CENTRO DE ENSINO SUPERIOR DOM BOSCO
SISTEMAS DE INFORMAÇÃO

AURÉLIO SOUZA MALHEIROS

ANÁLISE DE TRÁFEGO DE REDES : A automação do NMAP para garantia de segurança dos dados

São Luís
2020

AURÉLIO SOUZA MALHEIROS

ANÁLISE DE TRÁFEGO DE REDES: a automação do NMAP para garantia de segurança dos dados

Monografia apresentada ao curso de Sistemas de Informação do Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.
Orientador: Professor Ma. Rafael Cunha

São Luís
2020

Malheiros, Aurélio Souza

Análise de tráfego de redes: a automação do NMAP para garantia de segurança dos dados/ Aurélio Souza Malheiros. __ São Luís, 2020.
64 f.
Orientador: Prof. Ma. Rafael Cunha.
Monografia (Graduação em Sistema de Informação) - Curso de Sistema da Informação – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2020.

l. Automação. 2. Monitoramento. 3. Zabbix - NMAP. I. Título.

CDU 004.7

AURÉLIO SOUZA MALHEIROS

ANÁLISE DE TRÁFEGO DE REDES: A automação do NMAP para garantia de segurança dos dados

Monografia apresentada ao Curso de Sistemas de informação do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Sistemas de informação.

Aprovada em: _____/____/_____.

BANCA EXAMINADORA:

_____

Prof. Me. Rafael de Souza Cunha (Orientador)

Mestre em Engenharia de Eletricidade

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

_____

Prof. Me. Allison Jorge Silva Almeida

Mestre em Engenharia de Eletricidade com ênfase em inteligência artificial

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

_____

Prof. Me. Allan Kássio Beckman Soares da Cruz

Mestre em Design

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB)

“Desonesto é aquele que diz adeus quando a estrada escurece” - Disse Gimli (TOLKIEN, P. 345, 1991).

AGRADECIMENTOS

Agradeço a minha família, por todo suporte e auxílio nos momentos difíceis no desenvolvimento deste trabalho e no decorrer do curso de graduação, se não fosse por ela talvez não finalizaria o curso de sistemas de informação.

Agradecer a minha mãe, irmã e noiva, pela ajuda financeira e psicológica, pois por conta dessas três mulheres maravilhosas que fazem parte da minha vida, consegui concluir esse trabalho mesmo com toda dificuldade, que onde muita das vezes pensei em desistir.

Aos grandes amigos que conquistei nesses anos de jornada acadêmica, Sisnando, Enderson, Tarcisio, Marcelo, Gabriel, ao meu grande amigo Leonardo Viana e principalmente a minha companheira Ana Carolina espero que todos façam história em suas carreiras e possam usufruir dos conhecimentos adquiridos na UNDB.

Agradecer também aos professores Rafael Cunha e Maurício Moraes que auxiliaram na elaboração deste trabalho, graças a vocês consegui desenvolver cada dia melhor o meu projeto, obrigado também pelas críticas construtivas foram graças a elas que conseguir melhorar cada dia mais o meu trabalho. Mas também venho parabenizar por todo corpo docente que auxiliou a grande maioria dos alunos da instituição.

RESUMO

A segurança da informação, é um dos temas mais comentados do mercado da tecnologia da informação (T.I.), para se garantir a segurança dos ativos de rede de alguma instituição, é aplicado diversos métodos onde cada um deles tem uma característica diferente, porém a finalidade é a mesma garantir que não ocorra vazamento dos dados ou perda de informação por conta de criminosos. Essa necessidade de melhorar a segurança em um ambiente corporativo, é uma obrigação e responsabilidade dos administradores de rede. Este projeto, tem por objetivo de apresentar a automação do uso de uma ferramenta de segurança para fazer o mapeamento de serviços de rede, com isso dando maior facilidade na administração do ambiente monitorado. A proposta do trabalho foca também em integrar o NMAP com o Zabbix com intuito de analisar o ambiente monitorado pelo administrador de rede, fazendo com que não seja necessário o mesmo analisar as vulnerabilidades existentes no ambiente. O ambiente de homologação, tem ainda o intuito de apresentar testes práticos da integração entre as duas tecnologias, apresentando a simplicidade da configuração do NMAP em um sistema de monitoramento, além disso mostra uma solução viável para verificação de vulnerabilidade em qualquer empresa, sem que seja necessário verificação de todos ativos de rede de forma manual, já que, o monitoramento entregará esse serviço.

Palavras-chave: Automação, monitoramento, Zabbix, NMAP, redes

ABSTRACT

Information security is one of the most talked about topics in the information technology (IT) market, in order to guarantee the security of the network assets of some institution, several methods are applied where each one of them has a different characteristic, but the purpose it is the same to ensure that there is no leakage of data or loss of information due to criminals. This need to improve security in a corporate environment is an obligation and responsibility for network administrators. This project aims to present the automation of using a security tool to map network services, thereby making it easier to manage the monitored environment. The work proposal also focuses on integrating NMAP with Zabbix in order to analyze the environment monitored by the network administrator, making it unnecessary to analyze the vulnerabilities existing in the environment. The approval environment also aims to present practical tests of the integration between the two technologies, presenting the simplicity of configuring NMAP in a monitoring system, in addition to showing a viable solution for vulnerability checking in any company, without it being verification of all network assets is necessary manually, since monitoring will deliver this service.

Keyword: Automation, monitoring, Zabbix, NMAP, networks

LISTA DE FIGURAS

LISTA DE QUADROS - TABELAS

LISTA DE ABREVIATURAS E SIGLAS

T.I.	Tecnologia da Informação
NMAP	*Network Mapper*
WWW	*World Wide Web*
LAN	*Local Area Network*
IEEE	Instituto de engenheiros eletricistas e eletrônicos
VLAN	*Virtual Local Area Network*
WAN	*WIDE AREA NETWORK*
OSI	*Open Systems Interconnection*
ISO	*International Organization for Standardization*
IANA	Autoridade de números atribuídos
SSH	*Secure Shell*
VPN	*Virtual private network*
UDP	*User Datagram Protocol*
TCP	*Transmission Control Protocol*
SNMP	*Simple Network Management Protocol*

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação é um tema debatido nos ambientes empresárias e cada dia traz consigo melhorias e regras que devem ser aplicadas. Com isso, os profissionais de Tecnologia da informação (T.I.) devem está preparados para novos tipos de ataques ou mesmo modelos de segurança mais eficazes, já que, o intuito é garantir a segurança dos dados das instituições no qual são sendo administradas.

Uma das tecnologias utilizadas na área da segurança da informação é o *Network Maper* (NMAP) desenvolvida por Lyon (2002) e tem como principal objetivo, escaneamento de portas, descobertas de sistemas operacionais, descobertas de redes entre outros objetivos. Além disso é uma tecnologia que está em melhoria contínua, ou seja, sempre é feito novas melhorias.

No seguinte trabalho, será apresentado também a automação do NMAP para garantir precisão e redução de erros ao analisar os dados pelos profissionais que a utilizam. Lyon (2002) descreve a ferramenta como algo simples de ser utilizado, entretanto muitas das vezes ela se torna complexa pela quantidade de parâmetros (opções) que podem ser utilizadas e com isso muitas das vezes existe a necessidade de automatizar e além disso melhorar a visualização dos dados que estão sendo entregues pelo NMAP.

Segundo Silva (2003), prevenir as empresas de qualquer tipo de ataque é a melhor forma de reduzir a concretização de alguma ameaça existente no mercado, dessa forma podemos perceber que o principal objetivo é se antecipar em relação as vulnerabilidades dentro de um ambiente empresarial. Portanto, o profissional que compreende isso poderá ser mais eficaz na garantia da segurança dos dados na empresa no qual administra.

O trabalho será implantado fazendo o uso da ferramenta de monitoramento Zabbix junto com o NMAP, dessa forma podemos monitorar as vulnerabilidades do ambiente em tempo real. Além disso, será aplicado tanto em ambiente de teste que será um laboratório, quanto em uma empresa que trabalha como gerenciamento de ambientes empresariais, entretanto os dados serão reais, mas nomes e algumas informações vão ser fictícias para proteger os dados da organização.

Portanto, apresentar novas formas de segurança da informação é algo de suma importância para o nosso cenário atual, já que, as tecnologias (*Firewall, Switches,* Sistemas operacionais, ERPs, entre outros) estão evoluindo cada vez mais com intuito garantir melhorias nos ambientes empresariais e com isso a complexidade desses ambientes também vem crescendo, ou seja, implementar formas que dão precisão e velocidade na tomada de decisão são de grande ajuda para os profissionais de TI.

1.1 Problemática

A compreensão do administrador de redes de computadores sobre ferramentas de análise de redes para conseguir solucionar problemas de forma simples e saber identificar vulnerabilidades no ambiente onde é administrado. Isso pode evitar que dados ou informações vazem e, com isso tragam prejuízos para instituição.

Existem algumas ferramentas que podem ser utilizadas para auxiliar os administradores de redes para detectar essas vulnerabilidades, uma das quais podemos mencionar é o *Network Maper* (NMAP), que é um *port scan*, o mesmo dá a capacidade de descoberta de quais serviços, portas e sistemas operacionais que estão dentro de uma faixa de rede específica. Melo (2017), explica que o simples fato de um criminoso descobrir qual sistema operacional utilizado dentro de um ambiente já é considerado uma vulnerabilidade, pois isso abre a possibilidade de uma análise das vulnerabilidades daquele sistema específico.

Como podemos perceber, essa ferramenta tem um grande valor significativo para qualquer profissional, entretanto o procedimento de análise, muita das vezes, é cansativo, demorado e complexo. Portanto, questiona-se de que forma a automatização do NMAP pode reduzir as vulnerabilidades dentro de um ambiente empresarial?

1.2 Justificativa

Como já foi citado o NMAP é uma ferramenta utilizando para o escaneamento de portas e com ele podemos descobrir qual o sistema operacional está rodando dentro de um servidor, ou então, podemos descobrir qual *Switch* ou *firewall* que estão sendo utilizados dentro de uma empresa. Mota Filho (2013) afirmar que a partir do momento que um criminoso possui essas informações ele já pode procurar as vulnerabilidades existentes e com isso implementar os ataques.

Dessa forma, o cuidado com a gestão dessas informações demonstra que os profissionais não só devem, compreender como funciona o ambiente no qual estão administrando, mas também terem informações precisas onde consigam compreender tudo o que foi passado, com isso procurarem uma solução para tal problema, ou seja, automatizar o NMAP para que os administradores de rede consigam saber as vulnerabilidades dá a possibilidade de conseguir prevenir as empresas de possíveis ataques.

Além disso, é possível perceber que as formas como ocorre os ataques no mundo cibernético evolui cada vez mais rápido e as tecnologias aplicadas para proteção (Antivírus, *Firewalls* entre outros) em um determinado momento podem se tornar algo ineficaz. E com

isso tornar a instituição vulnerável podendo fazer com que percam seus dados. Portanto, implementar a automatização do NMAP é de suma importância para os profissionais de TI, com isso podem ter outras possibilidades para descobrir as vulnerabilidades nos seus ambientes.

2 OBJETIVOS

Diante do problema apresentado em questão, será apresentado os objetivos deste trabalho e com isso uma hipótese a ser pesquisada, os objetivos gerais e o específico, onde levarão o direcionamento para solucionar o problema apresentado.

2.1 Objetivos Geral

Automatizar o uso do NMAP para efetuar a análise de vulnerabilidades dentro de ambientes empresariais.

2.2 Objetivos Específicos

a) Apresentar o uso do NMAP para ambientes corporativos;
b) Utilizar o NMAP para evitar vulnerabilidades dentro dos ambientes empresariais;
c) Automatizar o uso do NMAP para auxiliar os profissionais de T.I..

3 FUNDAMENTAÇÃO TEÓRICA

Os conceitos abaixo são referentes as teorias e tecnologias que serão aplicadas no desenvolvimento desse projeto, onde são relacionados a rede de computadores, *port scaners*, análise de tráfego de redes, linguagem de programação, automação de tarefas e segurança da informação.

3.1 Redes de Computadores e suas aplicações

Redes de computadores tem uma relevância no mercado, tanto do ponto de vista doméstico quanto empresarial. As pessoas fazem o seu uso para fazer pagamentos, se comunicar, interconexão entre empresas, entretenimento, entre outros procedimentos. Com isso, podemos perceber que existe uma grande quantidade de processamento de dados e além disso informações de suma importância para as pessoas que as utilizam.

Tanenbaum (2011), descreve em sua obra a existência de diversas aplicações do mercado, as comerciais onde é explicado sobre o compartilhamento de recursos, por exemplo, servidores, onde os arquivos que são utilizados dentro da instituição ficam armazenados nele e com isso as informações ficam centralizadas, logo a sua manutenção e utilização é mais simples.

O autor descreve também que após o surgimento de World Wide Web (WWW), as pessoas fazem o uso de computadores dentro de suas residências principalmente para obter informações. É comentado em sua obra sobre os jornais que vem fazendo suas publicações na internet e com isso as pessoas podem ter acesso as informações de forma mais rápido e além disso ter uma grande variedade de informações sobre um determinado assunto. Porém com sua evolução podemos perceber que os usuários desses dispositivos vem utilizando para entretenimento e até mesmo comércio eletrônico.

Outro ponto que é perceptível é a existência da tecnologia móvel, onde é retratado na obra do autor sendo explicado que os usuários dessa tecnologia utilizam principalmente para troca de mensagens. Tanenbaum (2011), cita alguns setores onde é útil, como podemos ver abaixo:

a) Militares, onde muitas das vezes não é possível montar toda uma infraestrutura para eles, com isso fazem o uso de dispositivos móveis;
b) Taxistas, podem visualizar onde o seu cliente está ou mesmo receber algum atendimento via mensagem de algum aplicativo.

Portanto, podemos perceber as diversas aplicações das redes de computadores e que muitas das vezes não precisa de uma infraestrutura para existência de uma rede. Além

disso, é possível perceber que a aplicação das redes de computadores pode ser vista em diversos ambientes, sem empresariais ou mesmo para uso doméstico, onde grande maioria tem a finalidade de troca de informações.

Apresentamos até o momento o que seriam as aplicações das redes de computadores, porém vamos apresentar agora o que são elas, para Kurose (2013) são dispositivos finais conectadores com intuito de serem feitas comunicações entre esses dispositivos, abaixo temos um trecho da sua obra:

> A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente PCs de mesa, estações de trabalho Linux, e os assim chamados servidores que armazenam e transmitem informações, como páginas da Web e mensagens de e-mail. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede. (KUROSE, 2013, p. 3).

Dessa forma podemos perceber no momento que fazemos a comunicação entre dispositivos com intuito de transmitir dados já podemos considerar que os mesmos estão em uma rede de computadores. Esses dispositivos podem estar conectados por meio de enlace (cabos, fios de cobre, ondas de rádio, entre outras formas) e também por meio de roteadores ou *switches*, onde cada um deles tem uma característica específica. Os roteadores e *switches* são conhecidos também como comutadores de pacotes eles são responsáveis por enviá-los para os seus destinos finais.

Logo, podemos perceber que a rede de computadores estão em todos os locais, os mensageiros instantâneos que as pessoas utilizam, o pagamento de suas contas, dentro as suas casas para acessar sites e isso podemos perceber principalmente com o advento dos dispositivos móveis, pois traz ainda mais dispositivos conectados a rede.

3.1.1 Internet

Já explicamos sobre os equipamentos de rede e como eles funcionam dentro de um ambiente, porém existem outros pontos a serem explicados antes mesmo de compreendermos o que seria a internet é necessário falarmos sobre como tipos de rede são utilizados e além disso explicar como ela chega nas empresas e residências.

Tanenbaum (2011), explica que as redes locais são utilizadas em ambientes residenciais ou mesmo em ambientes empresariais. Outro nome para esse tipo de rede é *Local Area Network* (LAN). Um exemplo de seu uso é quando queremos fazer com que um notebook possa se comunicar com um servidor com intuito de acessar os arquivos presentes nele, logo podemos perceber que o objetivo desta comunicação é compartilhar recursos.

O autor explica que dentro das redes LAN elas são divididas em dois tipos, com fio que utiliza tecnologia de fio de cobre ou mesmo fibra óptica e as sem fio utilizam o padrão IEEE 802.11 também conhecido como Wifi, onde é ums dos mais populares no mercado, podendo conectar diversos usuários com apenas um equipamento (AP, roteador Wifi ou mesmo repetidor de sinal).

Com isso, as redes de computadores para ambientes empresariais ou domésticos são úteis para que as pessoas possam tanto compartilhar recursos quanto ter acesso à internet, porém para locais domésticos as redes LAN são bem mais simples onde geralmente é encontrado apenas um roteador com tecnologia Wifi ou mesmo alguns cabos rede. Quando precisamos montar uma rede empresarial podemos fazer o uso de equipamentos como *Switches* e criar redes virtuais.

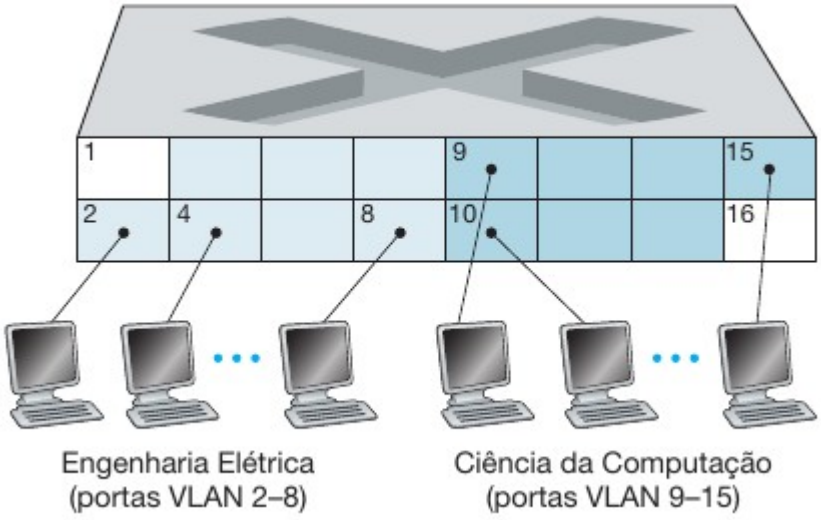
Tanenbaum (2011), também explica que esses equipamentos geralmente são aplicados quando precisamos de mais pontos de rede ou até fazer uma divisão da rede física em redes menores e isso é muito comum em empresas. Kurose (2013), explica que quando estamos trabalhando com locais onde é requer uma certa velocidade e praticidade deve-se fazer o uso de *Virtual Local Area Network* (VLAN).

Kurose (2013), descreve que as VLANs são utilizadas principalmente para separar setores dentro de uma empresa, por exemplo, existem 10 computadores que são utilizados pela gerência e 20 utilizados pelo setor administrativo, podemos separar os setores criando VLANs, ou seja, funciona como se os equipamentos estivessem conectados em *Switches* separados. Abaixo temos uma descrição mais detalhada:

> Como o nome já sugere, um comutador que suporta VLANs permite que diversas redes locais virtuais sejam executadas por meio de uma única infraestrutura física de uma rede local virtual. Hospedeiros dentro de uma VLAN se comunicam como se eles (e não outros hospedeiros) estivessem conectados ao comutador. Em uma VLAN baseada em portas, as portas (interfaces) do comutador são divididas em grupos pelo gerente da rede. (KUROSE, 2013, p. 357).

Os comutadores citados pelo autor é o mesmo que *Switche* além disso o autor explica como funciona uma VLAN. Dentro dos ambientes empresariais é de suma importância aplicarmos essa tecnologia, isso garante uma segurança e melhor gerência do ambiente, pois podemos limitar quem pode se comunicar com determinados dispositivos na rede e quais setores podem trocar informações. Na figura 1 retirada da obra do autor podemos verificar como funciona a separação dos setores.

Figura 1 - Dois setores separados dentro do Switche



Fonte: Kurose (2013)

Além da LAN existem também as redes *Wide Area Network* (WAN), enquanto as LANs estão localizadas geograficamente no mesmo local (casa ou sala), as WAN estão localizadas em locais, por exemplo, prédios ou até mesmo cidades diferentes. Tanenbaum (2011) afirma que são um conjunto de redes interconectadas além disso descreve a WAN como algo parecido com a LAN porém em um tamanho bem maior.

Kurose (2013), também comenta sobre os provedores de serviço de rede são eles que entregam a internet para os clientes (escritórios ou residências) e com isso esses locais tenham a acesso à internet, pois ele garante a comunicação das redes LAN com as redes WAN e dessa forma fazer os clientes terem acesso à internet. Abaixo temos uma explicação mais detalhada:

> Sistemas finais acessam a Internet por meio de Provedores de Serviços de Internet (Internet Service Providers — ISPs), entre eles ISPs residenciais como empresas de TV a cabo ou empresas de telefonia; corporativos, de universidades e ISPs que fornecem acesso sem fio em aeroportos, hotéis, cafés e outros locais públicos. Cada ISP é uma rede de comutadores de pacotes e enlaces de comunicação. ISPs oferecem aos sistemas finais uma variedade de tipos de acesso à rede, incluindo acesso residencial de banda larga como modem a cabo ou DSL (linha digital de assinante), acesso por LAN de alta velocidade, acesso sem fio e acesso por modem discado de 56 kbits/s. ISPs também fornecem acesso a provedores de conteúdo, conectando sites diretamente à Internet. Esta se interessa pela conexão entre os sistemas finais, portanto os ISPs que fornecem acesso a esses sistemas também devem se interconectar. (KUROSE, 2013, p. 3).

Portanto, podemos afirmar que a internet é um conjunto de sistemas de *software* e *hardware* conectados e se comunicando com intuito de garantir o compartilhamento de recursos e entrega de dados. E para existir a internet também deve haver a existência de

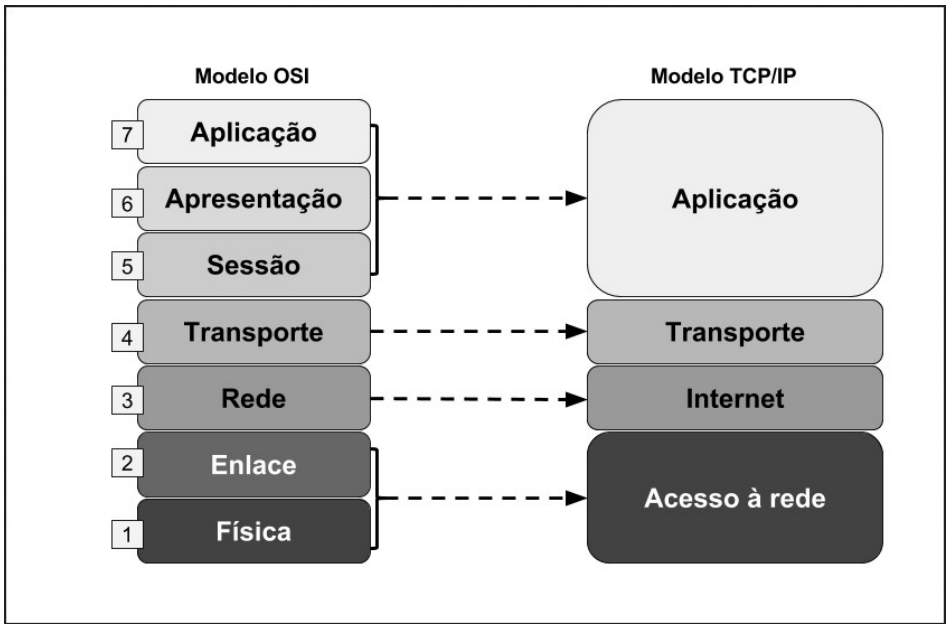
diversos itens que foram apresentados, como as redes LAN, WAN e os provedores de serviço de redes (ISPs), onde o último é que garante que as instituições e residências sejam capazes de ter acesso à rede mundial de computadores.

3.1.2 Modelo OSI e TCP/IP

Em redes de computadores existem diversos protocolos e até mesmo padrões que devem ser seguidos pelas empresas fabricantes dos equipamentos de rede, isso é uma forma de garantir que os sistemas computacionais possam se conversar sem que exista problemas relacionados a compatibilidade. Com isso, foram surgindo alguns modelos onde um deles é o TCP/IP utilizado para padronizar a rede de computadores.

Mota Filho (2013), explica que compreender o modelo OSI é uma das partes mais importantes do estudo sobre redes de computadores, pois nele que é descrito como deve ocorrer o funcionamento dos dispositivos e como os protocolos de rede devem trabalhar. Em sua obra o autor apresenta somente o modelo OSI e afirma que o entendimento dele suficiente para compreendermos redes de computadores, além do mais que o modelo TCP/IP tem basicamente o mesmo objetivo do modelo OSI, porém a quantidade de camadas é inferior como mostra na figura 2.

Figura 2 - Modelo OSI e TCP/IP



Fonte : Caetano (2016)

Felippetti (2017), afirma que essa falta de padronização fazia com que as empresas tivessem que aderir a somente a um fabricante ou mesmo que não conseguissem ter sucesso na implementação de uma nova tecnologia na sua empresa e com isso ficavam presos ao mesmo fabricante. Isso acontecia, pois a instituições que vendiam equipamentos de rede criavam protocolos “proprietários” isso significa que só pode ser utilizado por aquele fabricante.

O autor também explica que na década de 80 a *International Organization for Standardization* (*ISO)* vendo esses problemas organizou um grupo de pesquisadores para desenvolver uma forma de padronizar as redes de computadores e com isso surgiu o modelo *Open Systems Interconnection* (OSI), portando criando a padronização na transmissão, formatação, recebimento, envio e interceptação de dados entre dispositivos de rede.

Porém o autor apresenta também o modelo TCP/IP não tão respeitado na época quando o OSI, já que, não era tão bem estruturado e não tinha instituições que financiaram e implementavam suas documentações e melhorias. Entretanto o modelo TCP/IP era muito mais flexível que OSI e além disso trazia consigo uma simplicidade que não é vista no OSI. Os dois modelos são divididos em camadas onde cada uma delas representa dispositivos ou protocolos de rede e como eles devem funcionar.

3.1.3 Gerenciamento da segurança em redes de computadores

O mercado de T.I. (Tecnologia da informação) vem sempre buscando novas formas de garantir a segurança dos dados dos usuários e sistemas computacionais, entretanto da mesma forma criminosos buscam novas formas de burlar esses sistemas com intuito de roubar esses dados. Tanenbaum (2011), afirma que a segurança da informação tornou-se uma das maiores preocupações do mercado de T.I., logo é onde as instituições mais se motivam a melhorar.

O autor afirma que a segurança da informação tenta garantir que os dados não sejam modificados ou até mesmo visualizados por pessoa que não tenham autorização para tal procedimento, ou seja, é necessário se preocupar com tudo o que acontece no ambiente, isso é uma forma de garantir que os dados não sejam violados.

Dessa forma, podemos compreender que a segurança da informação pode abranger inúmeros tipos de problemas e também deve estar presente em todos os setores das instituições, por exemplo, o simples fato dos colaboradores compartilharem a senha de e-mail ou de usuário pode ser considerado uma falha de segurança e pode causar sérios problemas dentro de qualquer ambiente empresarial, além disso segundo Mota Filho (2013) alguns

ataques podem partir de dentro do ambiente, podendo ser feito por funcionários da própria instituição.

Dentro dos ambientes de rede existem diversos equipamentos ou sistemas que são capazes de garantir a segurança de uma empresa, um que podemos citar aqui são os Firewalls que segundo Mota Filho (2013), ele pode ser físico ou lógico e tem como principal objetivo garantir a segurança do ambiente, onde todo o tráfego deve passar por ele para que ele possa analisar e efetuar uma ação para os pacotes e requisições feitas no ambiente.

> Um dos mais importantes princípios para implementação de firewalls é o da defesa em profundidade. Em sistemas de firewalls, a defesa em profundidade agrega segurança, pois, como já foi visto, a existência de vários serviços na mesma máquina aumenta a possibilidade de intrusão. Por exemplo, uma máquina contendo um filtro de pacotes e um detector de varreduras de portas TCP/UDP abertas poderá ser ultrapassada caso o referido detector esteja vulnerável a uma intrusão. Com isso, o filtro de pacotes ficará inerte, não conseguindo atuar. (MOTA FILHO, 2013, p. 353).

Portanto podemos perceber que a implementação de um firewall dentro de um ambiente empresarial pode reduzir as vulnerabilidades do ambiente, logo que mesmo em pequenas empresas é possível visualizar diversos sistemas (Banco de dados, Sistemas operacionais, ERPs, entre outros), onde cada um deles tem um valor para instituição. Entretanto devemos lembrar que cada ambiente vai necessitar de uma implementação de segurança diferente onde vai depender do ambiente no qual será implantado.

Mota Filho (2013), também descreve os detectores de varredura de portas, são utilizados para evitar informações sobre os serviços implantados dentro de uma empresa e com isso conseguir efetuar um ataque remoto. Os sistemas de varreduras de portas (*port scans)* são utilizados para detectar quais portas estão abertas no ambiente e com isso ser possível descobrir quais serviços estão rodando no local.

3.2 Segurança da informação

Uma das maiores preocupações do mercado de T.I. (Tecnologia da informação) é em relação a segurança da informação, sendo um ponto crucial para qualquer ambiente empresarial, onde se faz necessário garantir que os dados não estejam em mão de pessoas não autorizadas, com isso garantir que todas as informações de uma instituição estejam realmente seguras e além disso, preservar todas as informações estejam disponíveis a todo momento quando se for necessário.

3.2.1 Confidencialidade Integridade Disponibilidade

Compreender os conceitos utilizados na segurança da informação é uma garantia que todo o processo de segurança de uma organização realmente esteja alinhada com os protocolos e com a organização internacional de normalização (ISO), reduzindo assim possíveis riscos as mesmas.

Devemos compreender também os principais elementos da segurança da informação que são aplicados em qualquer instituição que tenha uma gestão de segurança de informação, Torres (2015) descreve a confidencialidade, integridade e disponibilidade (CID) que são os pilares da segurança da informação, entretanto também são conhecidos como os princípios básicos.

O autor também descreve em sua obra os princípios, onde o primeiro que vamos descrever é a confidencialidade que é uma forma de garantir que só pessoas autorizadas podem ter acesso as informações ou dados de um determinado serviço ou dados, podendo ele estar dentro de um servidor ou mesmo sendo transmitida na rede. Essa confidencialidade, pode ser garantida por meio de criptografia ou mesmo um controle de acesso para validar quais pessoas devem ter acesso aos dados.

Hintzbergen (2018), afirma que a integridade é garantia que toda e qualquer informação não vão ser alteradas de forma indevida seja ela acidental ou mesmo proposital, caso ocorra é considerado uma violação dos dados, ou seja, é uma forma de certificar que os dados não sejam violados ou excluídas mesmo sendo proposital ou acidental. Formas de garantir isso, é validar se realmente é possível inserir determinado dado ou modifica-lo, ter um sistema de capaz de armazenar as ações dos usuários (*logs)* para definir quem fez as alterações e quando foram feitas.

Por fim, temos a disponibilidade é a parte que expõe que os dados e serviços devem estar disponíveis a qualquer momento para pessoas autorizadas, para o autor a disponibilidade tem três características básicas a informação está disponível quando necessário ser feito seu uso, caso ocorra algum problema ou mesmo falha nos sistemas será possível acessa as informações e por último deve ser suficiente para que a equipe possa trabalhar.

Portanto, podemos compreender que a segurança da informação é uma forma de garantir que somente pessoas autorizadas tenham acesso aos serviços e informações, que a todo momento esteja disponível para essas pessoas e além disso atestar que só seja possível alterar os serviços quando for realmente necessário alterar e fora isso deve confirmar que as pessoas que estão alterando estejam realmente autorizadas para fazer esse procedimento.

3.2.2 Ativos de informação

Dentro das instituições temos itens de grande valor, por exemplo, planilhas do excel, um banco de dados ou mesmo um simples arquivo de texto contendo algumas senhas. Marciano (2006) afirma que todo e qualquer item dentro de uma empresa pode ser considerado um ativo de informação, isso acontece pelo fato de que qualquer item pode gerar um impacto na segurança da informação do ambiente empresarial.

Na figura 3 que foi retirada da obra de Torres (2015) deixa bem claro o que são os ativos de informação e quem são os ativos de informação. Não podemos esquecer de mencionar sobre o que os ativos podem ficar sujeitos e como é dividido as categorias desses acontecimentos.

Figura 3 - Ativos de informação

Fonte : Torres (2015)

Um outro ponto importante é compreender as categorias que os ativos de informação se dividem, sendo três categorias: ameaças, vulnerabilidades e incidentes, o autor comenta sobre a preocupação ou falta dela em relação a esses itens e descreve cada um deles em sua obra.

O principal elemento que as instituições devem se proteger é das ameaças e o foco delas são os agentes, mas podem ser pessoas, software, informações, entre outros. Ele também comenta a existência de dois tipos de ameaças as acidentais que pode ser um erro no desenvolvimento de um software ou mesmo propositais, por exemplo, invasão de um sistema bancário. Entretanto devemos deixar claro que ameaça é tudo o que pode causar danos nos ativos de informação, um exemplo que podemos citar é um desastre natural que atinge uma determinada empresa e com isso destruindo os ativos de informação.

Vulnerabilidades, é descrito pelo Torres (2015) como falhas propositais e não propositais, podendo gerar diversos problemas como informações não confiáveis ou até

mesmo não gerar as informações. O grande problema das vulnerabilidades podem ser exploradas por uma ameaça e com isso conseguindo concretizar um ataque.

Por fim, temos o incidente que é quando um dos três pilares da segurança da informação são atingidos e com isso causando eventos indesejados para uma empresa. Abaixo temos um trecho da obra de Torres (2015), onde ele define de forma a clara o que seria um incidente:

> Conforme exposto na ISO/IEC TR 18044:2004, um incidente pode ser entendido por "um simples ou uma série de eventos de segurança da informação indesejadas ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação". Ou seja, eventos de segurança indesejados que violem algum dos principais aspectos da segurança da informação (Confiabilidade, integridade, disponibilidade, dentre outros). (TORRES, 2015, p. 16)

Dessa forma, quando um ou mais eventos infringem a segurança da informação de um ambiente é quebrado um ou todos os pilares e com isso causando prejuízos muita das vezes irreversíveis.

Logo, compreender o funcionamento da segurança da informação é relevante para darmos continuidade aos serviços de T.I. de uma empresa e com isso garantimos também que dados não sejam violados ou mesmo utilizados por pessoas não autorizadas, a título de exemplo, podemos comentar sobre uma falha de segurança que pode ser encontrada dentro dos ambientes empresariais no qual seria a descoberta de rede, bastando apenas utilizar softwares de *scan ports* para descobrir as portas que estão abertas dentro de um *firewall* ou mesmo em um servidor web. Se um profissional de segurança da informação consegue antecipar-se em relação a isso ele evita que tais informações fiquem nas mãos de pessoas não autorizadas.

3.3 NMAP

Existem algumas ferramentas que podem ser utilizadas para o escaneamento de portas e uma das mais conhecidas é o NMAP que segundo Lyon (2009) a ferramenta foi lançada no ano de 1997 e tinha como principal objetivo se consolidar no mercado de *scanners* de porta e exame de redes e segurança de um ambiente, a mesma é de código aberto e na época só era possível ser utilizada em sistemas operacionais GNU/Linux.

O autor descreve de forma detalhada as funções que foram adicionadas até o ano de 2019, onde cada uma delas deve ser aplicada em uma ocasião diferente, por exemplo, o NMAP tem funções específicas para detectar qual o sistema operacional do host ou então quais os serviços instalados em um determinado servidor, além disso é possível encontrar a ferramenta para as plataformas Unix, Windows, Mac OS e GNU/Linux.

Podemos perceber que essa tecnologia vem evoluindo ao longo dos anos e com isso vem sendo utilizada cada vez mais por administradores de redes, principalmente pelo fato de ser muito bem documentada, além disso a sua popularidade fez aumentar a quantidade de membros de sua comunidade, logo traz consigo novos adeptos trazendo novas melhorias para a ferramenta, já que, a mesma é de código aberto.

Entretanto Lyon (2009), descreve que da mesma forma que traz grandes vantagens para usuários mais experientes pode trazer grande dificuldades para os que não dominam muito bem o mundo da rede de computadores, logo os mesmos sentem dificuldades para trabalhar e até mesmo compreender o seu funcionamento. Onde o autor afirma que algumas de suas funcionalidades não foram ainda documentadas, porém ele detalha as principais funções existentes no NMAP.

Mas da mesma forma a documentação do NMAP deixa claro que o seu público-alvo é qualquer amante da tecnologia da informação, principalmente quando o assunto é segurança da informação, ou seja, pode ser útil tanto para novatos quanto para usuários avançados que tem por intuito fazer algum teste de segurança no ambiente no qual faz a administração. Contudo é necessário ter conhecimento na pilha TCP/IP e redes de computadores, já que na obra não é comentado com detalhes esses assuntos.

3.3.1 Exame de portas

Antes de entendermos o que é o exame de portas é necessário compreendermos o que seria uma porta qual a função dela. Podemos apresentar a explicação do Lyon (2009) sobre o que seria uma porta:

> Portas são, simplesmente, uma abstração de software, usada para distinguir entre canais de comunicação. Similares à forma com que os endereços IP são usados para identificar máquinas nas redes, as portas identificam aplicações específicas em uma única máquina. Por exemplo, seu navegador web, por omissão, se conectará à porta TCP 80 de máquinas em URLs HTTP. Se você, em vez disso, especificar o protocolo seguro HTTPS, o navegador tentará a porta 443, por omissão. (LYON, 2009, p. 115).

Portanto, funcionam como endereços virtuais de serviços utilizados em desktops ou servidores com intuito de identificar onde os serviços estão rodando ou mesmo afirmar qual o tipo de serviço, por exemplo, sabemos que por padrão as portas HTTP e HTTPs são respectivamente 80 e 443 e com isso podemos identificar qual o serviço roda nessas portas.

Mas isso acontece também, pois o autor comenta que as portas válidas de acordo com a Autoridade de Números Atribuídos (IANA) são apenas de 1 até 1023 (A instituição IANA descreve essas portas como reservadas), ou seja, essas portas já tem serviços definidos,

onde não pode ser utilizado por nem outro tipo de serviço. Com isso, podemos perceber que no momento que identificamos as portas podemos saber qual o serviço que está rodando.

O exame de portas é forma de detectar qual o estado de uma porta, por exemplo, caso for necessário saber se o serviço de *Secure Shell* (SSH*)* está rodando normalmente em um servidor ou mesmo dentro de um *firewall*, podemos fazer o uso de ferramentas como o NMAP para validar isso, da mesma forma podemos utilizar para saber quais portas estão abertas e que não estão sendo utilizadas nos servidores e com isso reduzir vulnerabilidades.

Lyon (2009), descreve que é de grande importância ser feito varreduras nos ambientes com intuito de detectar portas que não estão sendo utilizadas ou mesmo saber se as portas que estão abertas se encontram devidamente protegidas, com isso podemos ter um controle maior do nosso ambiente e dificultar o trabalho de atacantes.

Dessa forma podemos compreender que o exame de portas traz consigo diversas vantagens e se transforma útil no cotidiano dos administradores de redes, já que, da a possibilidade de verificar que determinados serviços estão ativos no ambiente, garantir a segurança e melhorar fazendo o uso de outras ferramentas, por exemplo, firewalls para fazer a limitação de quem pode e como deve fazer o uso dos serviços.

3.3.2 Como evitar NMAP

Já foi comentado como o NMAP trabalha e como podemos fazer o uso dele e dessa forma podemos perceber que as informações que ele gera podem ser valiosas para algumas pessoas e podem trazer grandes prejuízos a algumas instituições. Consequentemente devemos saber como evitar essa tecnologia com intuito de proteger informações relacionadas aos serviços que estão presentes na infraestrutura de rede de uma empresa.

Lyon (2009), descreve algumas orientações sobre como podemos evitar *Scanners* de porta, onde primeiramente escanear o seu próprio ambiente e mapear todas as portas que estão abertas e garantir que os serviços também estejam ativos, caso contrário desabilitá-los para evitar qualquer tipo de exploração de alguma vulnerabilidade.

Outra orientação do autor é fazer o uso de *firewall* para bloquear os serviços internos ou externo, por exemplo, se os colaboradores de uma empresa precisam acessar um determinado servidor e para isso precisaria liberar uma porta pode ser feito a configuração de uma *VPN SSL* para que os colaboradores acessem esse servidor de forma mais segura.

Logo, deve-se entender que corrigir as vulnerabilidades de rede de computadores, sendo ela complexa ou simples é unicamente de responsabilidade do administrador, pois é dessa forma que o mesmo poderá compreender a rede no qual administra e com isso

conhecendo todos os serviços presentes no ambiente e qual o procedimento deve ser feito para proteger e garantir que as vulnerabilidades sejam reduzidas.

3.4 Análise de tráfego de rede

Compreender o funcionamento de uma rede de computadores dentro de uma empresa é de suma importância para que o funcionamento da instituição esteja de acordo com o previsto e com isso todos os serviços dos clientes estejam funcionando normalmente. Porém muitas das vezes os administradores de rede não tem uma exatidão no que está acontecendo com o seu ambiente ou mesmo não sabem como corrigir falhas ou problemas que aparecem na rede no qual gerenciam.

Mota Filho (2013), explica em sua obra que o conhecimento em tráfego de redes pode reduzir a quantidade de erros dentro de uma instituição ou então ter uma precisão maior em qual a solução para uma situação indesejada, logo faz com que a equipe de T.I. (Tecnologia da Informação) não fiquem executando vários testes para poder solucionar o problema, ou seja, entender o funcionamento e importância da análise de tráfego de redes traz consigo diversas vantagens para um ambiente corporativo, por esse motivo os administradores de rede saber analisar o ambiente no qual administra.

Da mesma forma que o autor lista um conjunto de possibilidades que o profissional pode ter quando faz uma análise no tráfego de uma rede, por exemplo, conseguir encontrar equipamento com problemas físicos, podendo ser um cabo de rede ou mesmo uma porta de um *switch* com defeito, detectar falhas na segurança da rede ou mesmo bugs em serviços disponíveis na infraestrutura, tendo em mãos essa visão claro do ambiente o mesmo poderia solucionar os problemas de forma mais eficaz.

3.4.1 Diferença entre os protocolos UDP e TCP

Em redes de computadores em específico as TCP/IP existem dois tipos de protocolos para transporte de dados que são o *User Datagram Protocol* – (UDP) e o *Transmission Control Protocol* (TCP), onde cada um deles tem uma característica diferente e com isso deve ser aplicado em aplicações diferentes.

Kurose (2013), afirma que esses protocolos servem basicamente para garantir a entrega dos dados entre dois sistemas finais, da mesma forma que é possível verificar a integridade dos dados já que eles possuem campos de detecção de erros nos cabeçalhos, Entretanto o UDP não é considerado confiável já que ele não garante a entrega do dados enviados, diferentemente do TCP que tem a garantia da entrega dos dados.

O autor também descreve que isso acontece pela forma com é feita a conexão TCP, sempre será necessário dois dispositivos para fazer uma comunicação, um exemplo no qual no podemos citar é um navegador buscando informações de um servidor web. O primeiro a iniciar a conexão é o cliente, no qual ele envia uma solicitação para iniciar a comunicação, depois disso o servidor responder confirmando que pode iniciar a comunicação e por fim o cliente enviar o dado, o nome de todo esse processo é apresentação de três vias (*3-way handshake*).

Na obra do autor é apresentado também o funcionamento do protocolo UDP que diferentemente do TCP onde ocorre a apresentação de três vias para poder ocorrer a comunicação o UDP apenas envia os dados e não confirma se os mesmos foram recebidos, ou seja, a forma como ocorre a conversação entre as aplicações pode ser considerada mais rápida que a TCP.

Portanto, podemos perceber que o TCP garante a integridade dos dados e o UDP não preza por esse processo, e sim pela velocidade na entrega desses dados, por exemplo, o TCP é muito utilizado em aplicações cliente-servidor onde é preciso inserir informações dentro de banco de dados, para esses casos, devemos ter a garantia que os dados realmente foram enviados. Já o UDP, pode ser visto em vídeos online (*LiveStream*), pois nesses casos não é enviado uma confirmação dos dados enviados e necessário uma certa rapidez na entrega da informação.

3.5 Linguagem de programação

A linguagem de programação é um método padronizado utilizado por profissionais de T.I. (Tecnologia da informação), e pode ser aplicado em diferentes tipos de mercado, onde cada linguagem é voltada para algum tipo de aplicação em específico. O programador deve compreender como funciona sua aplicação para poder saber qual tipo de linguagem ele vai utilizar, além disso deve entender como funciona a linguagem no qual vai trabalhar, dessa forma ele vai poder desenvolver um *software* de acordo com a sua necessidade.

Souza (2011), afirma que um programa é representado por um conjunto de instruções (passo a passo) no qual foi definido para que o computador possa executar, ou seja, os dispositivos que executam esses programas apenas seguindo o que um programador “ordenou”. As linguagens de programação são basicamente um conjunto de passos no qual o computador compreende e deve seguir, ou seja, são regras com intuito de resolver um determinado problema.

Um ponto que podemos notar é que a linguagem de programação é um conjunto de orientações no qual os computadores devem seguir e com isso temos um programa, onde o mesmo deve ser utilizado para criação de um novo processo ou até mesmo automatizar um processo já existente, entretanto é executado de forma manual.

3.5.1 Automação de tarefas e sua importância

No dia a dia de quaisquer empresas temos diversas tarefas a serem executadas diariamente e cada uma delas com um nível de complexidade diferente. Sendo que maioria dessas tarefas podem ser executadas de forma automática sem a intervenção humana, por exemplo, um envio de email informativo para diversos colaboradores de uma mesma empresa.

Gaidargi (2019), afirma que a automação de tarefas é uma peça fundamental para o desenvolvimento de qualquer instituição, tornando assim as instituições mais eficientes fazendo com que os colaboradores possam focar em tarefas mais importantes. Entretanto, a automação de tarefas demora para ser implantada deve-se conhecer muito bem o processo a ser automatizado e quais os ganhos que a equipe vai ter.

Em diversos casos podemos fazer o uso de ferramentas já prontas para automatizar essas tarefas, mas algumas vezes devemos criar um pequeno sistema para resolver o problema, onde para esse caso a equipe deve ter um conhecimento básico sobre programação. Além disso, a equipe deve está alinhada sobre o que deve ser feito na nova solução.

Existem diversas formas de se automatizar uma tarefa e cada uma delas pode trazer um ganho diferente, Sweigart (2015) descreve em sua obra o uso da linguagem de programação Python para automatizar tarefas, o mesmo explica que diversas tarefas maçantes do dia a dia podem ser automatizadas e com isso facilitando a vida dos profissionais (não importa a área) que passam a executar suas atividades com uma maior precisão, abaixo podemos ver um trecho de sua obra:

> Eis a eficácia da programação de computadores. Um computador é como um canivete suíço que você pode configurar para realizar inúmeras tarefas. Muitas pessoas passam horas clicando e digitando para realizar tarefas repetitivas sem se darem conta de que o computador que estão usando poderia fazer seu trabalho em segundos se as instruções corretas fossem fornecidas. (SWEIGART, 2015, p. 29).

Com isso, podemos perceber que as ferramentas no qual possuímos nos computadores podem nos auxiliar na resolução de diversos problemas do nosso cotidiano e

com isso, agilizar processos que muitas das vezes passamos horas para finalizar tornam-se mais simples e rápidos para serem terminadas. Além disso, as instituições passam a ser mais propensas ao crescimento já que os profissionais podem focar em outras atividades mais complexas onde não podem ser automatizadas.

3.6 Monitoramento de redes

Garantir que todos os ativos de redes estejam rodando em seu perfeito estado tem grande importância para continuidade do serviço das instituições, mesmo elas sendo de pequeno ou grande porte, já que, existe uma necessidade das mesmas em adquirir sistemas capazes de apresentar tudo o que está acontecendo com os seus ambientes. E para isso, são utilizados sistemas de monitoramento que dão a possibilidade de dar uma resposta clara sobre tudo o que acontece dentro das organizações, entretanto existem diversas delas no mercado e cada um deles tem uma funcionalidade diferente.

Quando falamos em redes de computadores, o assunto monitoramento é ainda mais presente logo que se torna indispensável saber a saúde dos ativos rede. O uso de equipamentos dentro de uma instituição para garantir a continuidade do serviço se torna algo obrigatório e é crucial saber que cada um deles não podem parar e quando ocorre algum problema a equipe responsável pelos serviços devem ter com clareza o motivo do acontecimento.

Lima (2014), fala da importância da rede de computadores no ambiente empresarial e afirma que os profissionais de T.I. devem saber o que vai ser monitorado e por quais motivos está sendo feito o monitoramento desses equipamentos, sem esquecer em quais tecnologias vão ser aplicadas para o monitoramento dos ambientes. Com isso, os administradores de rede devem estar totalmente alinhados com a necessidade do negócio do cliente e assim entregar soluções realmente úteis para as empresas.

O autor também comenta sobre os problemas que podem acontecer na infraestrutura do cliente e como o monitoramento pode ser utilizado para dar uma resposta clara para os administradores. Abaixo tem um trecho da sua obra comentando sobre o assunto:

> Um serviço, quando é importante, jamais poderá estar indisponível. Ocorrendo um imprevisto, deverá ter contingência de recursos para manter o serviço no ar sem que os clientes percebam que algum problema está acontecendo. Mesmo com um acontecimento desse tipo, o sistema de monitoramento deverá ser capaz de registrar eventos, alertando administradores sobre possíveis falhas. Também podemos chamar isso de reação a incidentes, que é a capacidade de um sistema tentar se restabelecer automaticamente através da execução de rotinas automáticas a partir de um acontecimento. Quando o sistema não consegue restabelecer um serviço automaticamente, poderá (e deve) enviar alertas por e-mail e/ou SMS aos administradores, que atuarão para que o serviço volte ao ar o quanto antes, não gerando insatisfação dos clientes. (LIMA, 2014, p. 20).

Logo, podemos perceber que a função dos sistemas de monitoramento é prover uma resposta rápida e simples para os administradores de redes, já que, os sistemas empresariais não podem ficar indisponíveis por muito tempo, às vezes nem podem ficar indisponíveis, e o monitoramento deve passar essa resposta por meio de TVs (parte gráfica), e-mail, SMS ou utilizando mensageiros instantâneos. Onde, basicamente cada um deles vai dá a mesma resposta mudando somente o tipo tecnologia utilizada.

Lima (2014) explica, que esses sistemas devem entregar uma grande variedade de dados para os administradores e clientes, por exemplo, geração de relatórios e histórico, os dois podem ser úteis para ambas as partes do negócio, já que, o intuito principal é entregar informações relevantes e que tragam uma melhor tomada de decisão para as empresas. Portanto, consegue-se visualizar o histórico dos serviços e informações que podem ser usadas para melhorar o ambiente da empresa e até mesmo reduzir custos dos clientes.

Isso cria a chance das instituições planejarem o que deve ser feito dentro do ambiente, pois eles saem do achismo e passam a ter dados relevantes. Desse modo, os profissionais conseguem apresentar onde pode ser melhorado e por quais motivos deve ocorrer as melhorias, assim também o motivo de determinados problemas estarem acontecendo na infraestrutura dos clientes monitorados.

Lima (2014) apresenta alguns pontos muito importantes para o uso do monitoramento, um exemplo seria a segurança da informação, quando falamos de ativos de rede existem diversos dados rodando dentro desses servidores, onde é necessário garantir que os mesmos não vazem e que os dados estejam mãos apenas de pessoas autorizadas.

O monitoramento, também se faz útil quando queremos saber a performance de determinados ativos, por exemplo, saber o momento que um link de internet chega ao seu máximo de uso, quais servidores estão utilizando o máximo da CPU, memória ou disco, assim termos uma visão clara de toda a infraestrutura administrada.

Desta forma, o uso de ferramentas de monitoramento se transformam em algo indispensável para qualquer ambiente por mais simples que seja, com eles conseguimos definir quem acessou determinado servidor, a saúde do mesmo e assim tomar uma providência. Consegue-se, apresentar com clareza para pessoas do que está acontecendo nos ambientes e assim termos a capacidade de saber onde devemos atuar para solucionar problemas relacionados a lentidão de servidores, redes ou mesmo internet.

3.6.1 Zabbix

No mercado de T.I., existem diversos sistemas de monitoramento capazes de entregar soluções que estão aptos a sanar todas as necessidades referentes a uma infraestrutura de rede. E com isso, melhorando a visão das partes envolvidas no negócio com intuito de dar maior transparência a tudo o que ocorre nas instituições.

Lima (2014), descreve o Zabbix como uma ferramenta *OpenSource,* e isso significa que o seu código é aberto, sendo assim pode ser alterado para a necessidade de qualquer pessoa, já que, o indivíduo tem acesso a todo o seu algoritmo sem ser preciso comprar o *Software,* e é por esse motivo que não se faz a compra da licença, ou seja, o sistema é totalmente flexível e pode ser utilizado por qualquer indivíduo que tenha tecnologia (*hardware* e *software)* suficiente para implantá-lo.

Em um trecho de sua obra o autor explica como é um funcionamento do Zabbix da forma mais simples possível, apresentando os itens mais básicos do sistema e como ser utilizado o mesmo para um ambiente:

> Zabbix possui a capacidade de monitorar milhares de itens em apenas um servidor, além de ser possível ter um monitoramento distribuído. Dessa forma, podemos ter um servidor central de monitoramento e vários outros servidores subordinados a ele enviando as métricas para o servidor central ou apenas replicar as informações. Também é possível separar os servidores *web,* servidor de banco de dados e servidor de monitoramento para aumentar a flexibilidade e ganhar em desempenho. (LIMA, 2014, p. 23)

Dessa forma, podemos perceber que o sistema de monitoramento é capaz de entrar uma grande quantidade de dados de um único servidor, esses dados podem ir de uma simples verificação de portas, saber se está aberto ou não, como até mesmo se o mesmo está ligado ou desligado. Da mesma forma que foi explicado pelo autor, podemos separar a instalação do servidor Zabbix em sistemas isolados, por exemplo, podemos deixar a parte do Zabbix totalmente isolada do banco de dados, tendo uma maior escalabilidade e elasticidade do ambiente de monitoramento.

Lima (2014) afirma, que o mesmo é capaz de gerar relatórios que podem ser uteis para os administradores de rede poderem analisar os itens de um determinado sistema, sabendo a data e hora exata dos acontecimentos e essas informações além de poderem ser vistas em tempo real, elas podem ser configuradas pela interface *web* do sistema, com isso, transformando o trabalho do administrador de redes ainda mais simples.

Outro ponto importante a ser comentado, é a capacidade que o profissional tem de automatizar determinadas tarefas maçantes, como inserir equipamentos de rede de forma automática no sistema de monitoramento sem ser necessário intervir manualmente para cada

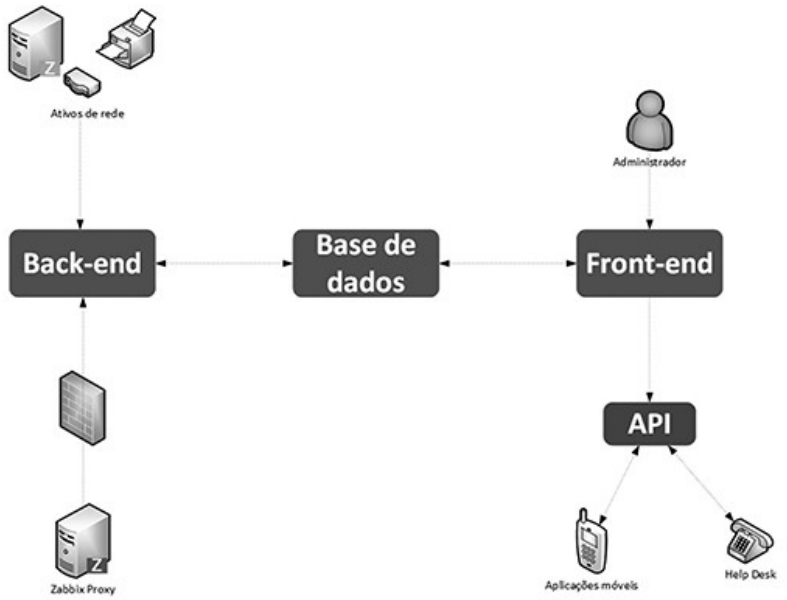
novo dispositivo. O autor apresenta também que podemos fazer o uso de *scripts* customizados, utilizando a linguagem Shell Script que é nativa dos sistemas operacionais GNU/Linux, e instalado dentro do servidor com intuito de serem usados para alertas, comandos remotos ou determinadas ações.

Logo, podemos perceber que o sistema traz consigo diversas vantagens, já que, é fácil de ser configurado não somente pelo fato em ser bem documentado, mas também por ter uma comunidade vasta de profissionais que podem auxiliar alguns que tem pouco conhecimento na implementação da tecnologia.

Podemos citar como vantagem, o fato de ser compatível com a maioria dos bancos de dados relacionais que existem no mercado, que é capaz de monitorar a maioria dos sistemas operacionais (Windows, Linux, Free BSD), *Switchs, firewalls*, banco de dados e além que é possível gerar alertar via SMS, telegram ou e-mail tudo isso sem precisar a aquisição de licenças ou algo semelhante.

Lima (2014), afirma que o Zabbix trabalha em uma abordagem de três camadas que são divididas em aplicação, banco de dados e interface *web.* Onde a aplicação é o que os desenvolvedores chamariam de *back-end*, ou seja, é basicamente ele que faz toda a coleta dos dados e envia para o banco de dados, onde esse é o responsável em armazenar todas as informações que podem ser extraídas posteriormente no *front-end,* que é onde o administrador pode ter uma resposta rápida do que está acontecendo, consegue gerar os relatórios com as informações contidas no banco de dados e por fim a configuração do sistema. Abaixo temos na figura 4 a representação do autor sobre o assunto:

Figura 4 - Arquitetura do Zabbix



Fonte: Lima (2014)

Sendo assim, é possível visualizar com clareza que a aplicação de um sistema de monitoramento em qualquer empresa pode trazer uma grande vantagem competitiva, podemos ter um retorno rápido de tudo o que está acontecendo no cliente e além disso sabemos o momento exato que o problema aconteceu. Não esquecendo, que o Zabbix traz consigo uma flexibilidade capaz de auxiliar o profissional na melhoria do ambiente e automatização sem muita dificuldade.

3.6.2 Conceitos e funções do Zabbix

No ambiente de monitoramento, o administrador de redes deve efetuar algumas configurações no servidor via interface web para que possa monitorar os equipamentos de rede dos clientes, para isso o profissional deve conhecer alguns conceitos que são utilizados no sistema de monitoramento Zabbix.

Lima (2014), apresenta em sua obra esses conceitos de forma bem simples, e descrever cada um deles, para ser feito um monitoramento de um *host,* que é qualquer equipamento de rede como servidores, sistemas operacionais, *Switches, Firewalls*, impressoras, entre outros. Logo, é todo equipamento que pode ser monitorado que contenha IP ou DNS.

O autor descreve também o Item, sendo ele uma forma que é utilizada para o Zabbix coletar as informações, existem diversos que podem ser utilizados no sistema de monitoramento, entretanto os mais utilizados são os agentes passivas quando o servidor busca as informações, ativos são dados processados por um agente instalado dentro do *host* e enviado as informações para o servidor e por fim o *Simple Network Management Protocol* (SNMP) que praticamente todos os equipamentos de rede possuem esse protocolo que é capaz de enviar algumas informações referentes ao *host*.

Após conseguir monitorar os equipamentos e sistemas é possível ativar os *triggers* que são expressões lógicas utilizadas para tratar os itens, somente depois disso conseguimos definir o nível de severidade de cada acontecimento, um exemplo que podemos citar é a indisponibilidade de um servidor, onde dependendo do negócio do cliente podemos dizer que o nível de criticidade é o máximo e com isso os responsáveis devem atender o mais rápido possível.

Por fim, o autor comenta sobre os *templates* que são arquivos xml que tem um conjunto de elemento pré-configurados que tem a função de facilitar no momento da criação de itens e *triggers,* já que, esses componentes já se encontram configurados no arquivo e dessa forma não se torna necessário configurar novamente. Além disso, podem ser aplicados em equipamentos os sistemas semelhantes, por exemplo, em uma empresa que tem cinco sistemas operacionais Windows Server 2012, pode-se aplicar o mesmo *template* para todos os servidores.

Assim sendo, é possível fazer as configurações de diversas formas sendo totalmente opcional da parte do administrador, entretanto é de grande importância que o responsável pelo sistema de monitoramento conheça todos os pontos apresentados para que ele possa configurar o seu ambiente de acordo com a necessidade do monitoramento.

Além do mais, o profissional pode automatizar todo o seu ambiente sem precisar fazer configurações complexas no monitoramento, pois o Zabbix traz consigo toda essa facilidade, um bom exemplo sobre isso é o uso de *templates* que é uma forma de configurar um monitoramento para somente um tipo de *host*, entretanto podemos aplicar para diversos que tenham a mesmas características. Com isso, podemos ter um monitoramento de acordo com o que o cliente precisa no seu ambiente.

4 AMBIENTE DE HOMOLOGAÇÃO

Abaixo, vamos descrever com detalhes como foram feitos os testes em laboratório, quais as tecnologias (Virtualização, monitoramento, sistemas operacionais, entre outras) foram utilizadas para a criação do projeto e como foi feito a implementação, vamos apresentar os diagramas de rede para melhor entendimento do trabalho.

4.1 Virtualização

Antes de iniciarmos a apresentação do projeto, se faz necessário explicar um item muito importante para esse projeto que é a virtualização que existe a bastante tempo no mercado e é utilizado tanto por empresas quanto por usuários domésticos e com isso é muito popular no mercado, já que, carrega consigo recursos que podem auxiliar na implantação de novas tecnologias.

Veras (2016), explica que a virtualização é uma forma de reduzir custos com equipamentos físicos com intuito de podermos instalar e configurar diversos sistemas operacionais em um mesmo servidor e com isso não é necessário a aquisição de equipamentos físicos para fazer o uso dessas tecnologias.

> Servidores virtuais criados com a virtualização oferecem um ambiente similar ao de um servidor físico e otimizam o uso de recursos, tornando as aplicações independentes do hardware. Transforma-se assim um ambiente baseado em servidores físicos em um ambiente baseado em servidores virtuais ou máquinas virtuais. (Veras, 2016, p. 37)

Dessa forma, podemos reduzir custos e além disso se torna algo mais simples, onde qualquer pessoa que tenha *hardware* suficiente e conhecimento técnico para fazer uso desse recurso pode usufruir da melhor forma o que a virtualização pode entregar. Portanto podemos utilizar os servidores virtuais para simular um ambiente semelhante ao de um servidor físico sem a necessidade de adquirir equipamentos para esse tipo de tarefa.

Veras (2016) afirma, que a virtualização é basicamente o particionamento ou compartilhamento de recursos físicos com HD, memória, CPU e entre outros, para outros servidores virtuais, também chamados de máquinas virtuais, e os mesmos fazem o uso isoladamente, ou seja, cada sistema tem o seu próprio núcleo, aplicações, arquivos e estrutura sem ser necessário depender do outro.

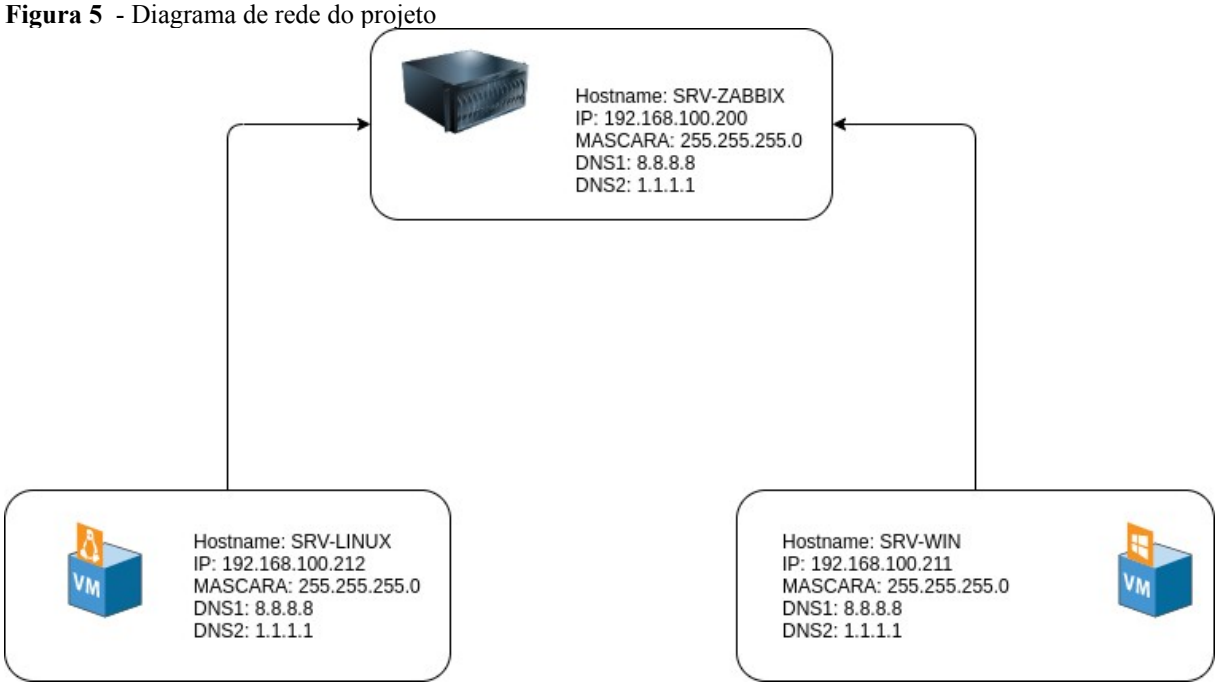
Com isso, pode compreender que a virtualização traz flexibilidade para qualquer profissional de T.I., pois garante melhor gerenciamento dos sistemas instalados no ambiente no qual administra e além disso, facilitam ambientes de testes, já que, não existe mais a necessidade da aquisição de equipamentos de hardware robustos para executar procedimentos simples como a simulação de um sistema operacional.

4.2 Tecnologias utilizadas

Antes de iniciar a instalação dos sistemas, primeiro foi feito o desenho do projeto com a definição dos Ips e sistemas a serem utilizados. Para esse caso, aplicamos três servidores, sendo um o Zabbix rodando em cima de um sistema operacional CentOS 7, um sistema operacional Windows 10 onde vão rodas diversos serviços, por exemplo, o de acesso remoto e, por fim, um servidor GNU/Linux Debian Buster, onde os dois últimos citados serão utilizados para serem monitorados pelo Zabbix.

Para melhor entendimento foi feito um diagrama de rede que é apresentado na figura 5 para apresentar o IP, os sistemas utilizados, entre outras informações:

Figura 5 - Diagrama de rede do projeto



Fonte : Aurélio Malheiros (2020)

Como foi explicado acima, temos os detalhes de cada servidor, onde o *Hostname* é o nome do servidor, ou seja, SRV-Linux é o sistema operacional Linux, SRV-WIN é o sistema operacional Windows e o SRV-Zabbix é o sistema onde está rodando o monitoramento. Para criação desse ambiente foi feito o uso do Virtual Box que é uma tecnologia de virtualização.

No site do Virtual Box, é possível obter detalhes sobre o sistema que é uma ferramenta de virtualização que é compatível com diversas plataformas, como Windows, Linux e MAC sendo apenas necessário instalação de alguns drivers para o uso da ferramenta. O mesmo também pode ser utilizado tanto para uso doméstico quanto para uso empresarial e a

ferramenta é desenvolvida pela Oracle como a própria instituição afirma, abaixo temos um pouco da descrição do sistema:

> VirtualBox é um poderoso produto de virtualização x86 e AMD64 / Intel64 para uso empresarial e doméstico. O VirtualBox não é apenas um produto extremamente rico em recursos e de alto desempenho para clientes corporativos, mas também a única solução profissional que está disponível gratuitamente como software de código aberto sob os termos da GNU General Public License (GPL) versão 2. (VIRTUALBOX, SEM PAGINAÇÃO, 2020).

Com o Virtual Box podemos utilizar apenas um computador para virtualização de todas as máquinas, sendo necessário apenas de hardware para isso, por exemplo, para o Zabbix foi adicionado 4 GB de memória e 30 GB de disco, sendo mais que suficiente para os testes realizados, portanto é possível virtualizar os sistemas operacionais sem a necessidade de vários servidores físicos ou mesmo de equipamentos robustos para esse tipo de procedimento.

No Zabbix, configuramos uma regra de descoberta por agente isso significa que todo equipamento que estiver naquela rede que foi configurada automaticamente ele será adicionado na lista de sistemas a serem monitorados, logo automatizando o processo de inserção de equipamentos bastando somente que as máquinas configuradas tenham o agente instalado. Abaixo vamos apresentar na figura 6 os dois servidores sendo monitorados:

Figura 6 - Monitoramento dos hosts

Fonte : Aurélio Malheiros (2020)

Após isso, foi feito a instalação do NMAP, script para automação e o template dento do servidor do Zabbix para que ele possa fazer o mapeamento das portas e inserir o *template* nos *hosts*, a instalação do *script* deve ser feito dentro servidor no diretório */usr/lib/zabbix/externalscripts,* nele devemos colocar todos os *scripts* que tenham o

intuito de automatizar determinadas tarefas. Abaixo é demonstrado na figura 7 e 8 o resultado da saída nos dois servidores monitorados:

Figura 7 - Mapeamento das portas do servidor SRV-WIN

```
[root@localhost externalscripts]# ./tcp-port-scan-lld.sh 192.168.100.211
{"data":[
{"{#PORTA}":"135", "{#SERVICO}":"msrpc"},
{"{#PORTA}":"139", "{#SERVICO}":"netbios-ssn"},
{"{#PORTA}":"445", "{#SERVICO}":"microsoft-ds"},
{"{#PORTA}":"3389", "{#SERVICO}":"ms-wbt-server"},
{"{#PORTA}":"5357", "{#SERVICO}":"wsdapi"}
]}
```

Fonte : Aurélio Malheiros (2020)

Figura 8 - Mapeamento das portas do servidro SRV-LINUX

```
[root@localhost externalscripts]# ./tcp-port-scan-lld.sh 192.168.100.212
{"data":[
{"{#PORTA}":"22", "{#SERVICO}":"ssh"}
]}
```

Fonte : Aurélio Malheiros(2020)

O que foi apresentado acima é um teste simples para verificar se o algoritmo está funcionando e se conseguimos verificar as portas que estão abertas, caso esteja apresentando dessa forma a configuração de todos os sistemas foi feito de forma correta (agente e servidor) e com isso será possível visualizar os resultados na interface gráfica do Zabbix.

Esse tipo de automação é recomendado pela própria Zabbix, onde existe um artigo no site oficial que comenta sobre isso escrito por Moarch (2016), onde o mesmo descreve a importância do uso do NMAP no mapeamento e ativos de redes com intuito de facilitar o trabalho do administrador de redes, ou seja, dessa forma conseguimos ter uma visão geral de todos os serviços que estão rodando no servidor sem a necessidade de acessar um por um para verificar sua disponibilidade, logo abaixo temos um trecho do seu artigo falando sobre o assunto:

> A qualquer momento, existem centenas, senão milhares, de serviços em execução em seus servidores. Muitos deles precisam estar acessíveis em uma rede. Os serviços da Web precisam estar disponíveis normalmente na porta 80 e / ou 443, serviços de FTP na porta 21, MySQL na 3306 e assim por diante. É extremamente importante monitorar sua conectividade. Acompanhar "qual serviço está sendo executado, onde e em qual porta" consome muito tempo. Ficar de olho na possibilidade de acesso desses serviços é uma tarefa gigantesca. À medida que o ambiente cresce, pode tornar-se quase impossível ficar por dentro dele. (MOARCH, SEM PAGINAÇÃO, 2016).

Com isso, o administrador de rede pode passar a se preocupar com outras tarefas do dia a dia, já que o seu monitoramento é capaz de da todas as repostas rápidas sem que seja

necessário uma pessoa para acessar o ambiente e verificar se determinado serviço parou de rodar ou mesmo saber se algum serviço está rodando quando na verdade era pra estar fechado.

Por exemplo, sabe-se que todo serviço aberto pode ser explorado e encontrado uma vulnerabilidade, entretando podemos fazer com que os serviços sejam limitados para determinados Ips ou mesmo somente para que alguns usuários possam utilizar, isso faz com que essas falhas de segurança diminuam e assim dando a garantia que não ocorra problemas para os clientes.

Moarch (2016), também comenta sobre os *Low-Level Discovery* (LLD) que são uma forma onde os administradores podem criar diferentes recursos no Zabbix como itens, *triggers* e gráficos sem a necessidade de fazer isso manualmente em cada dispositivo adicionado no Zabbix, entretanto para isso se faz necessário o administrador compreender sobre Shell Script que é uma linguagem programação nativa dos sistemas operacinais GNU/Linux.

Para alertas foi utilizado tanto a versão *Web* quanto a integração do telegram que é um mensageiro instânteneo utilizado para troca de mensagens, porém podemos fazer o uso dele para criação de *bots* com o BotFather e integrar com o Zabbix, dessa forma podemos gerenciar visualizar os alertas via telegram, ou seja, é feito a criação do *bot*, configuração dentro do Zabbix para que seja possível enviar alertas para o telegram.

Portando, o ambiente que foi apresentado nesse protótipo é uma forma automatizada de conseguimos detectar todas os serviços que estão rodando dentro de um servidor e com isso o administrador pode ter uma noção clara quais são as possíveis vulnerabilidades do ambiente no qual ele está administrando, logo ele pode ter uma melhor tomada de decisão para saber qual o melhor procedimento para a sua infraestrutura.

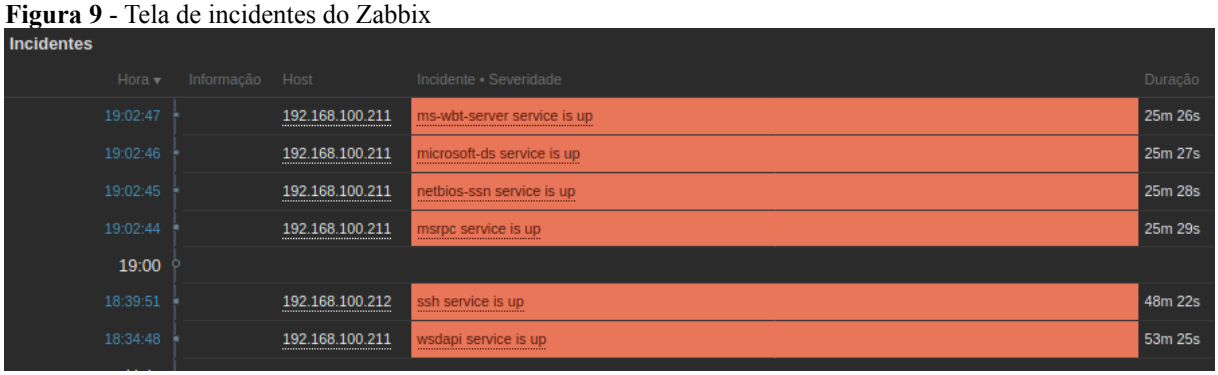
4.3 Resultado dos testes

Após ser feito a montagem do laboratório e todas as configurações que já foram citadas anteriormente, foi necessário verificar se tudo estava sendo monitorado corretamente e se era possível saber se as portas estavam abertas ou não e com isso ser possível tomar alguma medida para isso. Para esse caso, habilitamos somente o *firewall* do sistema operacional Windows e fizemos os bloqueios necessários para que não ocorresse monitoramento em algumas portas.

Na figura 9, é possível visualizar na tela de incidentes do Zabbix as portas que estavam abertas no sistema operacional SRV-WIN (IP 192.168.100.211), antes de qualquer procedimento de segurança feito no servidor, ou seja, as portas estavam abertas para e

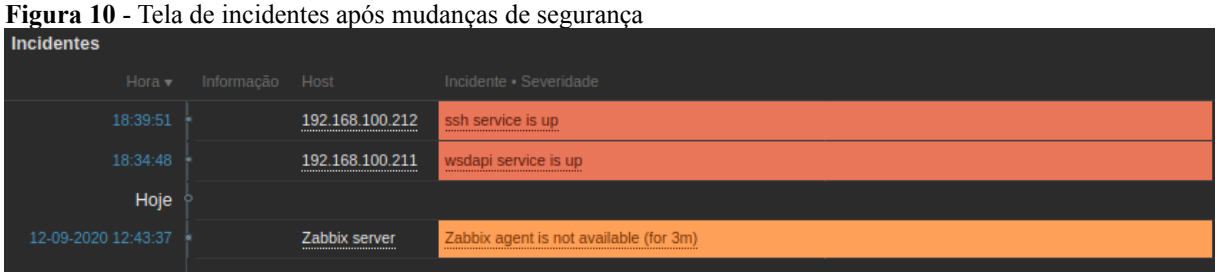
qualquer um poderia ter acesso aos serviços e poderiam explorar aquelas vulnerabilidades. Enquanto a figura 10 apresenta o estado do monitoramento após os bloqueio feitos no firewall.

Figura 9 - Tela de incidentes do Zabbix



Fonte : Aurélio Malheiros (2020)

Figura 10 - Tela de incidentes após mudanças de segurança

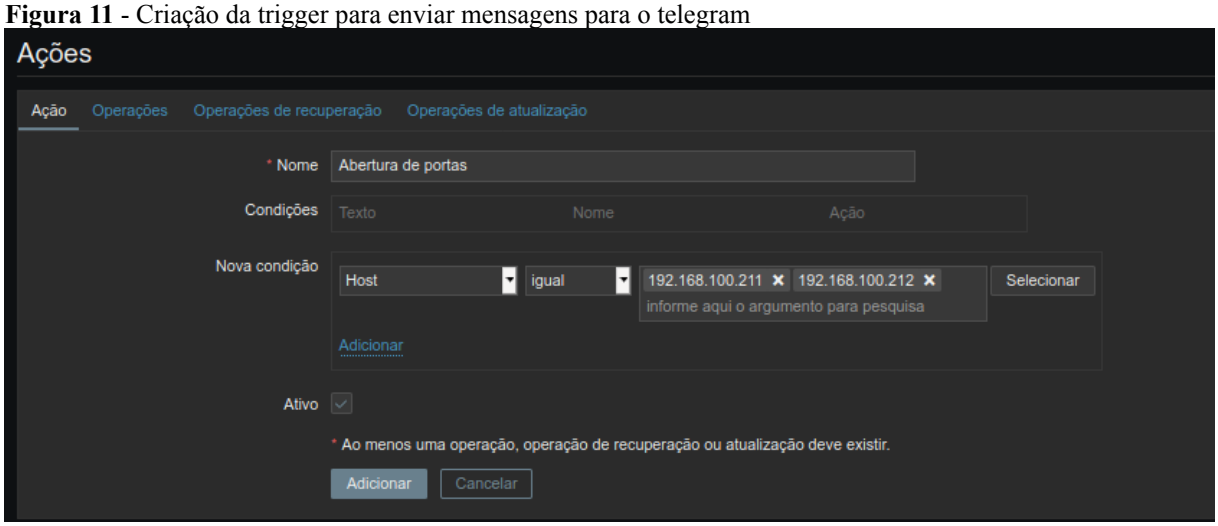


Fonte : Aurélio Malheiros (2020)

Os testes feitos foram realizados apenas no SRV-WIN e no SRV-LINUX foi apenas habilitado para saber se realmente estava sendo monitorado. Lembrando, que o intuito não é de bloquear os serviços de acesso remoto, *web* e entre outros para que ninguém consiga utilizar os serviços e sim de limitar quem possa acessar os mesmos.

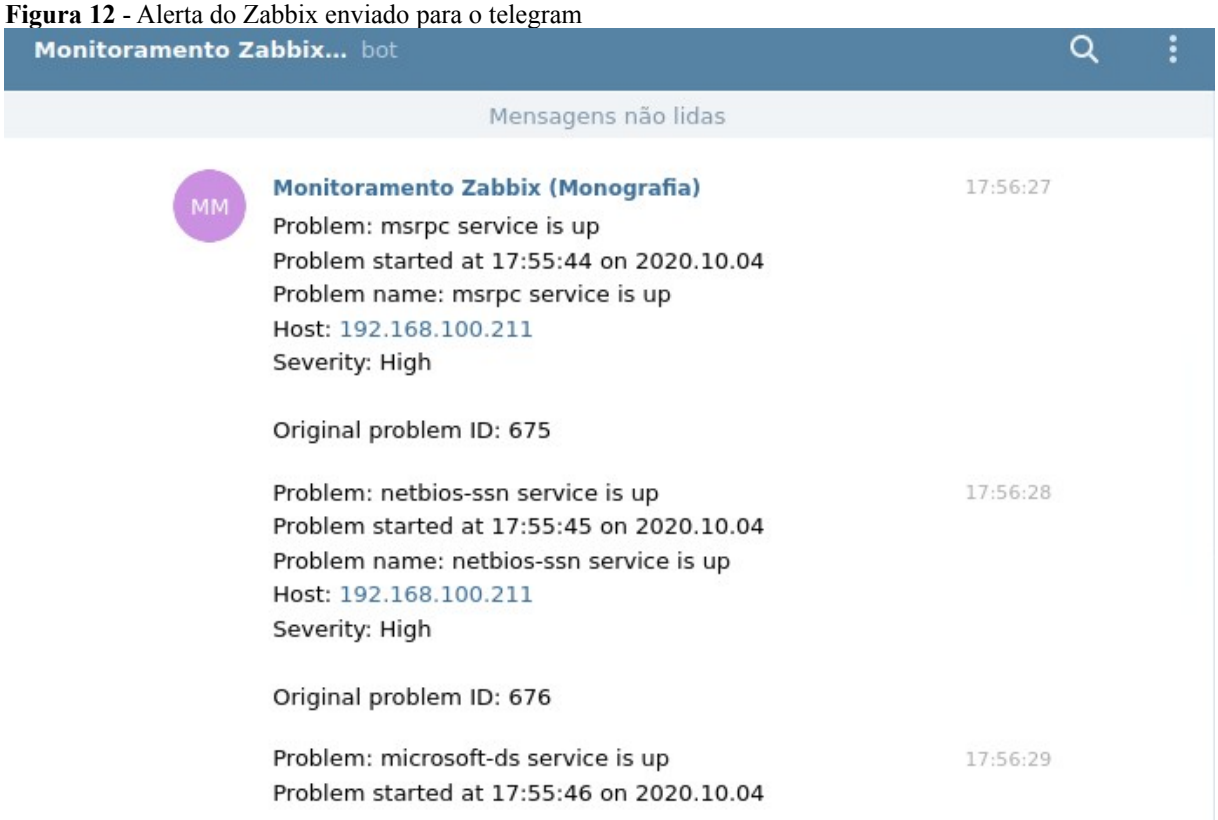
Outro ponto, que também foi desenvolvido foi a integração com o telegram, dessa forma foi possível exibir os alertas de abertura de portas via mensagem, contudo foi configurado apenas para verificação das portas, já que, esse é o foco do projeto. Seguindo a documentação do Zabbix foi feito a ativação da mídia telegram e inserimos o *id* do *bot* configurado e em ações criamos uma *trigger* como mostra a figura 11 para toda vez que ocorra alguma abertura de portas dos dois servidores (SRV-WIN e SRV-LINUX) seja alertado tanto via *web,* quanto via mensagem que é apresentando na figura 12.

Figura 11 - Criação da trigger para enviar mensagens para o telegram



Fonte : Aurélio Malheiros (2020)

Figura 12 - Alerta do Zabbix enviado para o telegram



Fonte : Aurélio Malheiros (2020)

Dessa forma, quando não for possível estar presente dentro da empresa ou mesmo quando o profissional de T.I. não estiver visualizando a tela de *Dashboard* do Zabbix, ele possa ser alertado via telegram para que quando ocorrer a abertura de alguma porta que estiver sendo monitorada dentro do ambiente que o mesmo administra gere um alerta para o

telegram que todas as pessoas que estão de posse desse telegram, e com isso pode verificar o que aconteceu com o ambiente e tomar uma medida para solucionar o problema ocorrido.

Portanto, quando for feito alguma alteração que abra as portas será possível visualizar isso de duas formas, onde a principal será via *Dashboard* do Zabbix e a outra é via telegram, dando maior com isso é possível tirar a centralização apenas do primeiro item, pois de posse de um celular que tenha instalado esse aplicativo, já será possível ter algumas respostas do ambiente dos clientes.

Agora, imaginando que tenhamos que administrar determinada empresa, onde a mesma tem um sistema web, geralmente utilizam as portas 80 e 443, instalado no servidor no qual administramos é necessário entender quem deve ter acesso a esse sistema, se ele precisa ser aberto onde as pessoas possam acessar de qualquer lugar, bastando ter internet, um computador e um navegador, ou se apenas na empresa que deve ser acessado esse sistema, para a última opção podemos limitar para que fora da empresa ninguém acesso o mesmo e dessa forma reduzimos as brechas de segurança.

E isso, o administrador de redes deve analisar para compreender a real necessidade do seu cliente e como ele pode melhorar a gestão de segurança do mesmo a partir das informações das regras de negócio. Lembrando, que vulnerabilidades sempre vão existir contudo o administrador deve garantir que elas não prejudiquem a segurança da organização administrada por ele.

Logo, percebemos que os testes feitos no monitoramento funcionaram de acordo com o esperado dando uma resposta clara ao administrador o momento que os serviços estavam abertos para que qualquer pessoa pudesse acessar. Com isso, ele poderia ter uma perspectiva mais clara de qual decisão tomar nesse caso, pois pode ser que o servidor entrou em manutenção e ele já estava ciente ou então alguém acessou o ambiente e desabilitou os sistemas de segurança com intuito de fazer um teste rápido, de qualquer forma os profissionais podem ter respostas mais claras sobre o que está acontecendo no ambiente administrado.

5 METODOLOGIA

Este trabalho tem como objetivo fazer um levantamento de dados relacionados a segurança da informação, automação de tarefas e monitoramento de redes em ambientes corporativos, além disso apresentar soluções simples e viáveis para os profissionais responsáveis pela administração de tais ambientes, todas as soluções e conceitos apresentado aqui foram baseados em artigos científicos ou mesmo em obras de autores renomados na área da tecnologia da informação, Gil (2002) descreve as vantagens de se fazer a pesquisa bibliográfica:

> A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Esta vantagem se torna particularmente importante quando o problema de pesquisa requer dados muitos dispersos pelo espaço. (Gil, 2002, p.50).

Além disso, baseado na obra de Gil (2002) a pesquisa tem como finalizada ser exploratória, pois o principal foco da pesquisa é aproximar sobre assuntos relacionados a automação de tarefas no ambiente da segurança da informação e monitoramento de redes, descritiva, já que, será analisado a utilizada e aplicabilidade do NMAP dentro de ambientes empresariais. O trabalho será experimental, pois é necessário aplicar para saber a eficacia da automação da ferramenta de rede, saber se realmente é útil e como podemos utilizar.

Portanto, a pesquisa seguirá um conjunto de etapas para o desenvolvimento do trabalho:

a) Levantamento bibliográfico;
b) Escolha do material bibliográfico;
c) Verificação de formas de automatizar;
d) Aplicação em ambientes de testes para validar a funcionalidade;
e) Teste em ambiente prático para saber o impacto gerado pela automação.

E por fim, a pesquisa vai ser qualitativa e quantitativa, já que, o intuito da projeto é tanto determinar a quantidade de vulnerabilidade dentro dos ambientes empresariais, mas também prover melhorias na segurança desses ambientes, da mesma forma apresentar novas formas de melhorias e análise de dados relacionados a redes de computadores.

6 RESULTADOS E DISCUSSÕES

Neste capítulo, será abordado a coleta de informações referentes ao ambiente da empresa CorpX, onde a mesma faz o uso do Zabbix para monitoramento dos seus clientes, porém não aplica o NMAP para fazer o monitoramento das portas e nem mesmo monitora os serviços que estão rodando dentro do servidor.

A instituição onde foi aplicado o projeto, solicitou total sigilo dos dados dos clientes, sendo apenas apresentado o necessário para finalização do projeto, em que fosse usado nomes fictícios para os colaboradores, empresas clientes e até mesmo para a própria. Sendo assim, todos os dados apresentados são reais, porém, nomes e alguns dados vão ser trocados para manter a segurança da instituição.

6.1 Entendimento do ambiente da empresa

Para ter uma maior percepção do ambiente da empresa, foi necessário fazer um questionário do cliente para entender se os responsáveis pelo monitoramento (Dois colaboradores) faziam o uso NMAP ou mesmo se conheciam ferramenta, qual era a visão deles sobre a mesma. Além disso, saber o que os profissionais entendiam sobre automação e o que ela traz para instituição que faz o uso.

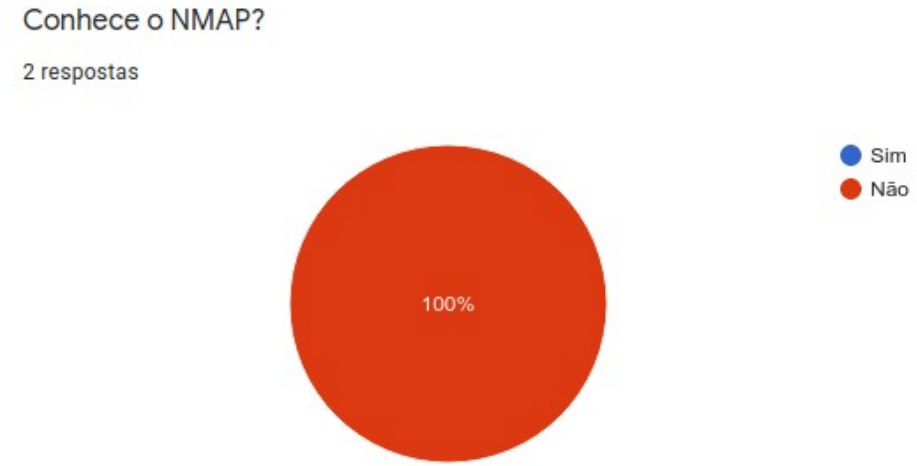
Foram perguntas simples e diretas, para que os mesmos não ficassem confusos nas respostas, dessa forma ele poderiam responder sem o auxílio de outra pessoa. Um ponto importante a ser lembrado é que os dados dos colaboradores não foram apresentadas pela solicitação da gestão da empresa.

Na figura 13, é apresentado a primeira pergunta, nela o intuito é saber se os profissionais conhecem algum tipo de ferramenta para mapeamento de portas de redes. Abaixo dessa figura, temos a figura 14 onde é possível visualizar que os dois indivíduos não conhecem o NMAP, ou seja, um deles já teve contato com uma ferramenta de mapeamento de portas, entretanto desconhece totalmente o NMAP.

Figura 13 - Pergunta sobre o mapeamento de portas

Fonte: Aurélio Malheiros (2020)

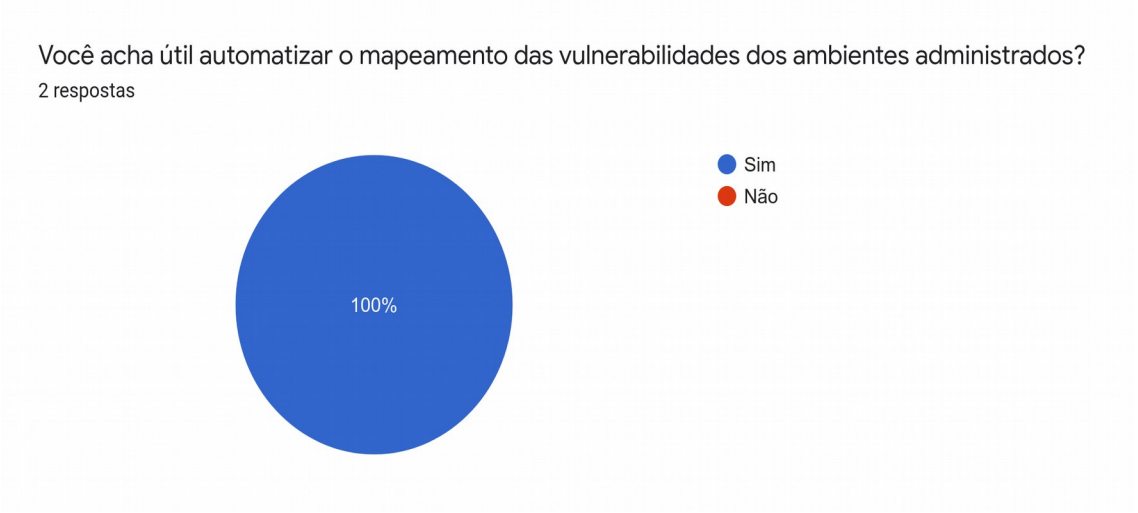
Figura 14 - Conhecimento do NMAP



Fonte:Aurélio Malheiros (2020)

Uma outra pergunta que foi feita para equipe, foi se os mesmos achavam útil o mapeamento automatizado das vulnerabilidades dos clientes administrados, a ideia dessa pergunta é compreender se eles preferem fazer o processo manualmente, já que, isso vai depender muito da cultura da empresa, entretanto na resposta que aparece na figura 15 é possível perceber que ambos acham útil.

Figura 15 - Utilidade da automação do mapeamento de portas



Fonte: Aurélio Malheiros (2020)

Portanto, podemos perceber que não é feito o uso do NMAP dentro da organização e além disso os colaboradores não tem conhecimento das funcionalidades da ferramenta, portanto foi orientado aos mesmos sobre o seu funcionamento e como poderia ser aplicado dentro da empresa para monitorar os clientes.

6.2 Implantação do projeto

O processo de implantação foi feita em etapas para não causa danos para o ambiente da empresa, já que, todo trabalho foi feito em um ambiente de monitoramento já em produção, ou seja, qualquer dano feito no ambiente poderia causar perda nas informações da empresa e em consequência perda de informações dos seus clientes.

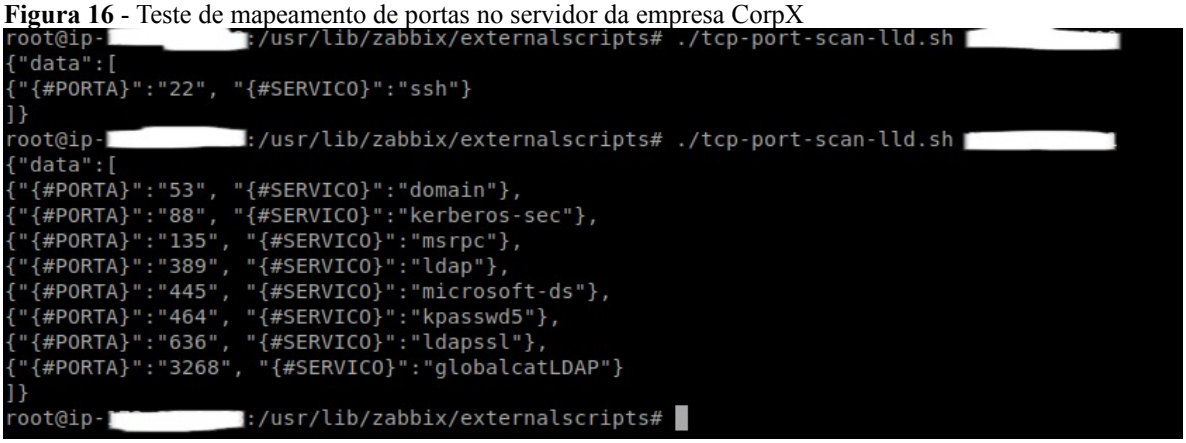
Dessa forma, o primeiro ponto foi criar uma documentação para implantação do projeto, que é um conjunto de passos para que a instalação seja feita com sucesso. Nesse documento, contém os requisitos mínimos para a funcionalidade do monitoramento das portas, além disso, boas práticas como backup do ambiente para não acontecer nem um tipo de transtorno.

O principal passo, foi orientar para que fosse feito a realização do backup do ambiente tanto do servidor, quanto do banco de dados para em um caso de erro ou problema na configuração fosse possível fazer uma restauração do ambiente. Foi necessário também, realizar a instalação do NMAP dentro do servidor Zabbix, para que fosse possível realizar o monitoramento das portas com LLD.

Foi necessário fazer o download do *script* para mapeamento das portas que deve ser colocado no diretório /usr/lib/zabbix/externalscripts, além disso se faz necessário dá as permissões de execução para os algoritmos ser executado pelo servidor Zabbix. É nesse diretório, que podemos colocar algoritmos externos no sistema de monitoramento, ou seja, dessa forma é possível trabalhado com a descoberta de baixo nível (LLD).

Após a instalação do *script* dentro do servidor, fizemos alguns testes em servidores da empresa para validar se já era possível verificar as portas abertas no ambiente, como mostra a figura 16.

Figura 16 - Teste de mapeamento de portas no servidor da empresa CorpX

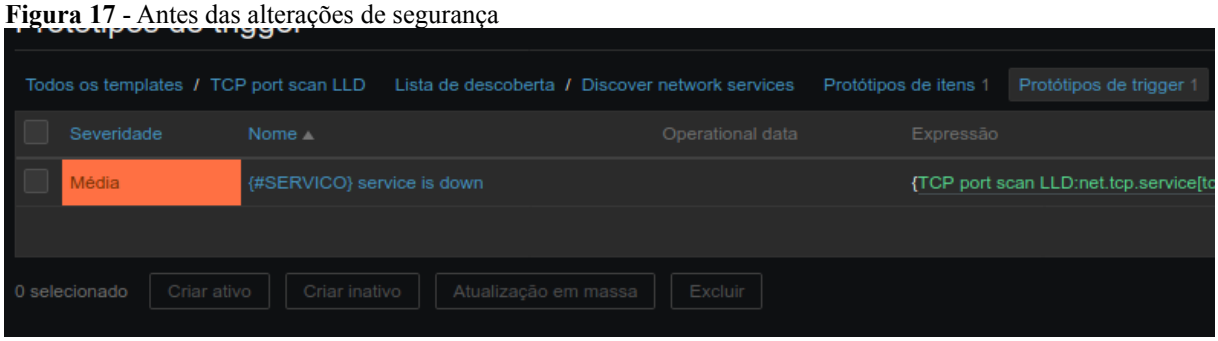


Fonte : Aurélio Malheiros (2020)

Finalizado os testes do *script*, passamos para a importação do *template,* importamos o mesmo para o servidor Zabbix via *Web,* e fizemos algumas alterações para que o mesmo atendesse as necessidades do projeto, onde no caso iriamos monitorar as portas que estavam abertas e com isso conseguiríamos ter uma visão das vulnerabilidades encontradas na empresa.

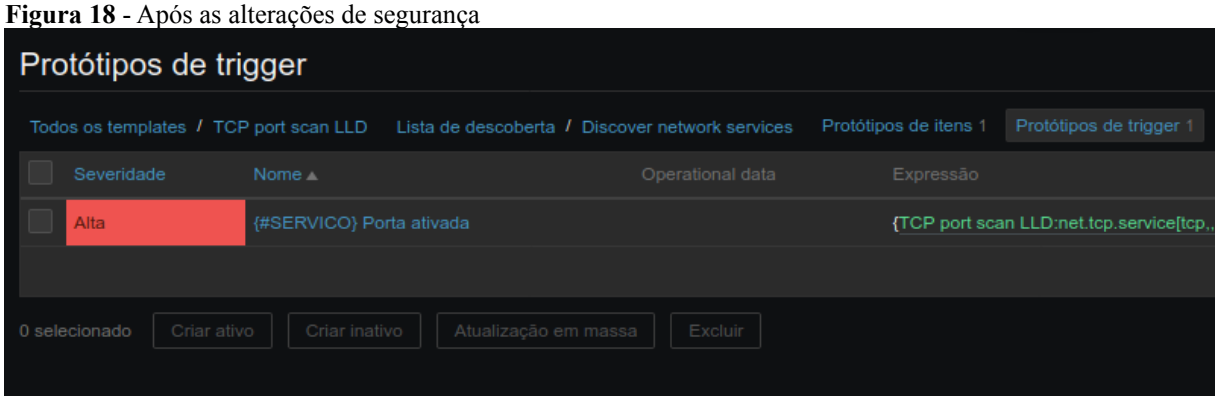
Abaixo, temos as alterações feitas no *template,* em severidade em vez de usar média alteramos para alta, já que, se trata de uma vulnerabilidade de segurança, onde tem escrito *service is down* alteramos para porta ativada, isso foi feito com intuito de facilitar a legibilidade para os administradores do sistema, nas figuras 17 e 18 vão ser apresentadas as mudanças.

Figura 17 - Antes das alterações de segurança



Fonte : Aurélio Malheiros (2020)

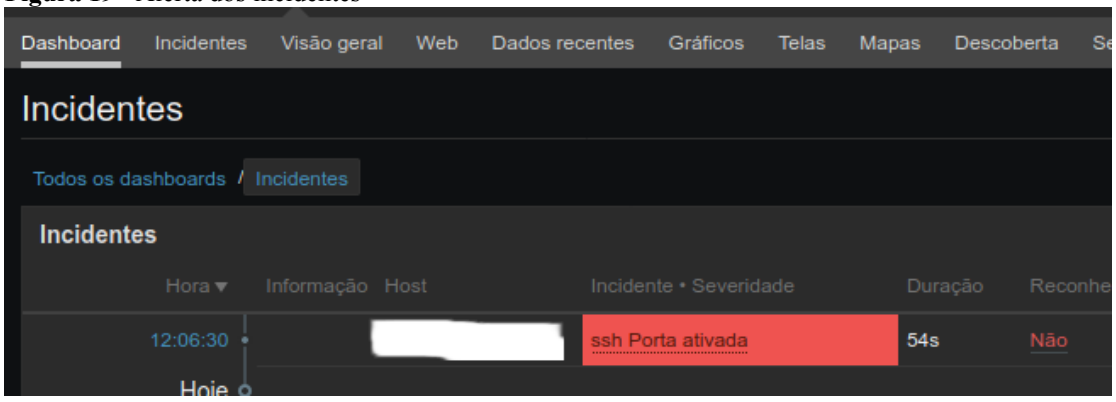
Figura 18 - Após as alterações de segurança



Fonte : Aurélio Malheiros (2020)

Finalizado as alterações, foram iniciados os testes somente em um servidor Linux para monitoramos as portas do sistema operacional, para isso, adicionamos a *template* em um dos servidores monitoramento da empresa e aguardamos a reposta de varredura de portas ser apresentando na *dashboard* como mostra a figura 19**.**

Figura 19 - Alerta dos incidentes



Fonte : Aurélio Malheiros (2020)

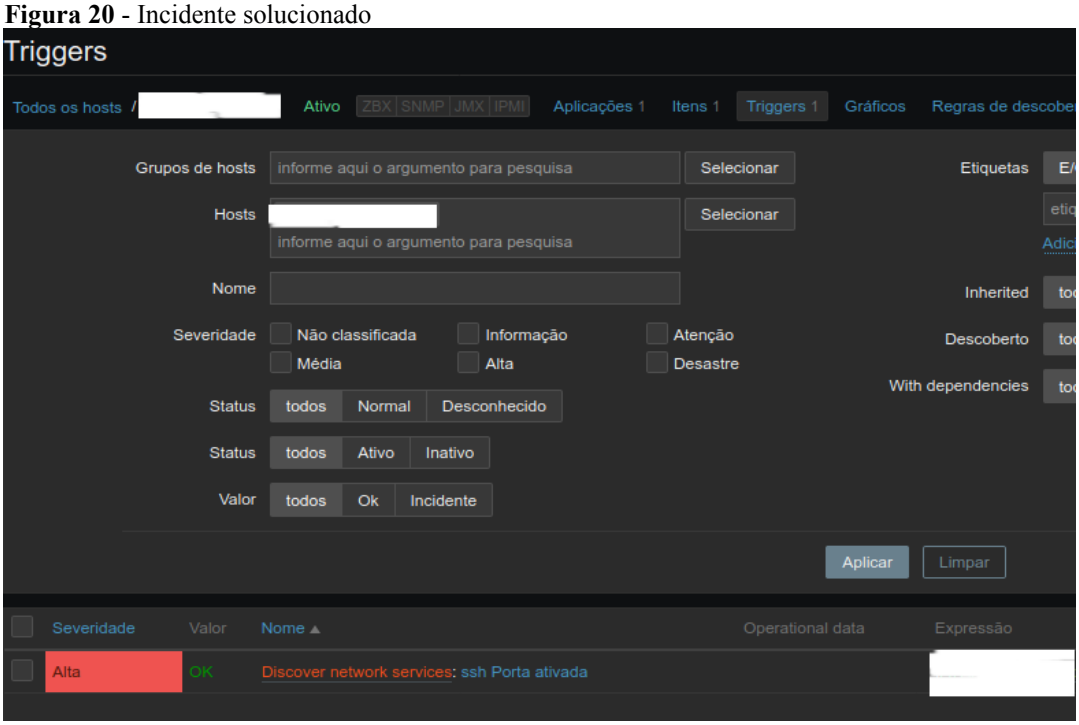
Visualizado o incidente, foram inicializados os procedimentos de segurança para que essa porta não estivesse aberta ao mundo virtual e somente para quem realmente fosse

utilizar esse tipo de acesso, nesse caso foram feitos os bloqueios dentro da lista de controle de acesso, isso significa que é feito a liberação apenas para um grupo específico de pessoas, Ips, sistemas operacionais ou grupos de segurança.

Portanto, foi possível automatizar o trabalho do profissional de T.I. sem que fosse necessário o mesmo intervir manualmente no ambiente, fazendo o uso da descoberta de baixo nível e além disso se torna automatizado a verificação da segurança da organização, sendo necessário apenas garantir que a lista de controle de acesso aos sistemas esteja de acordo com as politicas de segurança do ambiente. Dessa forma, os administradores de rede podem se preocupar com outros itens dos clientes, logo que a segurança das portas já se está sendo monitorada pelo Zabbix de forma totalmente automatizada.

Depois de ser feito as alterações de segurança, foi possível visualizar o incidente sendo solucionado no Zabbix, dessa forma foi possível validar que os servidores Linux estavam sendo monitorados e os administradores de rede conseguiam melhorar a segurança do ambiente. Na figura 20 é possível visualizar o incidente solucionado.

Figura 20 - Incidente solucionado



Fonte : Aurélio Malheiros (2020)

O estado de solução do incidente é possível visualizar ao lado de severidade em ok, isso significa que foi solucionado o problema. Dessa forma, o projeto foi implantado no

ambiente sendo fundamental, para os administradores verificarem quais as vulnerabilidades descobertas e como eles vão agir para solucionar os incidentes encontrados.

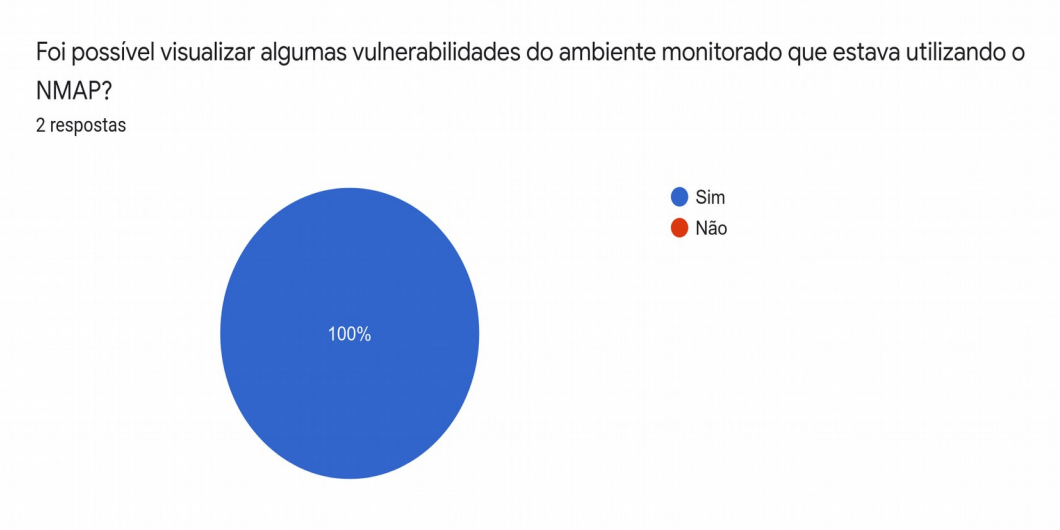
No caso dos servidores Linux, as portas ssh foram fechadas para somente na rede privada ou via VPN ser possível utilizar os seus recursos, isso reduz as chances de acontecer algum tipo de ataque no ambiente. E todas as regras utilizadas, foram aplicadas dentro da lista de controle de acesso e firewalls.

6.3 Resultados finais

Na CorpX, foi implementado somente em um ambiente monitorado, para primeiro a empresa ter uma visão se realmente o projeto poderia ser útil para eles e com isso da continuidade para outros clientes, depois disso será possível da continuidade do projeto. Por esse motivo, foram feitas perguntas após a implantação para saber os mesmos acharam o projeto útil e se pensam dar continuidade ao mesmo.

Na primeira pergunta, como mostra na figura 21, o intuito era saber se todos conseguiram visualizar as vulnerabilidades do ambiente de forma clara, assim também era necessário saber se realmente dava uma resposta clara para a equipe responsável pelo monitoramento e se os profissionais enxergavam o acompanhamento dos serviços de rede de forma automatizada útil para empresa.

Figura 21 - Visualização do monitoramento de vulnerabilidades



Fonte: Aurélio Malheiros (2020)

A próxima pergunta, que é apresentada na figura 22, teve como objetivo saber se os profissionais acham útil a automação de verificação de vulnerabilidades e se existe a possibilidade de dar continuidade ao projeto, ou seja, aplicar em todos os clientes da empresa

e corrigir todas as vulnerabilidades, já que, o ambiente monitorado utilizando o NMAP foi possível visualizar algumas falhas de segurança, logo após isso foi feito a correção das mesmas.

Figura 22 - A aplicação em outros clientes

Fonte:Aurélio Malheiros (2020)

Portanto, foi possível perceber que além dos profissionais conseguirem visualizar todas as vulnerabilidades do ambiente monitorado, é possível ver também que os mesmos pensam em dar continuidade, ao projeto de monitoramento de serviços dentro de outros clientes, para assim ter uma resposta mais rápida sobre serviços que estão abertos ao mundo ou mesmo que não deveriam estar abertos.

7 TRABALHOS RELACIONADOS

Neste capítulo serão apresentados diversos trabalhos que também se referem ao tema semelhante aos que foi escrito nesse trabalho de conclusão de curso, entretanto estão sendo aplicados em ambientes diferentes.

a. Subvertendo um sistema de detecção de intrusão: caso pratico utilizando o snort e NMAP. Biauzius, Mauricio Branco (2016)

Este trabalho de autoria Biauzius, Mauricio Branco (2016) tem por objetivo apresentar tanto o Snort, que é uma ferramenta de detecção de intrusão (IDS), tem por objetivo fazer uma análise na rede com intuito de alertar possíveis ataques, Branco (2016), também afirmar que o seu funcionamento é baseado em regras, ou seja, a análise é feita de acordo com a necessidade do administrador de rede.

Da mesma forma, o autor apresenta o NMAP que é uma ferramenta utilizada para escaneamento de redes, onde ele coleta as informações baseando-se no envio de pacotes para um determinado *host* e assim conseguir informações relevantes, por exemplo, nome do *host* e serviços que estão rodando nele.

Branco (2016), apresenta na sua obra uma forma de analisar uma rede sem ser detectado por ferramentas de IDS, desse modo o mesmo apresenta as vulnerabilidades dessas ferramentas e que mesmo com toda robustez de determinados sistemas (Firewall, IDS, IPS, entre outros) é possível fazer uma varredura detalhada e coletar informações sobre uma determinada rede.

b. Teste de invasão: Um relato de experiência em uma instituição pública de ensino no Brasil. Silva, Thiago Francisco de Andrade (2019)

Nesta obra o autor apresenta como foi feito a verificação das vulnerabilidades na instituição de ensino Universidade Federal Rural de Pernambuco, descrevendo detalhadamente cada passo feito nesses testes dentro da instituição, além disso é apresentado o conjunto de ferramentas utilizadas no processo, como mostra a figura 23. Todas as tecnologias listadas na imagem, foram aplicadas para análise do ambiente ou então para efetuar algum tipo de ataque.

Figura 23 - Quadro de ferramentas

Ferramenta	Etapa	Descrição
Kali Linux	Teste de Invasão	Sistema Operacional
Nmap	Coleta de Informação	Mapeamento de Rede
Nbtscan	Coleta de Informação	Mapeamento de Rede
Nessus	Mapeamento de Vulnerabilidade	*Scanner* de Vulnerabilidade
Metasploit	Exploração	Exploração de Vulnerabilidade
Aircrack-NG	Exploração	Quebra de Senha

Fonte : Andrade (2019)

No projeto, foi feito aplicado o NMAP para verificar todos os *hosts* ativos na rede e suas possíveis vulnerabilidades, ou seja, foi feito uma divisão das etapas para a exploração do ambiente, dessa forma cada uma delas era aplicado alguma das ferramentas listadas na figura 23.

O principal objetivo do autor, é apresentar que qualquer instituição mesmo tendo uma equipe de Tecnologia da informação (T.I.) está propícia a vulnerabilidades e as mesmas não podem ser menosprezadas, principalmente quando falamos de ambientes empresariais sendo públicos ou privados, já que, nessas instituições carregam informações sigilosas de diversas pessoas. E Silva (2019), deixou claro isso quando apresentou em seu artigo o conjunto de vulnerabilidades da instituição de ensino superior UFRP, da mesma forma que o autor Biauzius (2016) explorou uma falha na segurança do Snort.

7.1 Análise de trabalhos relacionados

Após ser apresentado os dois trabalhos agora vamos analisar onde cada trabalho se assemelha e onde cada um deles se diferencia, apresentando de forma bem clara a ideia de cada um dos autores e se os seus resultados foram esperados, dessa forma analisando o uso das tecnologias e suas aplicações.

Os dois autores aplicaram o NMAP com intuito de fazer o mapeamento de rede e descobrir possíveis vulnerabilidades, onde o interesse principal era apresentar que os administradores de rede devem sempre ficar atentos as vulnerabilidades do seu ambiente e com isso sempre melhorando a sua segurança.

As diferenças é que Silva (2019) faz um uso mais básico do NMAP com o objetivo apenas de descobrir os hosts e portas abertas no ambiente e com isso fez o uso de outras tecnologias para fazer o restante da exploração, enquanto Biauzius (2016) explorou diversos recursos do NMAP com intuito analisar um determinado *host* sem que o mesmo

detectasse, outro ponto importante a ser observado é que, enquanto Silva (2019) faz um projeto prático o Biausius (2016) apresenta um laboratório com algumas máquinas virtuais.

No caso, podemos citar que a área de estudo comum entre os trabalhos são: Segurança da informação, redes de computadores, NMAP, análise de redes, monitoramento de rede, vulnerabilidades, programação, automação, Zabbix, dentre outros. Abaixo vamos lista na tabela 1 uma comparação entre os três trabalhos.

Tabela 1: Comparação entre os trabalhos

	Subvertendo um sistema de detecção de intrusão: caso pratico utilizando o snort e NMAP	Teste de invasão: Um relato de experiência em uma instituição pública de ensino no Brasil	Análise de tráfego de redes: A automação do NMAP para garantia de segurança dos dados
Segurança da informação:	X	X	X
Redes de computadores	X	X	X
NMAP	X	X	X
Análise de redes	X	X	X
Monitoramento de rede	X		X
Vulnerabilidades	X	X	X
Automação			X
Programação			X

Fonte: Aurélio Malheiros (2020)

Como foi apresentado acima, temos a tabela listando uma comparação sobre os trabalhos e os seus respectivos assuntos abordados, onde podemos perceber que existe uma grande semelhança entre os três trabalhos, entretanto a diferença que podemos notar é sobre a automação de tarefas e uso da programação na verificação dessas vulnerabilidades, ou seja, é implementado dois itens para verificação desses problemas.

8 CONCLUSÃO

A finalidade desse trabalho foi demonstra como a automação de tarefas é útil para os administradores de rede, mas além disso apresentar o NMAP como uma ferramenta fundamental para o mapeamento de rede, e como sua utilidade pode ser aplicada para verificar as vulnerabilidades dentro do ambiente administrado. Dessa forma, promovendo uma flexibilidade no trabalho dos profissionais de rede.

Para aplicação do projeto foi necessário fazer o uso de diversas tecnologias, onde a principal foi a ferramenta de mapeamento de redes NMAP, que a mesma era responsável por mapear as portas abertas dos serviços. A linguagem de programação Shell Script, foi útil para conseguir automatizar a leitura das portas dentro do servidor Zabbix, também foi aplicado no monitoramento do Zabbix para confirmarmos se realmente a aplicação do projeto era funcional.

O Zabbix, foi uma peça fundamental para conclusão do projeto, já que, pela própria documentação o mesmo tinha capacidade de fazer a leitura de *scripts* instalado dentro do servidor sendo indispensável apenas da as devidas permissões para todos os que forem instalados dentro do servidor. Além disso, outro ponto importante foi a vasta documentação da ferramenta, em que se tornou muito proveitoso o seu uso, pois nela continha todas as informações para configuração do ambiente.

Para isso, é feito o uso da descoberta de baixo nível, dando a possibilidade da criação de *triggers* e itens de forma totalmente automatizada. Outra vantagem para o uso do LLD, é ser possível monitorar diversos itens dentro de um ambiente empresarial sem que seja necessários diversas configurações dentro do *frontend* do Zabbix.

Foi desenvolvido um protótipo para fazer todos os testes possíveis, e com isso ser possível saber se realmente poderia ser aplicado o NMAP dento do Zabbix, como poderia ser feito, quais os possíveis problemas e quais as vantagens de fazer o uso do NMAP integrado ao Zabbix. A elaboração do projeto foi dividido em etapas onde cada uma foi feito diversas tarefas até ocorrer a conclusão dos testes.

a) Configuração do VirtualBox
b) Instalação e configuração dos três servidores
c) Instalação do Zabbix e configuração do ambiente de monitoramento
d) Instalação do agente nos servidores a serem monitorados
e) Configuração da descoberta de baixo nível
f) Teste nos servidores a serem monitorados
g) Integração do Zabbix com o telegram para se ter uma resposta mais rápida

Foi feito uma implantação em um ambiente prático, para se ter uma visão do impacto que é gerado em um ambiente real. Entretanto, foi solicitado que todos os dados fossem mantidas em sigilo para que não ocorresse nem um tipo de vazamento das informações dos clientes administrados pela empresa, com isso o projeto ficou limitado a poucas informações, não sendo possível revelar nem mesmo o nome dos colaboradores.

Portanto, foi possível visualizar que aplicação do NMAP é útil para garantir a segurança de um ambiente empresarial, já que, automatiza o trabalho do administrador de redes, sem que seja necessário a intervenção do mesmo no ambiente administrado constantemente, ou seja, se torna mais simples a visualização das vulnerabilidades do ambiente e com isso também, fácil a correção das mesmas.

8.1 Dificuldades encontradas

Para o desenvolvimento desse trabalho, foi enfrentado algumas dificuldades até a sua conclusão, uma parte era por falta de conhecimento nas tecnologias utilizadas e a outra era por conta das pessoas que muita vezes tinham uma certa resistência em relação ao uso do NMAP. Um outro contratempo, foi a falta de recursos de hardware para fazer os testes em laboratório e com isso foi necessário fazer a aquisição de hardware para conseguir desenvolver o projeto.

Foram feitas diversas tentativas para desenvolver o projeto, a primeira tentativa foi desenvolver uma plataforma web para fazer o escaneamento dos ativos de rede e via interface web apresentar as portas que estavam abertas e com isso automatizar o trabalho do administrador de sistemas.

Foi elaborado um projeto, que o intuito era desenvolver uma ferramenta utilizando a linguagem de programação Python e a biblioteca nmap3, onde sua funcionalidade iria ser da seguinte forma, era instalado dentro de um servidor e constantemente rodaria

o algoritmo no mesmo, após algum tempo o relatório iria ser enviado por e-mail e sua leitura poderia ser feita utilizando PowerBI, entretanto um dos principais pontos desse trabalho não era respeitado, que é a automação de tarefas, por esse motivo o projeto foi abandonado.

Foi necessário estudar e aprofundar ainda mais os estudos relacionados a desenvolvimento, expressões regulares, sistemas operacionais Linux e monitoramento. Já que, tonaram-se fundamentais para a elaboração do projeto e continuidade do mesmo, com isso foi

necessário criar um plano de estudos para desenvolver e aplicar o trabalho de forma que fosse possível entregar o que estava sendo proposto.

Outro ponto que vale frisar neste trabalho, é a falta de conhecimento em relação ao NMAP, muitas instituições acreditam que a ferramenta tem a única funcionalidade para ataques, e só é utilizado por criminosos para levantar informações sigilosas de empresas. Com isso, a implantação prática do projeto se tornou difícil, mesmo citando que seu uso é recomendado pelos próprios desenvolvedores do Zabbix.

E o problema é mencionado por Lyon (2009), criador do NMAP, onde descreve o problema em relação escaneamento de portas, entretanto o mesmo relata que existem algumas instituições que fazem o seu uso para verificar a disponibilidade dos serviços, saber quais tipos de serviços estão rodando no ambiente e principalmente quais as principais vulnerabilidades existem no local administrado.

8.2 Trabalhos futuros

Além do que já foi desenvolvido para esse projeto, foi pensado em alguns planos para desenvolvimento futuro que são melhorias, novas funcionalidade e até mesmo desenvolvimento de projeto que não use a ferramenta Zabbix. Isso é uma forma de trabalhar com a melhoria contínua desse projeto para que o mesmo continue sendo útil para comunidade.

a) Automatizar o processo de monitoramento de portas: Percebe-se, que são diversos passo para que seja possível monitorar os serviços utilizando o NMAP, portanto o próximo passo é diminuir ainda mais a quantidade de passos, ou seja, com alguns cliques já seja possível utilizar os recursos do mapeamento de portas em um ambiente de monitoramento.

b) Monitorar não somente os serviços de um ambiente corporativo: Sabe-se que é de grande importância saber todas as possíveis vulnerabilidades em um ambiente corporativo e uma das formas que foi apresentado nesse projeto é o monitoramento das portas que estão abertas, porém o NMAP também dá a possibilidade de descobrir as vulnerabilidades de um ambiente de diversas formas sendo automatizado, por exemplo, é possível descobrir se determinado *firmware* de um *firewall* tem alguma falha de segurança, detectar *malwares*, entre outros, dessa forma, tem-se maior controle do ambiente monitorado.

c) Desenvolvimento de uma ferramenta Web: Um projeto que foi pensado, é o de desenvolvimento de uma ferramenta *Web* capaz de monitorar todo o ambiente do cliente entregar utilizando NMAP sem a necessidade do uso de tecnologias de terceiros como o

Zabbix, o intuito dela é de verificar quais os serviços abertos no ambiente, as principais falhas de segurança, geração de relatórios e apresentar um conjunto de procedimentos básicos que podem ser feitos no ambiente para melhoria da segurança.

9 REFERÊNCIAS

BIAUZUS, Mauricio Branco. **Subvertendo um sistema de detecção de intrusão: Caso prático utilizando o Snort e NMAP**. 2016. 87 f. Monografia. Curso de sistema de informação, Universidade Federal de Santa Catarina, Florianópolis, 2016.

CAETANO, Lauro de Lacerda. **Redes Veiculares: Tendências e Estudo de Caso**. Rio De Janeiro: 2016. Disponível em: <https://www.researchgate.net/figure/Figura-3-Modelo-OSI-e-TCP-IP_fig1_310193861>. Acesso em: 8 Set de 2020.

FILHO, João Eriberto Mota. **Análise de tráfego em redes TCP/IP: Utilize tcpdump na análise de tráfegos em qualquer sistema operacional.** São Paulo: Novatec Editora 2013.

FILHO, João Eriberto Mota. Scripts em Shell Bash. In:_____. **Descobrindo o Linux: Entenda o sistema operacional GNU/Linux.** São Paulo: Novatec Editora, 2012. Cap. 25, p 455-484.

FILIPPETTI, Marco Aurélio. Modelo OSI. In: _____. **CCNA 6.0 Guia completo de Estudo.** Florianópolis: Visual Books, 2017. Cap. 2, p. 31-71.

FILIPPETTI, Marco Aurélio. Modelo TCP/IP. In: _____. **CCNA 6.0 Guia completo de Estudo.** Florianópolis: Visual Books, 2017. Cap. 4, p. 111-137.

GAIDARGI, Juliana. **Tudo sobre estrátegia de automação de T.I.** São Paulo: 2019. Disponível em: <https://www.infonova.com.br/fale-conosco/>.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. In:_____. **Métodos das ciências sociais.** São Paulo: Atlas, 2008. Cap. 2, p. 8-25.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. In:_____. **Pesquisa social.** São Paulo: Atlas, 2008. Cap. 3, p. 26-32.

HINTZBERGEN, Jule. Definição e conceitos de segurança. In: _____. **Fundamentos de segurança da informação: Com base na ISO 27001 e na ISO 27002.** São Paulo: Brasport, 2018. Cap. 4, p. 64-28.

SILVA, Thiago Francisco de Andrade. **Teste de invasão: um relato de experiência em uma instituição publica de ensino no Brasil**. 2019. 50 f. Monografia. Curso de sistema de informação, Universidade Federal Rural de Pernambuco, Serra Talhada, 2019.

LIMA, Jassen dos Reis. **Monitoramento de redes com Zabbix: Monitore a saúde dos servidores e equipamentos de rede.** Rio de Janeiro: BRASPORT Livros e Múltimidia, 2014.

LYON, Gordon. Iniciando-se com NMAP. In:_____. **Exame de redes com NMAP**. Rio de Janeiro: Ciência Moderna Ltda, 2009. Cap. 1, p. 1-32.

LYON, Gordon. Visão geral do exame de portas. In:_____. **Exame de redes com NMAP**. Rio de Janeiro: Ciência Moderna Ltda, 2009. Cap. 4, p. 115-150.

LYON, Gordon. Defesas contra o NMAP. In:_____. **Exame de redes com NMAP**. Rio de Janeiro: Ciência Moderna Ltda, 2009. Cap. 11, p. 467-484.

MARCIANO, João Luiz Pereira. **Segurança da informação: Uma abordagem social**. UNB Brasília: 2006. Disponível em: <https://repositorio.unb.br/handle/10482/1943>

MELO, Sandro. Capítulo 5. In:_____. **Exploração de Vulnerabilidades em Redes TCP/IP.** Rio de Janeiro: Alta Books, 2017. Cap. 5, p. 63-126.

MORCH, Martin. **Monitor network services automatically**. Zabbix.tips: 2016. Disponível em : <https://zabbix.tips/monitor-services-automatically/>. Acesso em: 20 de Set. de 2020.

SWEIGART, AI. **Automatize tarefas maçantes com Python.** São Paulo: Novatec Editora 2015.

SOUZA, Marco Antonio Furlan.Introdução. In:_____. **Algoritmo e Lógica de programação.** São Paulo: Cengage Learning, 2011. Cap. 1, p 1-24.

SILVA, Pedro Tavares. Teoria da segurança. In:_____.**Segurança dos sistemas de informação: Gestão estratégica da segurança empresarial**. Lisboa: Centro Atlântica LDA. Cap. 1, p. 17- 33.

VERAS, Manoel. Conceitos Centrais. In:_____. **Virtualização: Tecnologia central do DataCenter.** Rio de Janeiro: Brasport, 2016. Cap. 3, p 37-48

VIRTUALBOX, **Welcome to VirtualBox.org**. Disponível em : <https://www.virtualbox.org/ >. Acesso em: 20 de Set. de 2020.

TANENBAUM, Andrew Stuart. Uso de redes de computadores. In:_____. **Redes de computadores**. São Paulo: Pearson Education do Brasil, 2011. Cap. 1, p. 1-52.

TANENBAUM, Andrew Stuart. Camada de transporte. In:_____. **Redes de computadores**. São Paulo: Pearson Education do Brasil, 2011. Cap. 6, p. 310-380.

TANENBAUM, Andrew Stuart. Segurança de redes. In:_____. **Redes de computadores**. São Paulo: Pearson Education do Brasil, 2011. Cap. 8, p. 310-380.

TOLKIEN, J. R. R. Livro II Capitulo III: O Anel vai para o sul. In:_____. **Senhor dos anéis: A sociedade do Anel.** São Paulo: USP, 2001. Cap. 3, p. 344-362.

TORRES, Fábio Cabral. **Conceitos e princípios da segurança da informação.** In: LYRA, Maurício Rocha. Governança da segurança da informação. Editor do Autor, 2015. p. 9-20.

Kurose, James F. Redes de computadores e a internet. In:_____. **Redes de computadores e a internet: Uma abordagem Top-Down**. São Paulo: Pearson Education do Brasil, 2013. Cap. 1, p. 1-58.

Kurose, James F. Camada de Transporte. In:_____. **Redes de computadores e a internet: Uma abordagem Top-Down**. São Paulo: Pearson Education do Brasil, 2013. Cap. 3, p. 135-222.

Kurose, James F. Segurança em redes de computadores. In:_____. **Redes de computadores e a internet: Uma abordagem Top-Down**. São Paulo: Pearson Education do Brasil, 2013. Cap. 3, p. 495-553.