⊞ CSeq: 1 INVITE
      User-Agent: Teste Alison
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
    ⊟ Proxy-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="1446d9e8"
        Authentication Scheme: Digest
        algorithm=MD5
        realm="asterisk"
        nonce="1446d9e8"
      Content-Length: 0
```

Figura 3.20 – *Authentication Required*
Fonte: Captura de tela Wireshark

Caso esses pacotes *INVITES* fossem direcionados a troncos IP do PABX que não necessitem de autenticação, chegaria até o ramal atendedor (dando a sensação de estar recebendo uma chamada), além de consumir recursos do PABX. O próprio programa SIPVicious alerta sobre o *INVITE* enviado quando utilizado a aplicação svwar, conforme a figura 3.21.

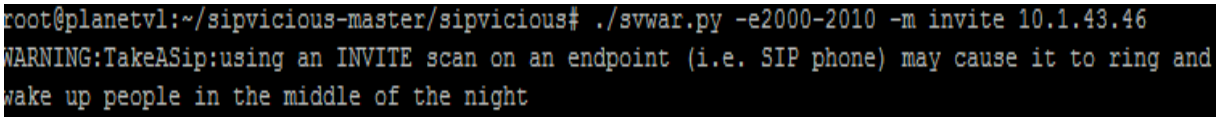


Figura 3.21 – *Ring*

Fonte: Captura de tela Putty

Com a descoberta dos ramais ou troncos que existem no PABX IP, o usuário mal-intencionado pode eleger qual maneira atacar o PABX. Uma possibilidade é enviar enxurradas de *INVITES* para prejudicar a disponibilidade da central, ataque este denominado SIP *Flood*.

Uma outra alternativa para tentar atacar o PABX é descobrir a senha dos ramais, podendo assim realizar chamadas externas para outros destinos. Através da aplicação svcrack[4], buscou-se identificar a senha do ramal 2000 utilizando a quebra de senha (ataque por dicionário). Dentro do código da aplicação svcrack, é possível definir quais possíveis senhas serão utilizadas para tentar quebrar a senha do ramal, geralmente essas tentativas iniciam pelas senhas mais óbvias como o próprio o número do ramal ou 12345. Com a finalidade de descobrir a senha do ramal, o SIPVicious envia pedido de registros (mensagem REGISTER) para o PABX IP referente a cada senha contida no seu dicionário. A tentativa foi bem-sucedida conforme a figura 3.22, onde temos a resposta que a senha do ramal 2000 é: 2000.

[4] Svcrack: um cracker de senha on-line para PABX IP SIP

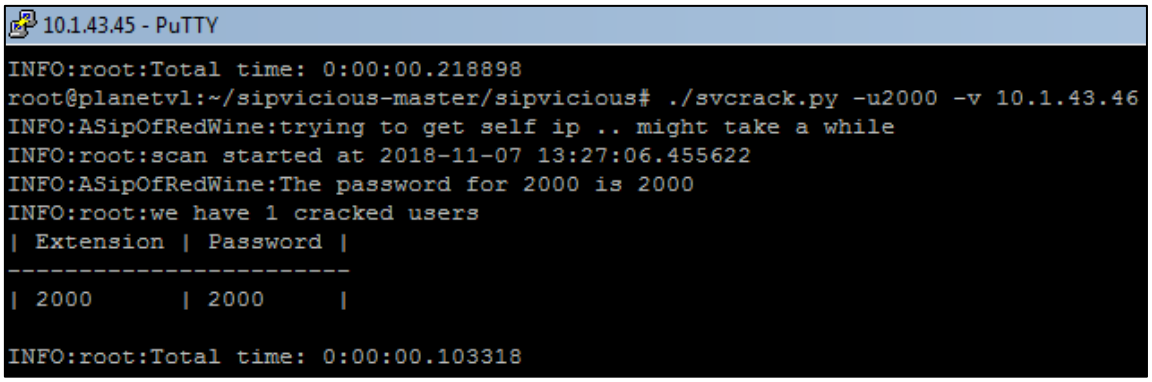


Figura 3.22 – Svcrack

Fonte: Captura de tela Wireshark

No monitoramento realizado no PABX, é possível identificar o envio do pedido de registro do IP 10.1.43.45, o PABX envia a resposta 100 (*Trying*) e em seguida solicita o desafio enviando a resposta 401, incluindo o campo *Authorization*. Na sequência, o atacante resolve o desafio enviando novamente o pedido de registro contendo o response. Como a primeira tentativa de registro foi utilizando a senha correta, o SIPVicious não envia mais pedidos. Caso contrário, iria enviar requisições até descobrir a senha de autenticação ou esgotar as senhas definidas em seu dicionário. A figura 3.23 representa o registro bem-sucedido realizado pelo invasor.

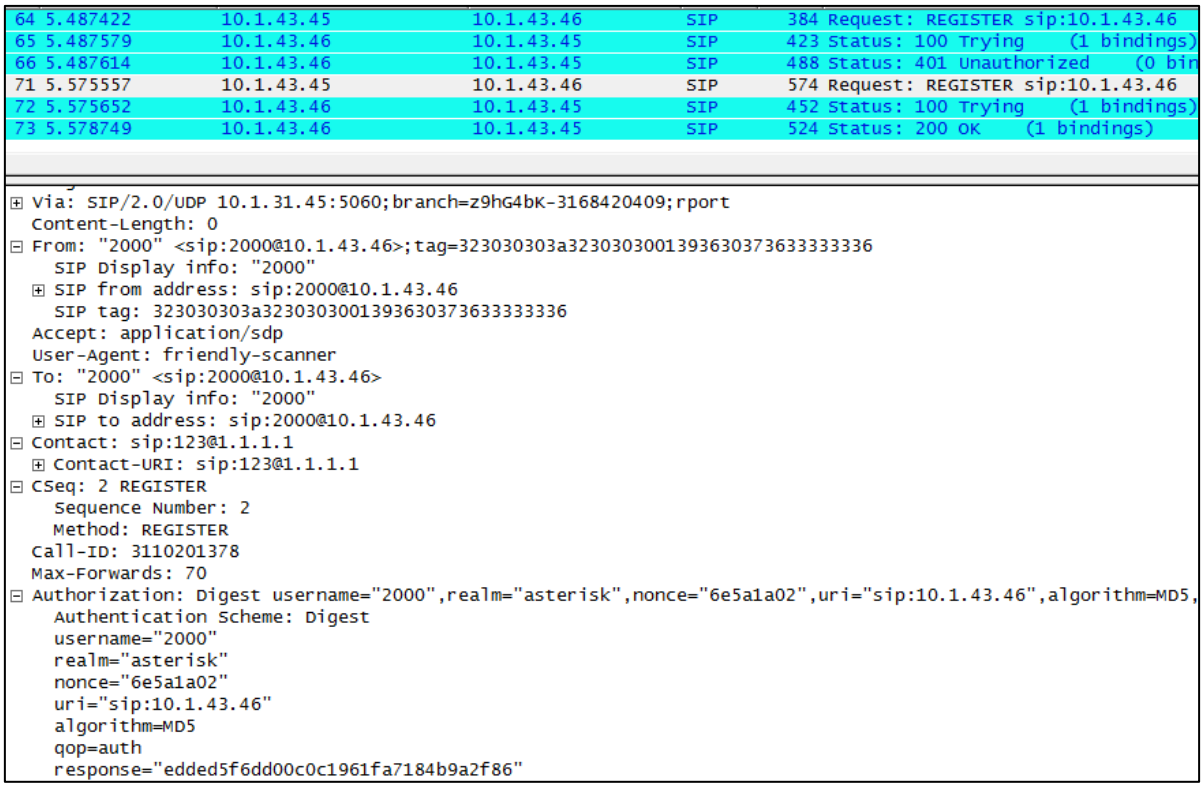


Figura 3.23 – Register (SIPVicious)

Fonte: Captura de tela Wireshark

A fim de sintetizar os testes efetuados e facilitar o entendimento dos cenários e tipos de ataques recebidos, foi elaborada a tabela 4, a qual contém a descrição para os principais ataques recebidos:

Tipos de Ataque	**Objetivo do ataque**	**Descrição**	**Protocolo**
Varredura	Descobrir quais portas estão disponíveis no PABX	Envio do método OPTIONS	SIP UDP
SIP *Flood*	Indisponibilizar o PABX com inundações de pacotes	Envio da mensagem INVITE	SIP
Quebra de senha (ataque por dicionário)	Descobrir a senha de uma extensão SIP	Tentativa de registro. Envio da mensagem REGISTER	SIP

Acesso remoto	Ter acesso as configurações do PABX para indisponibilizá-lo ou utilizá-lo para benefício próprio.	Tentativa de acesso via HTTPS e Telnet	TCP

Tabela 4 – Descrição dos ataques recebidos

4 CONTRAMEDIDAS

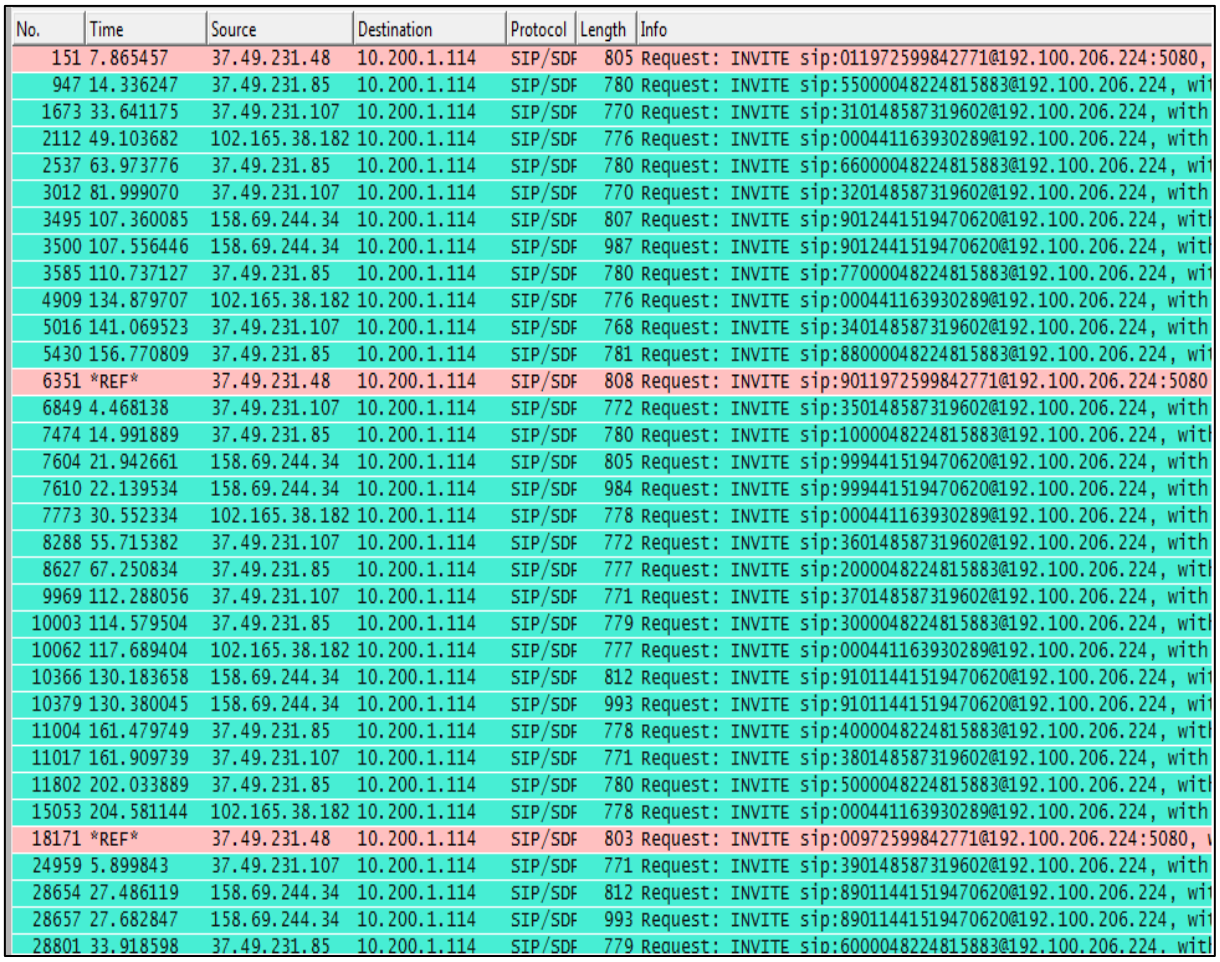
Após analisar os cenários acima descritos, procuram-se identificar medidas de prevenção aos ataques maliciosos. Essas medidas devem garantir que o tripé da segurança da informação seja preservado, possibilitando assim uma comunicação VoIP confiável, disponível e íntegra.

4.1 Alteração da porta SIP

Como primeira contramedida indica-se a modificação da porta de escuta SIP no equipamento VoIP. De acordo com a RFC 3261, a porta padrão SIP é a 5060, motivo pelo qual a maioria dos ataques são direcionados a esta. Todavia, o protocolo permite a alteração da porta SIP, alteração esta que dificulta a tentativa de ataque. Conforme apresentado na figura 4.1 o simples fato de alterar a porta de escuta SIP no cenário 2, minimizou o alcance a porta correta do PABX IP, já que muitos ataques são automatizados e buscam a porta 5060, pois a maioria dos PABX a utilizam.

Ao realizar a captura dos logs na interface de rede do PABX durante aproximadamente 10 minutos, foram recebidos 43 *INVITES* de diferentes endereços IP.

Analisando as 43 tentativas de chamadas, apenas 3 delas foram atendidas pelo PABX, isso ocorreu devido ao invasor enviar o *INVITE* de 40 chamadas destinadas a porta 5060 e apenas 3 delas com destino a porta 5080, conforme apresentado na figura 4.1.

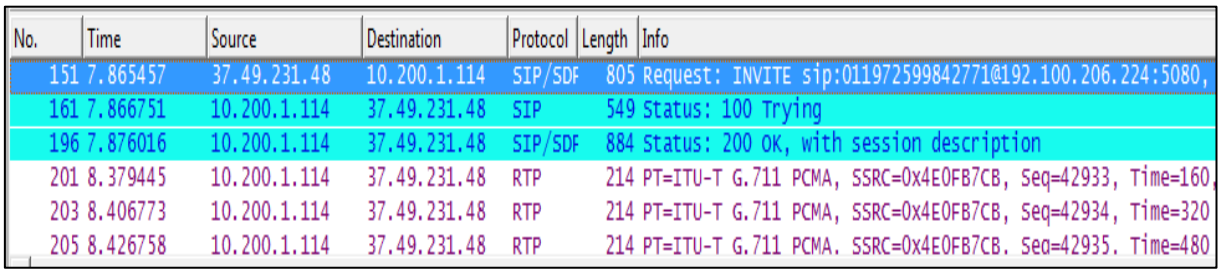


No.	Time	Source	Destination	Protocol	Length	Info
151	7.865457	37.49.231.48	10.200.1.114	SIP/SDP	805	Request: INVITE sip:011972599842771@192.100.206.224:5080,
947	14.336247	37.49.231.85	10.200.1.114	SIP/SDP	780	Request: INVITE sip:55000048224815883@192.100.206.224, wi
1673	33.641175	37.49.231.107	10.200.1.114	SIP/SDP	770	Request: INVITE sip:310148587319602@192.100.206.224, with
2112	49.103682	102.165.38.182	10.200.1.114	SIP/SDP	776	Request: INVITE sip:000441163930289@192.100.206.224, with
2537	63.973776	37.49.231.85	10.200.1.114	SIP/SDP	780	Request: INVITE sip:66000048224815883@192.100.206.224, wi
3012	81.999070	37.49.231.107	10.200.1.114	SIP/SDP	770	Request: INVITE sip:320148587319602@192.100.206.224, with
3495	107.360085	158.69.244.34	10.200.1.114	SIP/SDP	807	Request: INVITE sip:9012441519470620@192.100.206.224, wit
3500	107.556446	158.69.244.34	10.200.1.114	SIP/SDP	987	Request: INVITE sip:9012441519470620@192.100.206.224, wit
3585	110.737127	37.49.231.85	10.200.1.114	SIP/SDP	780	Request: INVITE sip:77000048224815883@192.100.206.224, wi
4909	134.879707	102.165.38.182	10.200.1.114	SIP/SDP	776	Request: INVITE sip:000441163930289@192.100.206.224, with
5016	141.069523	37.49.231.107	10.200.1.114	SIP/SDP	768	Request: INVITE sip:340148587319602@192.100.206.224, with
5430	156.770809	37.49.231.85	10.200.1.114	SIP/SDP	781	Request: INVITE sip:88000048224815883@192.100.206.224, wi
6351	*REF*	37.49.231.48	10.200.1.114	SIP/SDP	808	Request: INVITE sip:9011972599842771@192.100.206.224:5080
6849	4.468138	37.49.231.107	10.200.1.114	SIP/SDP	772	Request: INVITE sip:350148587319602@192.100.206.224, with
7474	14.991889	37.49.231.85	10.200.1.114	SIP/SDP	780	Request: INVITE sip:1000048224815883@192.100.206.224, wit
7604	21.942661	158.69.244.34	10.200.1.114	SIP/SDP	805	Request: INVITE sip:999441519470620@192.100.206.224, with
7610	22.139534	158.69.244.34	10.200.1.114	SIP/SDP	984	Request: INVITE sip:999441519470620@192.100.206.224, with
7773	30.552334	102.165.38.182	10.200.1.114	SIP/SDP	778	Request: INVITE sip:000441163930289@192.100.206.224, with
8288	55.715382	37.49.231.107	10.200.1.114	SIP/SDP	772	Request: INVITE sip:360148587319602@192.100.206.224, with
8627	67.250834	37.49.231.85	10.200.1.114	SIP/SDP	777	Request: INVITE sip:2000048224815883@192.100.206.224, wit
9969	112.288056	37.49.231.107	10.200.1.114	SIP/SDP	771	Request: INVITE sip:370148587319602@192.100.206.224, with
10003	114.579504	37.49.231.85	10.200.1.114	SIP/SDP	779	Request: INVITE sip:3000048224815883@192.100.206.224, wit
10062	117.689404	102.165.38.182	10.200.1.114	SIP/SDP	777	Request: INVITE sip:000441163930289@192.100.206.224, with
10366	130.183658	158.69.244.34	10.200.1.114	SIP/SDP	812	Request: INVITE sip:91011441519470620@192.100.206.224, wi
10379	130.380045	158.69.244.34	10.200.1.114	SIP/SDP	993	Request: INVITE sip:91011441519470620@192.100.206.224, wi
11004	161.479749	37.49.231.85	10.200.1.114	SIP/SDP	778	Request: INVITE sip:4000048224815883@192.100.206.224, wit
11017	161.909739	37.49.231.107	10.200.1.114	SIP/SDP	771	Request: INVITE sip:380148587319602@192.100.206.224, with
11802	202.033889	37.49.231.85	10.200.1.114	SIP/SDP	780	Request: INVITE sip:5000048224815883@192.100.206.224, wit
15053	204.581144	102.165.38.182	10.200.1.114	SIP/SDP	778	Request: INVITE sip:000441163930289@192.100.206.224, with
18171	*REF*	37.49.231.48	10.200.1.114	SIP/SDP	803	Request: INVITE sip:00972599842771@192.100.206.224:5080,
24959	5.899843	37.49.231.107	10.200.1.114	SIP/SDP	771	Request: INVITE sip:390148587319602@192.100.206.224, with
28654	27.486119	158.69.244.34	10.200.1.114	SIP/SDP	812	Request: INVITE sip:89011441519470620@192.100.206.224, wi
28657	27.682847	158.69.244.34	10.200.1.114	SIP/SDP	993	Request: INVITE sip:89011441519470620@192.100.206.224, wi
28801	33.918598	37.49.231.85	10.200.1.114	SIP/SDP	779	Request: INVITE sip:6000048224815883@192.100.206.224, wit

Figura 4.1 – Porta 5080

Fonte: Captura de tela Wireshark

Na figura 4.2 é apresentado detalhadamente o pacote SIP enviado pelo atacante e o atendimento da chamada pelo PABX.



No.	Time	Source	Destination	Protocol	Length	Info
151	7.865457	37.49.231.48	10.200.1.114	SIP/SDP	805	Request: INVITE sip:011972599842771@192.100.206.224:5080,
161	7.866751	10.200.1.114	37.49.231.48	SIP	549	Status: 100 Trying
196	7.876016	10.200.1.114	37.49.231.48	SIP/SDP	884	Status: 200 OK, with session description
201	8.379445	10.200.1.114	37.49.231.48	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x4E0FB7CB, Seq=42933, Time=160
203	8.406773	10.200.1.114	37.49.231.48	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x4E0FB7CB, Seq=42934, Time=320
205	8.426758	10.200.1.114	37.49.231.48	RTP	214	PT=ITU-T G.711 PCMA, SSRC=0x4E0FB7CB, Seq=42935, Time=480

Figura 4.2 – Chamada atendida

Fonte: Captura de tela Wireshark

Esse tipo de ataque recebido leva o usuário acreditar que está recebendo uma chamada válida. Caso todos os INVITES fossem recebidos pelo PABX poderíamos

considerar um tipo de ataque DoS, já que o PABX consumiria recursos para tratar as chamadas falsas, podendo deixar de atender chamadas reais.

Dessa forma entende-se que alterar a porta SIP é uma boa prática em ambientes VoiP que pode inibir ataques do tipo SIP Flood e quebra de senha.

4.2 Alteração de senhas

Além da modificação da porta SIP, outra alteração é não configurar senhas simples nos ramais. Quando há senhas fracas nos equipamentos VoIP, estes tornam-se alvos fáceis para servidores mal-intencionados. Existem equipamentos VoIP que não permitem que sejam criadas senhas simples, obrigando o usuário a utilizar caracteres especiais, números, além de diferenciar letras maiúsculas de minúsculas. Foi realizada a alteração da senha do ramal 2000 do PABX IP de teste para 2000@Teste e diferente do que ocorreu na figura 3.18 não foi possível descobrir a senha do ramal IP. O atacante enviou pedidos de registro até finalizar as senhas disponíveis no seu dicionário, conforme ilustrado na figura 4.3. Essa simples alteração dificultou o ataque de quebra de senha. Essa é uma recomendação para qualquer aplicação ou sistema que use senhas.

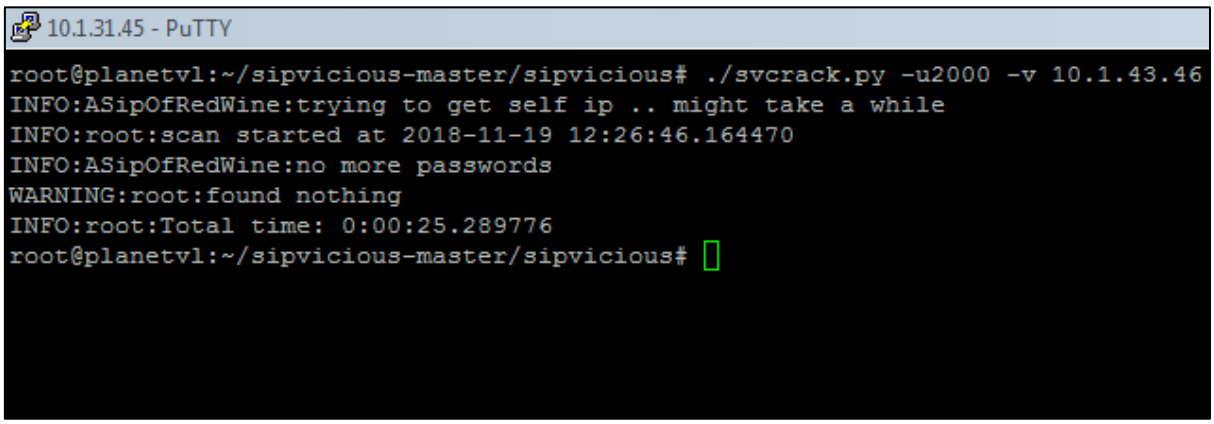


Figura 4.3 – *No more passwords*

Fonte: Captura de tela Putty

Na figura 4.4 no monitoramento realizado na interface de rede do PABX, é possível visualizar diversas requisições de registro oriundas do atacante com destino ao PABX e sem sucesso na autenticação.

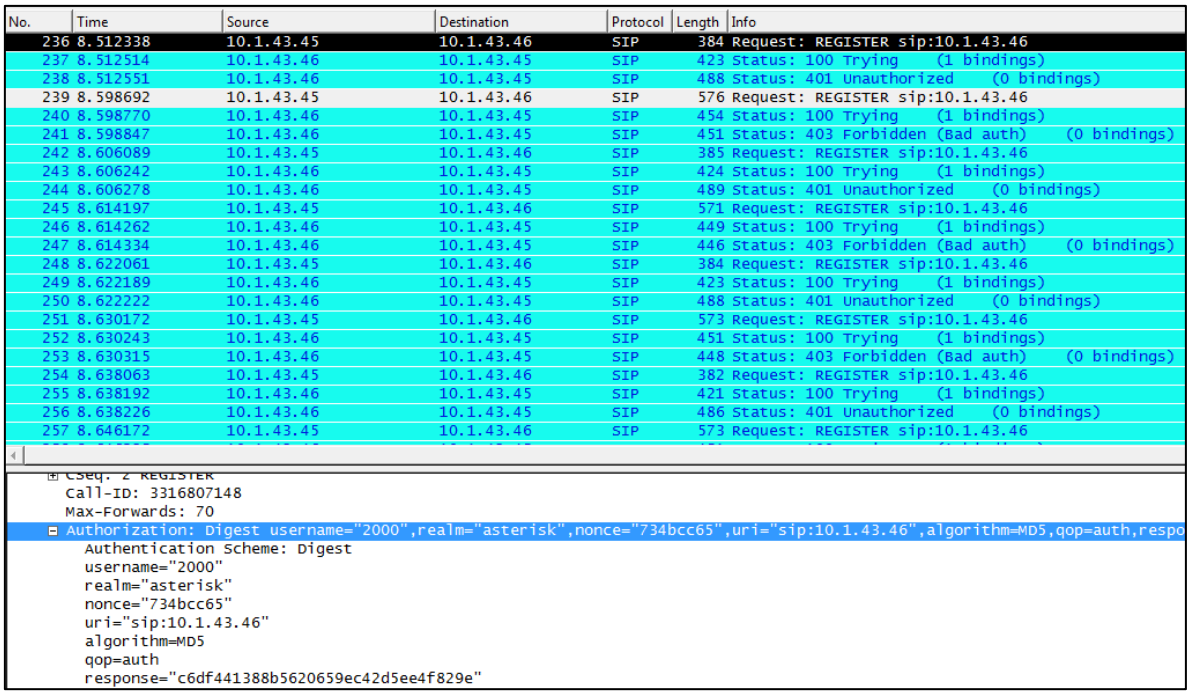


Figura 4.4 – Bad Auth

Fonte: Captura de tela Wireshark

4.3 Filtragem de pacotes e Firewall

Uma outra alternativa para reforçar a segurança de um ambiente VoIP é a utilização da filtragem de pacotes. Com as devidas configurações, é possível permitir que pacotes oriundos de endereços IP conhecidos alcancem o destino desejado. Já os pacotes cuja a origem é desconhecida, serão barrados, impedindo assim de acessar o equipamento VoIP. Na figura abaixo foi realizado um filtro de pacotes em conjunto com um script que possui o intuito de bloquear inundações de pacotes SIP REGISTER oriundos de um mesmo endereço IP, caso a quantidade recebidas desses pacotes sejam superiores a 10 tentativas em 1 segundo, o endereço IP é adicionado na política DROP (blacklist).

```
#!/bin/bash
touch /root/teste.txt
# Alimenta o arquivo BLOQUEIO.txt com pedidos na porta 5060 para ser verificado
tcpdump -c 200 -n -i eth1 port 5060 and dst 10.200.1.114 > BLOQUEIO.txt

# Faz separação por segundo de cada pacote ( deixa todos pacotes em cada segundo )
cat BLOQUEIO.txt | cut -d . -f 1 | uniq | while read HORA; do
    # Faz separação de cada IP ( exclui IPs repetidos )
    cat BLOQUEIO.txt | tr -s " " | cut -d " " -f 3 | sort | cut -d . -f 1,2,3,4 | uniq | while read LINE; do
           # Verifica se há regras do IP amostrado no arquivo rc.local
           cat /etc/rc.local | grep "INPUT -s" | grep "$LINE" &> /dev/null
           if [ $? = 1 ]; then
              #caso não tenha IP na regra, casa com esse IF pra verificar quantas tentativas esse IP teve em 1
              # Contabiliza número de vezes que o IP enviou o pedido de registro ( SIP REGISTER )
              quantos=$(cat BLOQUEIO.txt | grep ^$HORA | grep -c $LINE)
              if [ $quantos -gt 10 ]; then # se passar de 10 tentativas ele inclui o IP na blacklis
              iptables -A INPUT -s $LINE -j DROP
              iptables -A FORWARD -s $LINE -j DROP
              echo "iptables -A INPUT -s $LINE -j DROP" >> /etc/rc.local
              echo "iptables -A FORWARD -s $LINE -j DROP" >> /etc/rc.local
              data=$( date )
              echo "#$data. Add o IP $LINE na regra de blacklist.
              Com $quantos tentativas em 1 segundo na hora $HORA!!" >> /etc/rc.local
           fi
        fi
    done
done
```

Figura 4.5 – Filtro de pacotes

Fonte: Captura de tela Putty

Após a aplicação dessa regra no cenário 2, foram adicionados 87 endereços ips na blacklist, a análise iniciou no dia 22/12/2018 e foi até o dia 29/01/2019. Com essa regra foi possível evitar ataques com tentativas de quebra de senhas oriundas de um mesmo endereço ip. A figura 4.6 demonstra um dos momentos que o atacante envia 126 pedidos de registros em 1 segundo e o endereço ip 87.7.13.157 é adicionado na blacklist.

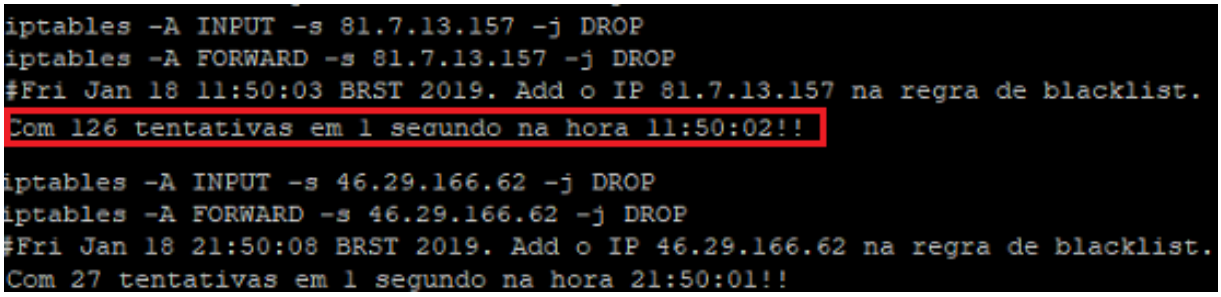


Figura 4.6 – Tentativa de registro

Fonte: Captura de tela Putty

Existem alguns modelos de PABX IP que possuem um *firewall* interno onde há a possibilidade de a central analisar o tipo de pacote recebido e se identificado que se trata de um possível ataque, passa a descartar esses pacotes. Dentro das configurações são definidas a quantidade de tentativas de *login* SIP falhos que o PABX irá aceitar, o período de verificação define um tempo dentro do qual serão analisados os números de logins, caso o número exceda a quantidade de login falho o endereço IP será bloqueado, além de uma *White list*, onde geralmente são informados os endereços IP dos ramais conhecidos que estão registrados na central e dessa forma ficam livres de bloqueio. A figura 4.7, mostra as possibilidades de configurações de bloqueio de um *firewall* interno de um PABX IP.

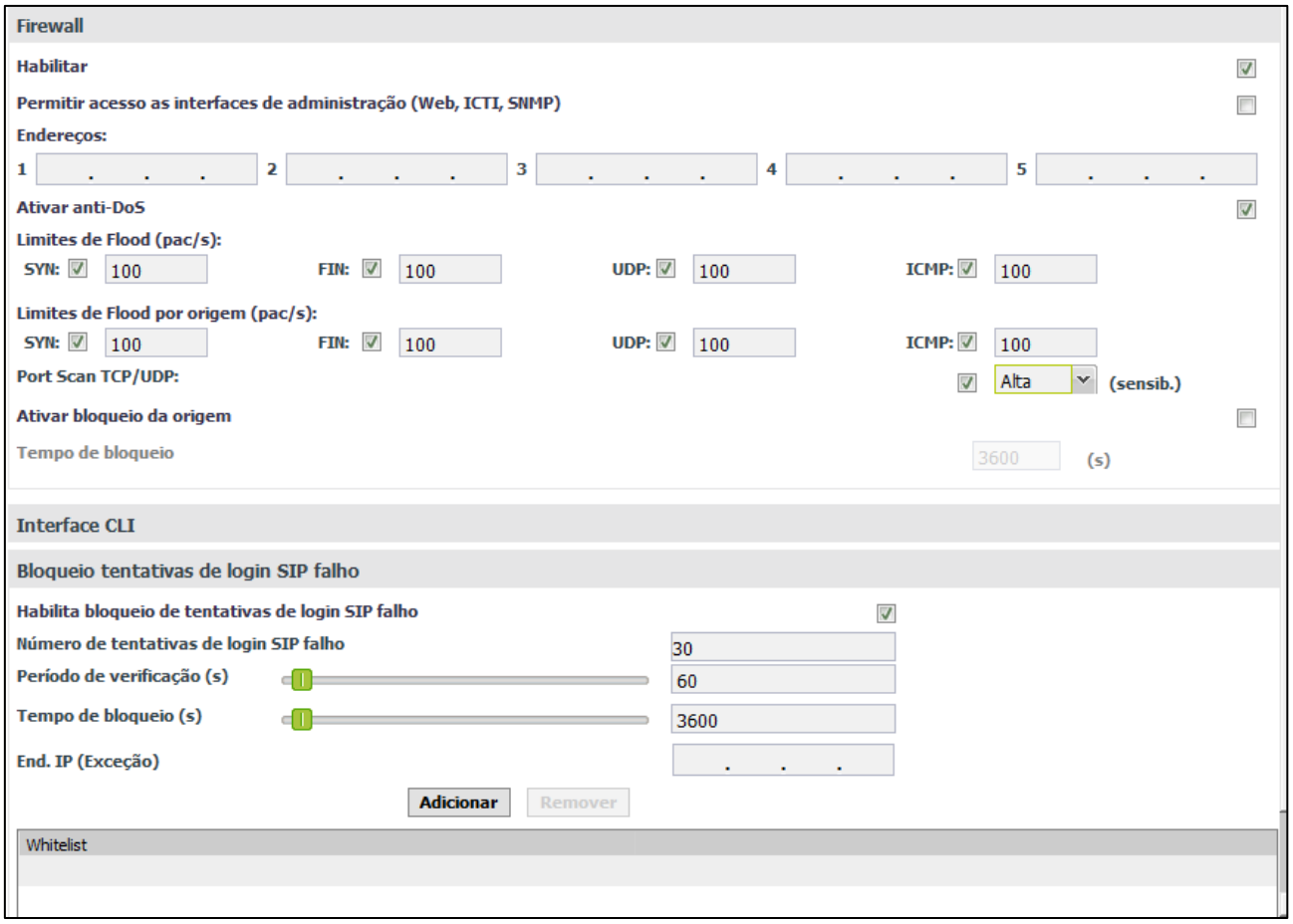


Figura 4.7 - Firewall interno de um PABX IP

Fonte: Captura de tela PABX IP

O recebimento de ataques de negação pode fazer com que o PABX consuma recursos (processamento, memória) para descartar esses pacotes, deixando de atender solicitações legítimas dos usuários da própria central. Por isso, é de grande importância ter um *firewall* que proteja a rede, evitando assim que o PABX consuma recursos desnecessários.

Após ser configurado o *firewall* interno do PABX do cenário 1, notou-se um pacote SIP com o método *REGISTER* proveniente da rede externa com o endereço 51.15.146.34, porém o PABX descarta esse pacote e não envia resposta ao invasor, conforme a figura 4.8.

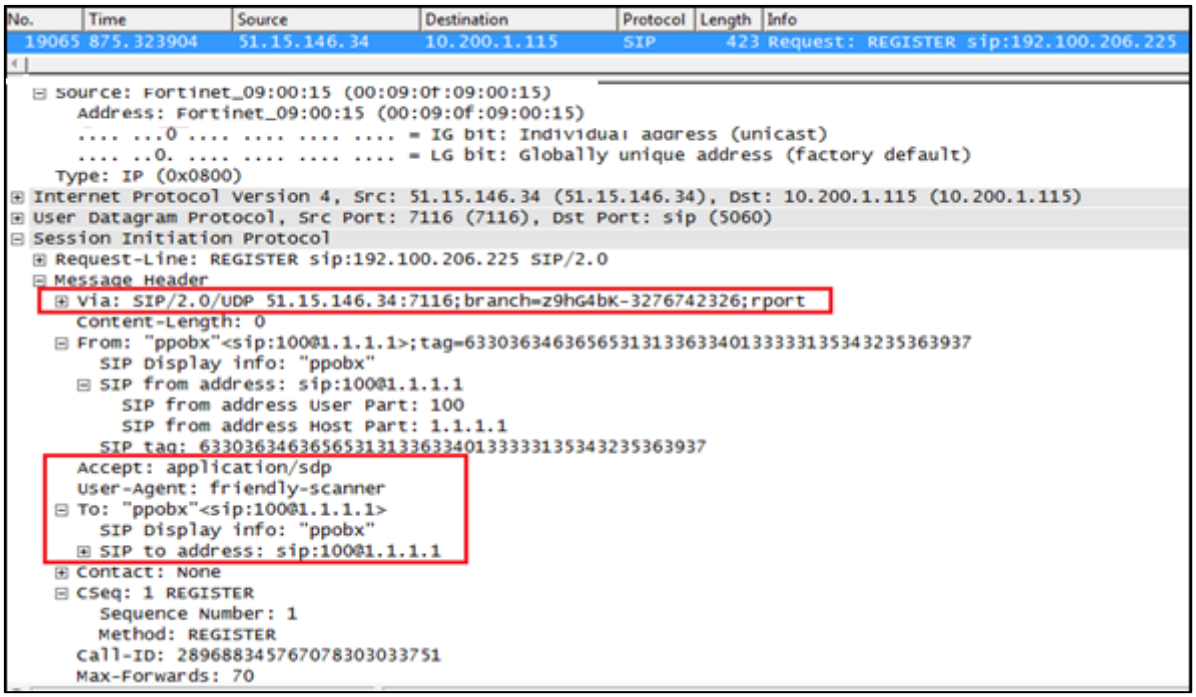


Figura 4.8 – Firewall (cenário 1)

Fonte: Captura de tela Wireshark

Caso o atacante voltasse a tentar ingressar ao PABX com um endereço IP diferente, este pacote não seria bloqueado, já que a análise está sendo realizada através do endereço IP. Uma outra alternativa de bloqueio a esse tipo de ataque, é analisar os campos *User-agent* e *From User*. Um exemplo válido é a verificação estática que a empresa SIPPulse[5] faz no seu sistema, são analisados esses campos nas mensagens recebidas e caso contenham informações iguais as que foram definidas em um script previamente configurado, os pacotes recebidos são descartados e não são encaminhados ao PABX IP.

Com essas verificações, ao receber um pacote SIP contendo no *User-Agent* ou no *From User* as informações sipcli, friendly-scanner, sipvicious, sundayddr, thiisthecanary e ssecuser, a operadora pode optar por não responder esses pacotes. Uma outra verificação estática praticada pela operadora SIPPulse é a análise das origens de pacotes recebidos, caso seja um endereço IP oriundo da Palestina, local que eles não possuem clientes, os pacotes são descartados no mesmo momento. O bloco de rede da Palestina é 37.8.0.0/16.

[5] SIPPulse: empresa de tecnologia voltada ao desenvolvimento para soluções de telecomunicações.

4.4 SIPS (SIP com TLS)

O serviço TLS (*Transport Layer Security*) é implementado em cima da pilha TCP/IP, é um protocolo criptográfico definido pela RFC 2246. É composto de duas camadas, a *TLS Record Protocol* que é responsável por garantir a segurança da conexão e a *TLS Handshake Protocol*, que negocia os parâmetros de segurança a serem utilizados na conexão segura e o algoritmo de encriptação de chaves antes de enviar informações. O uso do TLS faz com que terceiros não possam decifrar as mensagens SIP trocadas entre os equipamentos VoIP. Além disso, é possível autenticar os agentes de usuário por meio de certificados digitais.

Este protocolo garante a segurança nas trocas de sinalização do procolo IP de chamadas, mas não há garantias referente a segurança dos canais de voz (RTP). Para esse tipo de segurança é utilizado o protocolo SRTP. Tanto a configuração do TLS quanto a do SRTP necessita da criação de um par de chaves que são utilizadas pelo telefone IP/*softphone* e pelo PABX IP para criptografar os dados que são trocados entre eles.

4.5 SRTP

Com a finalidade de garantir a confiabilidade da mídia durante uma chamada IP, foi desenvolvido o protocolo SRTP, que é documentando na RFC 3711, cuja as principais características são a confidencialidade e integridade do fluxo de mídia RTP.

A confiabilidade do fluxo de mídia é garantida pela utilização da criptografia dos pacotes transmitidos, antes de qualquer pacote de mídia ser enviado, é realizada uma negociação das chaves criptográficas das partes envolvidas na ligação. Equipamentos que possuem esse recurso proporcionam um nível maior de segurança aos usuários envolvidos na conversação, devido a criptografia que é realizada, evitando assim que o áudio seja escutado caso receba o ataque *Call Eavesdropping*.

4.6 NIDS

Os NIDS (*Network intrusion detection systems*) foram desenvolvidos para sinalizar aos administradores da rede quando alguma indicação de tráfego malicioso é detectada, através de informações contidas nos *payloads* dos pacotes que estão

sendo monitorados. O NIDS deve ser distribuído nos pontos onde passa a maior parte do tráfego. Devido ao fato do sistema de detecção de intrusão baseado em rede serem em tempo real, assegura a vantagem da agilidade para quem gerencia a rede agir.

Tendo conhecimento de todas as contramedidas apresentadas o administrador da rede pode implementá-las visando reforçar a segurança do ambiente VoIP. O NIDS pode ser usado para automatizar o reconhecimento automático de ataques, com base em padrões de mensagens previamente conhecidos. A figura 4.3 também pode ser considerada um tipo de NIDS. Com esse tipo de proteção é possível evitar ataques DoS como SIP Flood, quebra de senha.

A desvantagem de um sistema NIDS é que ele é incapaz de analisar o tráfego criptografado e tem limitações para analisar redes com grande fluxo de dados.

4.7 IPS

Os IPS (Intrusion Prevension System) foram desenvolvidos para fornecer políticas e normas de segurança para o trafego de rede. Possui a capacidade de bloquear qualquer tipo de pacote independente do protocolo utilizado. Suas principais funções são realizar o monitorar o trafego da rede, identificar e gerar alarme com logs de informações suspeitas, além de interromper esse trafego assim que identificado.

No cenário 2 onde foram recebidos 1377 INVITES de servidores mal-intencionados, poderia ter sido evitado o recebimento destes pacotes caso estivesse utilizando IPS. Como todos os INVITES citados constavam na blacklist na página VoipBl, um IPS previamente configurado consultando essa lista de bloqueios em tempo real poderia bloquear as tentativas de chamadas, consequentemente elas não alcançariam o PABX. Na página constam instruções explicando como fazer a instalação/configuração desse script em conjunto do Fail2ban[6].

4.8 VPN

VPN (*Virtual Private Network*) é um túnel seguro entre dois ou mais pontos, que tem por objetivo proteger o tráfego transmitido de possíveis ataques mal-intencionados. Devido ao fato de não passar por redes públicas não confiáveis é uma

[6] Fail2ban: estrutura de software de prevenção de intrusões que protege os servidores de computadores contra ataques de força bruta.

boa alternativa para proteger o tráfego SIP, os dados são encapsulados e criptografados na origem, encaminhados via túnel até o destino onde são descriptografados.

5 CONCLUSÃO

Ao fim deste trabalho pôde-se constatar que foram encontrados indícios de tipos de ataques similares aos que foram apresentados na fundamentação teórica. Não são apenas os ataques em cima de SIP que chegam até os equipamentos, mas também ataques que tem como objetivo acessar remotamente o PABX IP para utilizá-lo para benefício próprio ou até mesmo indisponibilizá-lo.

Através de uma análise minuciosa nos pacotes recebidos de origem duvidosa, pôde-se identificar que em grande parte os campos *From* continham a informação sipvicious e *User-agent* como friendly-scanner, o que levou a uma pesquisa mais aprofundada sobre esses termos, que resultou na descoberta da ferramenta SIPVicious. Essa ferramenta, ao mesmo tempo que pode ser utilizada para atacar intencionalmente um ambiente VoIP, pode utilizar de seus recursos para avaliar o quão suscetível a intrusões está determinado equipamento, podendo assim trabalhar em cima de melhorias no sentido de reforçar a segurança deste. Devido aos recursos disponíveis essa ferramenta foi utilizada no desenvolvimento dessa pesquisa.

Durante os testes realizados em cenários reais, foram monitoradas as interfaces de rede de dois PABX que ficaram expostos a rede externa, ficando assim susceptíveis ao recebimento de pacotes maliciosos provindos da Internet. Notaram-se com maior frequência tentativas de ataques do tipo SIP Flood e Quebra de senha.

Tendo conhecimento de como se deram as tentativas de incursões maliciosas, foi possível definir contramedidas que visam proteger os equipamentos. Dentre as medidas que foram sugeridas estão: troca de porta de escuta SIP, uso de senhas complexas, uso de firewall na rede ou no próprio equipamento VoIP (se este permitir), uso de VPNs, TLS, SRTP e NIDS.

5.1 Trabalhos futuros

Como possibilidades para trabalhos futuros sugere-se:

- Quantificar as ocorrências de ataques a PABX IP, determinando a probabilidade de ocorrência de cada tipo de ataque.

- Propor uma infraestrutura para automatizar o monitoramento de ataques em PABX e sua prevenção automática.
- Ampliar a base de PABX analisados, visando relacionar as melhores práticas para prevenção de ataques.

REFERÊNCIAS

ANTONIAZZI, André Scomazzon. **Segurança em VoIP: Ameaças, Vulnerabilidade e as Melhores Práticas de Segurança**. 2008. 55 f. TCC (Graduação) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, UFRGS, Porto Alegre, 2008.

COONEY, Michael. **Aumentan los ataques cibernéticos a través de VoIP.** 2016. Disponível em: <https://www.networkworld.es/seguridad/aumentan-los-ataques-ciberneticos-a-traves-de-voip>. Acesso em: 21 maio 2018.

FERDOUS, Raihana; LOCIGNO, Renato. **Social Behavior Analysis of VoIP Users and its application to Malicious Users Detection.** Trento: Disi, 2014. Disponível em: <http://eprints.biblio.unitn.it/4267/1/TR-DISI-14-001.pdf>. Acesso em: 04 maio 2018.

FURLAN, Káren Bartholo; SANTOS, Guilherme Rezende dos. **Ataques DDoS.** 5. ed. Santa Rita do Sapucaí: Inatel, 2017.

GOMES, Carlos Francisco Simões. **Gestão da Cadeia de Suprimentos integrada à Tecnologia da Informação.** São Paulo: Thomson, 2004.

JOHNSTON, Alan B. ***SIP: Understanding the Session Initiation Protocol*.** 3. ed. Norwood: Artech House, 2009.

JUNIOR, Márcio de Salles Paiva; JÚNIOR, Mário Ferreira Silva. **Abordagem de segurança em VoIP - SIP.** Santa Rita do Sapucaí: Inatel, 2017.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** Uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013.

MACHADO, Felipe do Nascimento. **SEGURANÇA EM VOIP**: Ameaças aos Sistemas VoIP. 2007. 48 f. Monografia (Especialização) - Curso de Gerência de Redes de Computadores, UFRJ, Rio de Janeiro, 2007.

NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

NET WORK SYSTEMS SOLUTIONS.**Voipblocklist.** Disponível em: <http://www.networksystemssolutions.eu/voipblocklist.php>. Acesso em 08 de fevereiro de 2019.

NOMOTO, Leonardo Juniti; FERREIRA, Mário. **Segurança e Privacidade em redes VoIP.** Santa Rita do Sapucaí: Inatel, 2016.

PORTER, T., GOUGH, M. ***How to Cheat at VoIP Secutity***. Rockland: Syngress Publishing, 2006.

RFC 2543 **SIP: Session Initiation Protocol.** 1999. Disponível em: <https://www.ietf.org/rfc/rfc2543.txt>. Acesso em: 17 maio 2018.

RFC 3261 **SIP: Session Initiation Protocol.** 2002. Disponível em: <https://www.ietf.org/rfc/rfc3261.txt>. Acesso em: 08 mar. 2018.

SANTOS, Valdeci Otacilio dos. **Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008**. Campinas, 2012. Disponível em: <http://repositorio.unicamp.br/handle/REPOSIP/259797>. Acesso em: 25 maio 2018.

SOUTO, André Ribeiro**. A Importância da Segurança Aplicada à Tecnologia VOIP.** 2008. 34 f. TCC (Graduação) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, UFRGS, Porto Alegre, 2008.

TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Elsevier, 2003.

THERMOS, Peter; TAKANEN, Ari. **Securing VoIP Networks:** Threats, Vulnerabilities, and Countermeasures. Boston: Pearson Education, 2007.

VOIP BLACKLIST. **What is Voip BL?** Disponível em: <http://www.voipbl.org/#advanced>. Acesso em: 05 de fevereiro de 2019.

WIKI IFSC SJ. **O protocolo SIP**. Disponível em:

<https://wiki.sj.ifsc.edu.br/wiki/index.php/RMU-2015-1> Acesso em: 13 maio 2018.