INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE - CAMPUS PASSO FUNDO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

RENATO WAGNER ANUNCIAÇÃO

ANÁLISE DA USABILIDADE DE FERRAMENTAS DE MONITORAMENTO E DETECÇÃO DE VULNERABILIDADES EM REDES DE COMPUTADORES

João Mário Lopes Brezolin

PASSO FUNDO
2018

RENATO WAGNER ANUNCIAÇÃO

ANÁLISE DA USABILIDADE DE FERRAMENTAS DE MONITORAMENTO E DETECÇÃO DE VULNERABILIDADES EM REDES DE COMPUTADORES

Monografia apresentada ao Curso de Tecnologia em Sistemas para Internet do Instituto Federal Sul-rio-grandense, Câmpus Passo Fundo, como requisito parcial para a obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador (a): Prof. Dr. João Mário Lopes Brezolin

PASSO FUNDO

2018

AGRADECIMENTOS

Agradeço muito ao professor João Mário Lopes Brezolin, que acreditou e me ajudou com várias contribuições com suas orientações excelentes. A todos os professores do Instituto Federal Sul Rio-Grandense que passaram um ótimo conhecimento durante a minha vida acadêmica.

Agradeço aos meus amigos que me apoiaram e acreditaram que seria possível fazer um ótimo trabalho de conclusão.

EPÍGRAFE

“Se houver várias maneiras de executar a mesma tarefa, escolha apenas uma. Ter duas ou mais maneiras de fazer o mesmo está procurando por problemas.”

Andrew S. Tanenbaum

RESUMO

O objetivo deste estudo é avaliar a usabilidade de ferramentas de detecção de vulnerabilidades de segurança de redes de computadores. As determinadas ferramentas de segurança verificam se existem vulnerabilidades nos serviços que ficam instalados no servidor. Algumas ferramentas funcionam em tempo real, exibindo os dados sobre determinados serviços e seus respectivos estados. Outras, no entanto exigem a ação direta do usuário para realizar o escaneamento, apenas exibindo problemas, caso os mesmos existam. Entretanto, faz-se necessário avaliar se as informações exibidas pelas mesmas são intuitivas e podem auxiliar o administrador de rede no processo de tomada de decisão. Com base nisso foram realizados testes com usuários que possuem um conhecimento básico na área de redes para avaliar a usabilidade das ferramentas de detecção de vulnerabilidades, visando analisar se o uso das mesmas é intuitivo e se ajudam o administrador a tomar medidas preventivas para coibir ataques. Ao final deste trabalho foi possível fazer a avaliação sobre as ferramentas de detecção de vulnerabilidades com sucesso, onde dois usuários fizeram teste com as ferramentas e através dos mesmos foi possível considerar qual a melhor ferramenta pode ser usada por administradores de redes.

Palavras-chave: Segurança em rede de computadores, Usabilidade, Ferramentas de monitoramento e detecção de vulnerabilidades.

ABSTRACT

The objective of this study is to evaluate the usability of tools for detection of security vulnerabilities of computer networks. The certain security tools verifies if there are vulnerabilities in services that are installed on the server. Some tools work in real-time, displaying the data on certain services and their respective states. Others however require the direct action of the user to perform the scanning, only displaying problems, if they exist. However, it is necessary to assess whether the information displayed by the same are intuitive and can help the network administrator in the decision making process. On this basis were performed tests with users who have a basic knowledge in the area of networks to assess the usability of the tools of detection of vulnerabilities, aiming to analyze if the use of the same is intuitive and help the administrator to take preventive measures to curb attacks. At the end of this work, it was possible to make the evaluation on the tools of detection of vulnerabilities with success, where two users did test with the tools and through the same was possible to consider network administrators can use what is the best tool.

Keyboards: Security in a network of computers, Usability, Tools for monitoring and detecting vulnerabilities.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

API - Application Programming Interface
ccTLD's - country code Top Level Domains
DHCP - Dynamic Host Configuration Protocol
DNS - Domain Name Servers
DOS – Denial of Service
FTP - File Transfer Protocol
GNU - GNU is Not Unix
GPL – General Public License
gTLD - generic Top-Level Domain
HTTP - Hypertext Transfer Protocol
HTTPS - Hypertext Transfer Protocol Secure
IMAP - Internet Mail Access Protocol
IP - Internet Protocol
IPv4 - Internet Protocol version 4
MIB - Management Information Base
OS/2 - Operating System 2
POP3 - Post Office Protocol
SMTP - Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SO - Sistema Operacional
SSH – Security Shell
SSL – Secure Socket Layer
TCC – Trabalho de Conclusão de Curso
TLD's - Top Level Domains
UFSM - Universidade Federal de Santa Maria
URL - Uniform Resource Locator

SUMÁRIO

1 INTRODUÇÃO

A importância nos dias de hoje em se utilizar uma ferramenta de detecção de vulnerabilidades ao administrador de redes é de extrema relevância. O que as ferramentas auxiliam é um fator primordial, ou seja, com as informações disponibilizadas fica mais fácil o controle dos dados que são transmitidos, para um melhor controle da rede.

Atualmente vive-se em um mundo conectado no qual as pessoas realizam através dos meios informatizados diferentes tipos de atividades. Por meio da internet, é possível realizar transações bancárias, enviar e-mail e usar a nuvem para guardar dados importantes. No entanto, é necessária a garantia de que estes dados estejam seguros. Nesse sentido, é importante estabelecer mecanismos para verificar o quanto os mesmos estão seguros, pois alguns serviços de redes podem deixar seus dados desprotegidos. Para que haja segurança, de modo que os dados corram menor risco de serem sequestrados, deve-se realizar testes para verificar a existência de vulnerabilidades. Caso exista alguma, o administrador de redes deverá tomar medidas cabíveis para que isso não venha ocorrer novamente.

Para avaliar esses ambientes, faz-se necessário utilizar um conjunto de ferramentas de segurança que verifiquem problemas e falhas nos servidores que armazenam dados.

1.1 OBJETIVOS

O objetivo deste Trabalho de Conclusão de Curso (TCC) é avaliar os recursos disponibilizados pelas ferramentas de monitoramento e detecção de vulnerabilidades verificando se eles auxiliam o administrador de rede na detecção de problemas e se o uso e configuração da ferramenta é intuitiva para o administrador.

1.2 Objetivo geral

Avaliar a eficácia e a usabilidade de ferramentas de detecção de vulnerabilidades da segurança de redes de computadores disponíveis para o sistema operacional Debian/Linux.

1.3 Objetivos específicos

- Realizar a revisão bibliográfica acerca dos conceitos de segurança de redes;
- Avaliar trabalhos relacionados ao tema da pesquisa;
- Revisar os conceitos de eficácia e usabilidade;
- Implementar um ambiente para testes no servidor Debian/Linux;
- Realizar e avaliar os testes com as ferramentas de detecção de vulnerabilidade no servidor Debian/Linux;
- Avaliar a interface das ferramentas com relação a sua usabilidade;

1.4 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está organizado como segue: no capítulo 2 o referencial teórico, no capítulo 3 aborda sobre as ferramentas de detecção e monitoramento de vulnerabilidades, no capitulo 4 a metodologia aplicada, no capitulo 5 as considerações finais sobre os testes.

2 REFERENCIAL TEÓRICO

Esta seção apresenta o embasamento teórico sobre a segurança de redes de computadores abordando o conceito geral e qual seus objetivos. Após é exposto o conceito de vulnerabilidades que os sistemas podem possuir através de softwares ou de portas abertas em serviços configurados que não utilizam nenhum método de segurança avançado. E também visa destacar a importância em utilizar-se ferramentas de segurança que ajudam na detecção de vulnerabilidades e que são de grande apoio aos administradores de redes.

2.1 SEGURANÇA DE REDES

Segundo Tanembaum (2003), a segurança em redes em computadores nas primeiras décadas de sua existência não necessitou de muitos cuidados, pois era utilizada principalmente por universitários para correio eletrônico e funcionários de empresas que precisavam compartilhar impressoras. Mas com o grande crescimento dos meios informatizados tornou o acesso aos serviços mais facilitado.

Com isso, foi preciso criar regras para que o acesso fosse protegido, pois quando se utiliza a rede você pode enviar qualquer tipo de informação. E essas informações, estando seguras, faz com que a quantidade de usuários aumente gradativamente.

A política de segurança é um conjunto de regras sobre o que deve ser feito para garantir proteção conveniente às informações e serviços importantes para a empresa (FERREIRA; ARAÚJO, 2008). Confiabilidade, integridade e disponibilidade são características necessárias para a segurança de redes. Toda a informação deve chegar de forma íntegra e confiável, para isso, todos os elementos de rede por onde os dados serão transmitidos até chegar ao seu destino final devem estar disponíveis (NAKAMURA; GEUS, 2007)

Segundo Laureano (2005), os princípios básicos para garantir a segurança da informação são: limitar o acesso à informação, garantir que a informação não seja alterada e garantir que os usuários autorizados tenham acesso à informação.

A segurança da informação não trata apenas da proteção dos dados, mas da sua possibilidade em prevenir, fazer a monitoração e as respostas geradas por alguma invasão.

2.2 VULNERABILIDADES

Hoje em dia segundo *Alert* Security (2016), há uma grande discussão sobre a segurança da informação, a percepção do mercado e outros termos como a análise a vulnerabilidades**,** além de análise de risco e testes de penetração mais conhecidos como Pentest.

Vulnerabilidades podem ser chamadas de falhas ou fraquezas, por exemplo, uma parede rachada. Dentro de uma rede podemos encontrar está “rachadura”, ou falha, em um design mal planejado, implementação mal realizada, ou até em controles internos de um sistema mal realizado. Podem também serem criadas a partir de configurações erradas do computador ou de sua segurança. Quando se aborda sobre as vulnerabilidades. Também se abordam os riscos que estão ligados às vulnerabilidades. Segundo Alert Security (2016), “um risco é uma alternativa de perigo que contém ameaças, vulnerabilidades e a sua grandeza em se proteger.”

A análise de vulnerabilidades segundo Alert Security (2016), “tem como objetivos identificar falhas e vulnerabilidades que apontam para ameaças, as falhas podem ter erros de programação, uma configuração errada de algum serviço ou alguma falha humana.” Esse tipo de análise mapeia todos os sistemas que tendem a ter falhas e vulnerabilidades, gerando relatórios conclusivos do sistema em si. Através dessas informações pode-se tratar e solucionar as vulnerabilidades encontradas, buscando garantir uma maior e melhor segurança dos dados. A técnica de análise é mantida por várias ferramentas de segurança que serão avaliadas neste trabalho.

2.3 USABILIDADE

Segundo Nielsen e Loranger (2007), a usabilidade é um atributo de qualidade relacionado à facilidade do uso de algo. Refere se à rapidez com que os usuários conseguem aprender a utilizar determinada ferramenta, a eficiência deles ao usá-

las, o quanto lembram a forma de utilização, seu grau de propensão a erros e o quanto gostam de utilizá-las.

Para iniciar a abordagem de usabilidade de cada ferramenta de detecção de vulnerabilidade é necessário definir alguns pontos que proporcionem aos usuários. Segundo Tableless (2011) os critérios da usabilidade são: a facilidade do aprendizado, facilidade em memorizar, maximização da produtividade, minimização da taxa de erros e a maximização da satisfação do usuário.

Esses critérios serão utilizados para realizar a avaliação das ferramentas de detecção de segurança de redes de computadores. Com esse procedimento, o administrador de redes poderá escolher qual é a melhor ferramenta para se utilizar em sua corporação.

2.4 TRABALHOS RELACIONADOS

Já foram realizados estudos comparativos com a ferramenta Nagios em relação ao software Zabbix no que tange ao consumo dos recursos computacionais, o tráfego na rede que era feito pela troca de informações entre as máquinas, a precisão que os dados eram coletados e o tempo de resposta que a ferramenta respondia para o administrador (BORGES; VALENTIM; LIMAS; ANTUNES, 2015). Porém o estudo realizado não leva em consideração a questão da usabilidade da ferramenta. Além disso, propõe-se neste trabalho a comparação da mesma com outras ferramentas.

O Nessus é uma ferramenta amplamente utilizada e já foi avaliada em diferentes trabalhos como o realizado por Buzzatte (2014), que utilizou a mesma para detectar vulnerabilidades na rede da Universidade Federal de Santa Maria (UFSM).

O OpenVAS também foi avaliado no trabalho desenvolvido por Buzzatte (2014), concluindo que os softwares LanGuard, Nessus e o OpenVAS ajudam na descoberta de ativos de rede, ou seja, sistemas operacionais em execução, portas abertas, serviços, porém, neste não apresenta um estudo comparativo entre as ferramentas.

A ferramenta de monitoramento Cacti foi apresentada em um trabalho por Neto e Uchôa que fazem uma análise de ferramentas de monitoramento de vulnerabilidades que possuem o código aberto, que fazem a conclusão de que as

ferramentas de código aberto são capazes de exibir ao administrador de redes de forma eficiente e confiável as informações de toda a rede, avisá-lo sobre falhas ou outro mal funcionamento no servidor.

Entretanto poucos trabalhos se preocuparam em avaliar a usabilidade das ferramentas com demonstrações de simulações de ataques DOS, verificando se a ferramenta estava auxiliando o usuário a tomar alguma medida para prevenir a ocorrência.

3 FERRAMENTAS DE DETECÇÃO DE VULNERABILIDADES

A identificação e correção de vulnerabilidades relacionadas aos softwares é um grande problema enfrentado pelas empresas atualmente. Há evidencias que algumas empresas ainda utilizam softwares com vulnerabilidades conhecidas há anos. Nesse sentido, 44% das violações conhecidas em 2014 foram causadas por vulnerabilidades não fixadas que tinham entre dois a quatro anos de idade, segundo Microfocus (2016).

Por isso que as ferramentas de análise de redes são tão importantes. Algumas ferramentas atuam de forma semelhante ao antivírus realizando a varredura dos softwares instalados na intranet das empresas buscando vulnerabilidades. Geralmente estas ferramentas possuem um banco de dados com informações sobre os softwares instalados e as atualizações necessárias.

Para auxiliar na detecção de vulnerabilidades, faz-se necessário um estudo acerca das ferramentas de detecção de segurança disponíveis para verificar a usabilidade dos recursos que ela disponibiliza e de como esses podem vir a auxiliar o administrador de rede a detectar falhas e estabelecer parâmetros para que o mesmo possa corrigi-las. Para esse estudo foram escolhidas algumas ferramentas de monitoramento e detecção de vulnerabilidades que sejam *open source* para a realização dos testes.

3.1 FERRAMENTAS DE MONITORAMENTO

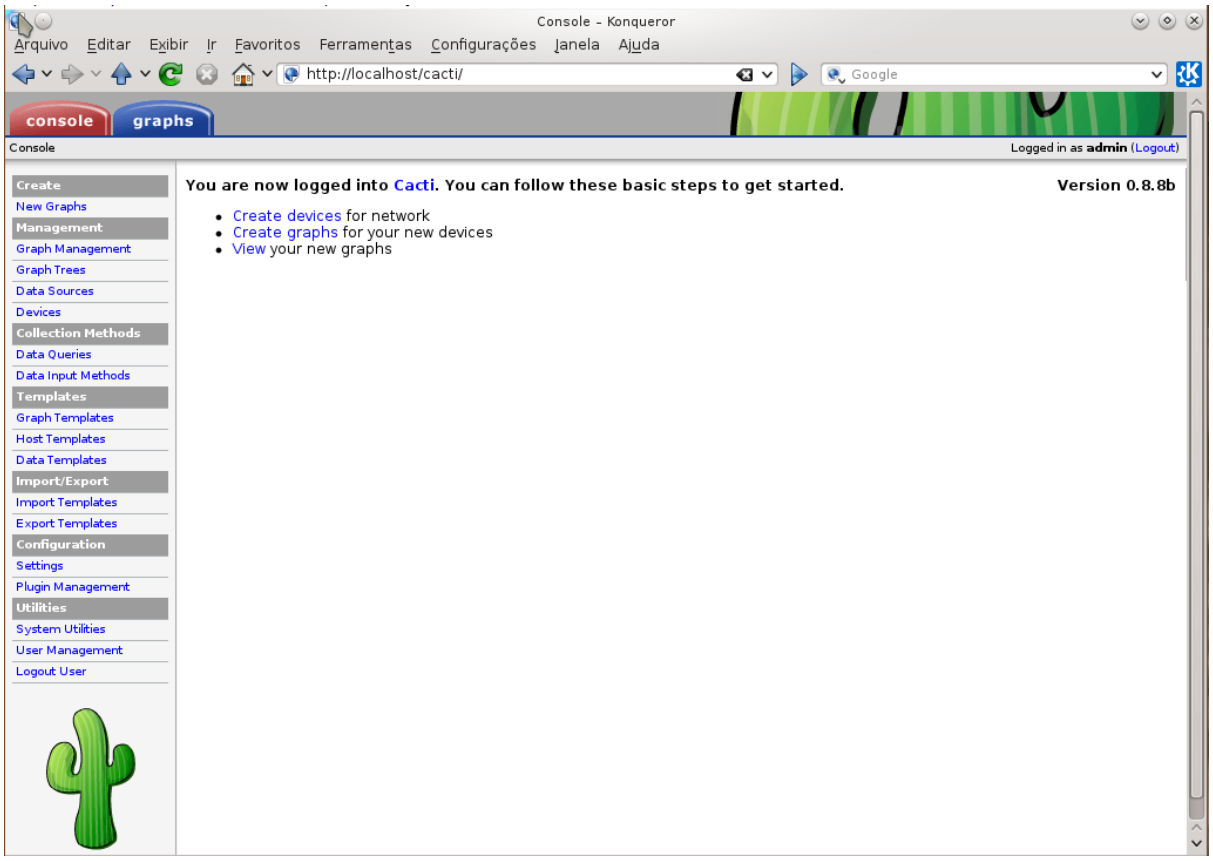
Nessa seção serão apresentadas as ferramentas CACTI e NAGIOS que estão classificadas como ferramentas de monitoramento em tempo real.

3.1.1 CACTI

Segundo Monolito Nimbus (2015), é uma ferramenta que monitora e analisa os dados sobre o desempenho de uma rede de computadores usando gráficos discriminados. Foi desenvolvida na forma que assegure facilidade e agilidade no processo de recebimento das informações. O software está fundamentado para atuar na organização do RRDTool (*Round Robin Database*).

O RRDTool é um sistema que tem como objetivo coletar periodicamente e inspecionar as informações obtidas sobre o estado dos serviços instalados em servidores de rede. Ele utiliza o SNMP (*Simple Network Management Protocol*), que é um protocolo de gestão estabelecido para aplicação e é utilizado para obter informações dos servidores SNMP. Na Figura 1, é exibida a interface inicial da ferramenta, sendo necessário passar por todo o processo de configuração para poder saber o que está acontecendo na rede.

Figura 01 - Interface inicial da ferramenta CACTI



Fonte: do Autor.

3.1.1.2 INSTALAÇÃO DA FERRAMENTA CACTI

Antes de iniciar a instalação, verificou-se se o servidor estava em sincronismo com o repositório do software.

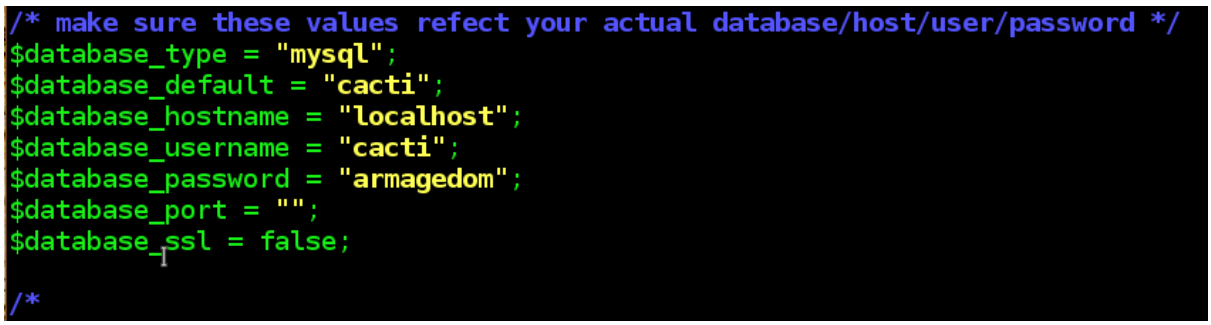
Caso o MySQL não esteja instalado no servidor, é necessário determinar uma nova senha para o administrador. No próximo passo, basta estabelecer qual servidor web seria usado selecionando o apache2. Após isso, foi configurado o banco de dados do Cacti automaticamente utilizando o comando “dbconfig-common” e

selecionou-se a opção “Yes”. Com esses processos executados, é fundamental inserir novamente a senha de administrador do MySQL, em seguida a senha para o novo usuário do banco de dados Cacti, onde irá utilizar essa senha para fazer a interação com o banco de dados MySQL.

É necessário editar o arquivo debian.php que é criado no momento da instalação da ferramenta.

Na Figura 02, é exibido um exemplo do arquivo de configuração do banco de dados MySQL. Na primeira linha define o banco de dados; na segunda o nome do banco que foi criado durante o processo anterior. Após, define-se o “hostname” como “localhost”; na quarta linha o nome do banco e por fim na quinta linha a senha do MySQL na penúltima e última linha não precisa editar.

Figura 02 - Arquivo de configuração do banco de dados MySQL



Fonte: do Autor.

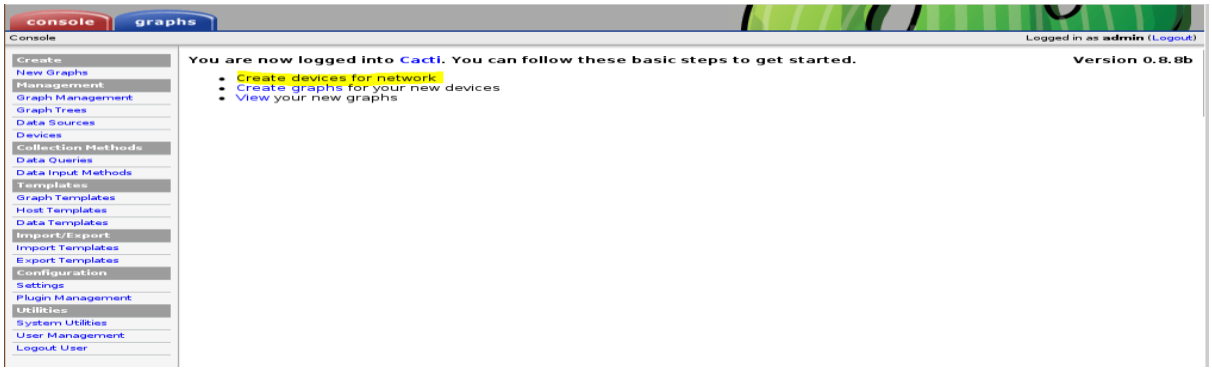
Passando por todos estes processos, entrou-se no browser e inseriu-se o seguinte endereço “http://localhost/cacti” para poder acessar a ferramenta.

Ao acessar esse endereço aparece uma tela de ajuda para a configuração. Selecionou-se o tipo de instalação, que foi “*New Install*”, clicou-se em next, em que foram abertas as configurações já selecionadas, que são as informações sobre caminhos binários dos serviços que a ferramenta utiliza.

Após é necessário clicar no botão “*finish*”. No primeiro acesso, solicita-se as informações do banco de dados e a sua senha. Na sequência, realiza-se o redirecionamento para a página de *login* do sistema. Por padrão, utiliza-se o nome de usuário “*admin*” e sua senha “*admin*”. Em seguida, é só fazer o login e utilizar a ferramenta da forma mais apropriada.

Com a ferramenta aberta, passa-se ao processo de configuração de um host. Na Figura 03, é mostrada a tela inicial e clicar em “*Create devices*”, que está demarcado em amarelo.

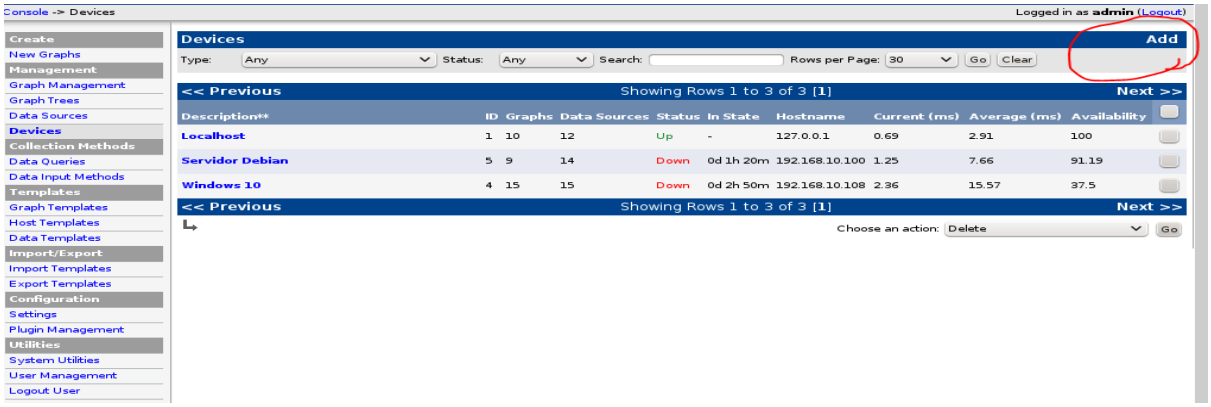
Figura 03 - Criando hosts para serem monitorados



Fonte: do Autor.

Para configurar um monitoramento inicialmente deve-se clicar-se no botão “add” para adicionar um novo host, que foi circulado em vermelho na Figura 04.

Figura 04 - Adicionar um host

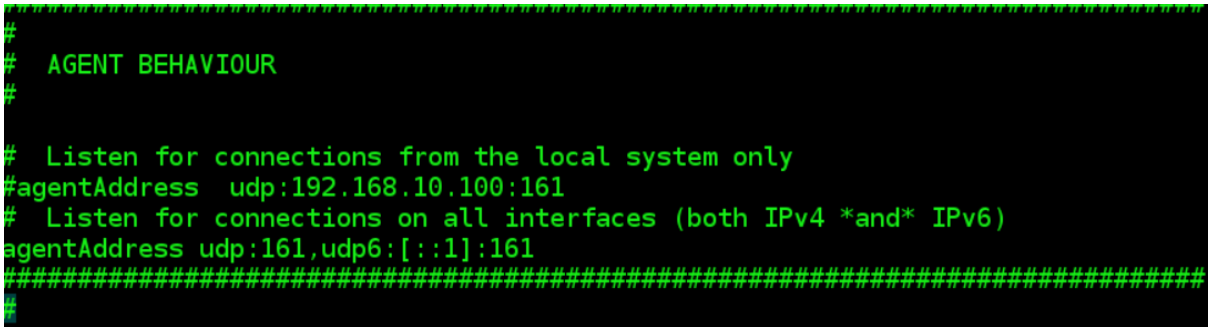


Fonte: do Autor.

Informaram-se os dados sobre o servidor a ser monitorado, na parte de “*General Host Options*” e inseriram-se algumas informações a respeito do host; em “description” o nome definido pelo usuário;- em “*hostname*”, o endereço IP da máquina;- em “*host template*”, seleciona-se “*Generic SNMP-enabled Host*”;- nas outras duas opções não é preciso selecionar nenhuma das opções. Em “*Availability* ou *Reachability Options*”, as opções já são selecionadas no momento em que o “*Host Template*” for escolhido como Generic SNMP.

Também é necessário fazer a instalação do SNMP (Figura 05) no host que será monitorado, já que este serviço faz a coleta das informações e as envia para a ferramenta, segundo Pessoa (2001).

Figura 05 - Configuração da porta que será utilizada

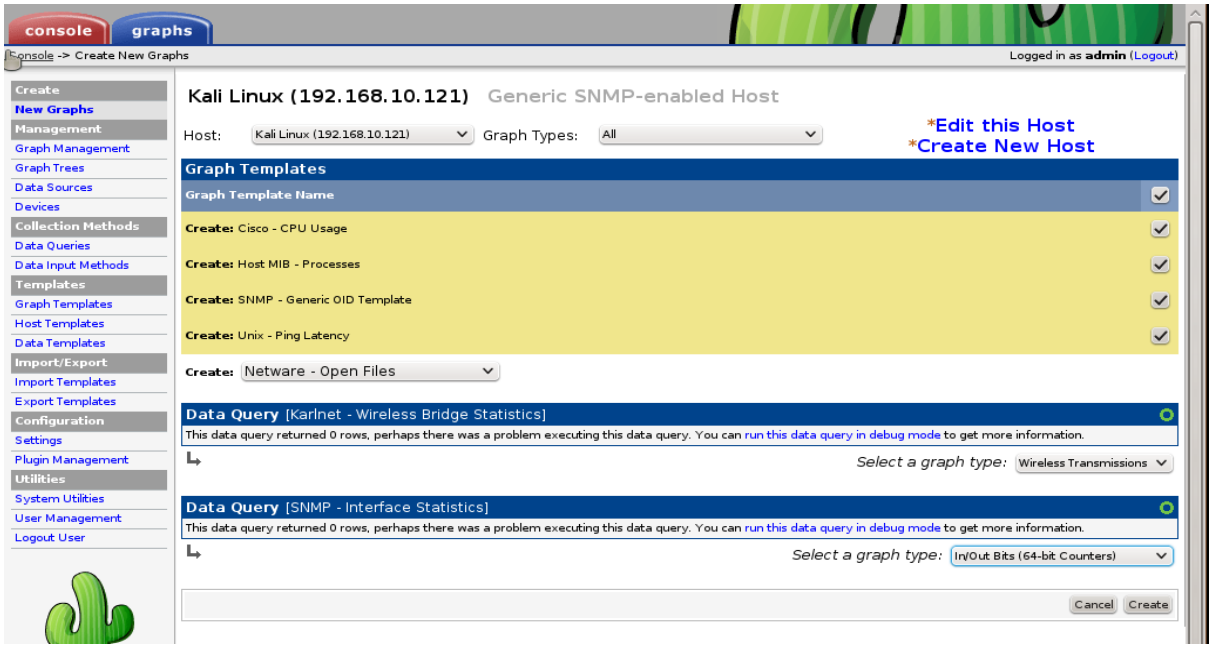


Fonte: do Autor.

Em SNMP *Community* insere-se o nome da comunidade criada no arquivo de configuração da máquina do cliente que faz o trabalho de um agente. Para essas informações serem transmitidas, é utilizada a porta “161’, sendo que as outras opções já são padronizadas e são preenchidas automaticamente.

Para associar algum gráfico em “*Associated Graph Templates*”, seleciona-se uma opção em “*Add Graph Template*” e clica-se em “*add*” no canto inferior direito da ferramenta (Figura 06).

Figura 06 - Associando o template dos gráficos



Fonte: do Autor.

Com todas as etapas concluídas, é preciso montar a árvore de gráficos para poder visualizar as informações. No menu seleciona-se “*Graphs Trees*” no canto superior direito, e clica-se em “*Add*” para adicionar um novo gráfico. Informa-se o nome do servidor a ser monitorado e salva-se a configuração. Feito isso, aparece uma nova opção abaixo da mesma tela que são os itens da árvore nomeados de “*Trees Items*”. Então, seleciona-se a opção “*Add*”. Em “*Tree Item Type*” opta-se por *Host*, no qual estão carregadas as informações sobre os hosts que estão configurados com a ferramenta. Seleciona-se o “*Host*” qual o *template* do gráfico e o tempo em que esse gráfico vai ser atualizado e salvar a configuração.

Para a visualização basta ir até a opção de *graphs* e selecionar o *host* que desejar para ver as informações disponibilizadas pela ferramenta.

3.1.1.3 RELATÓRIO COM CACTI

A forma como esta ferramenta retorna as informações é bem diferente e bastante interessante, isto é, para entender o que está acontecendo é essencial conseguir analisar muito bem os gráficos que a mesma gera. Esses gráficos são gerados através dos MIBs, que são as informações que são enviadas por cada processo e são atualizados periodicamente. É feito um cálculo estatístico para retornar a média que um determinado processo está consumindo da máquina configurada.

3.1.2 NAGIOS

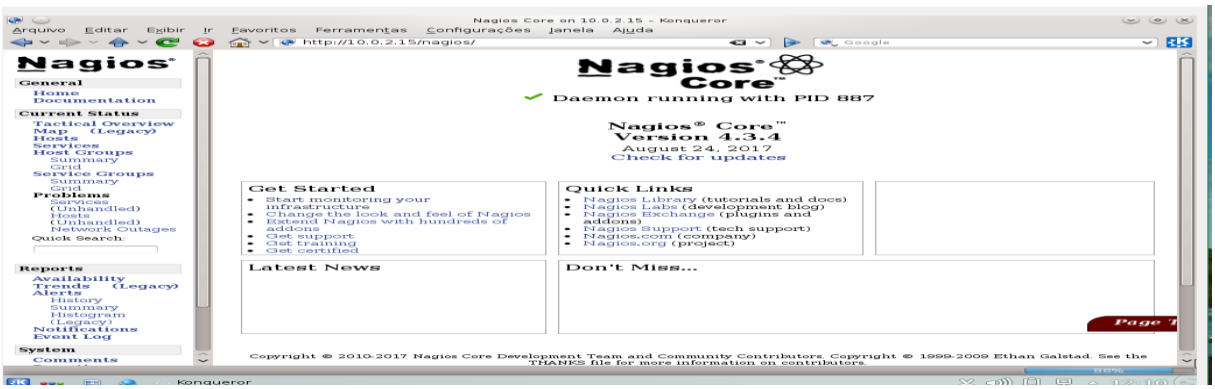
É uma aplicação popular, de código aberto, que monitora o tráfego da rede interna e de serviços instalados em servidores e que está licenciada pela General Public License (GPL), segundo consta na documentação disponibilizada. O software pode supervisionar tantos hosts quantos serviços, avisando quando acontecem problemas. As informações trocadas entre o host monitorado e o servidor são encriptadas utilizando os serviços Security Shell (SSL) e o Secure Socket Layer (SSH).

Tem a capacidade de notificar o administrador de redes quando um serviço apresentar problemas via e-mail ou qualquer outro meio, que é definido no momento

da configuração da ferramenta. Possui uma eficiência para tratar eventos, faz as tarefas funcionarem quando ocorrer situações inusitadas ou tentar corrigir o problema de forma automática. Também abrange de uma excelente interface web para visualizar o status atual da rede segundo Nagios BR.

Nagios é uma aplicação bem complexa, pois, para instalar é necessário baixar vários pacotes e também seus plug-ins. É um processo demorado e deve o usuário que for configurá-la tomar muito cuidado em cada comando que é digitado. A documentação aborda bem os passos de sua instalação. Seu design mostrado na Figura 07, apresenta a página inicial da mesma, fazendo o usuário recorrer a documentação para explorar de uma melhor forma a ferramenta.

Figura 07 - Interface inicial da ferramenta de segurança Nagios



Fonte: do Autor.

Na estrutura desse arquivo é necessário descrever qual host você quer fazer uma varredura, atribuindo um nome, e informando o endereço Internet Protocol version 4 (IPv4) do cliente. A cada serviço é definido qual host irá fazer o escaneamento, o nome do serviço e o tipo de checagem, onde, para cada serviço a ser examinado é obrigatório informar o tipo de auditoria que será abordada. Este registro trabalha com uma estrutura em forma de objetos, onde qualquer tarefa é abordada como se fosse um objeto com uma estrutura bem definida. E em relação a utilidade é possível analisar que a ferramenta consegue analisar de fato cada protocolo e trazer uma resposta de forma clara para o usuário.

3.1.2.1 INSTALAÇÃO DA FERRAMENTA NAGIOS

A instalação da ferramenta é feita a partir dos arquivos fontes que estão

disponibilizados no site da documentação da ferramenta, e seguir os passos do manual de instalação.

A ferramenta é cheia de arquivos de configurações, onde é necessário alterar antes de começar a fazer o monitoramento de qualquer host. Seu arquivo principal é o “nagios.conf”, que é responsável pela intervenção do Nagios. Esse arquivo é criado automaticamente ao instalar o Nagios.

Os arquivos de configuração de objetos, onde são conhecidos como configurações dos clientes estão empregados para determinar serviços. São nesses arquivos que são estabelecidos quais hosts irão ser supervisionados.

Objetos usados pelo Nagios:

- Serviços.
- Clientes (hosts).
- Grupo de Clientes.
- Contatos.
- Grupo de Contatos.
- Comandos.
- Períodos de tempo.
- Escalonamento de serviços.
- Dependências de serviço.
- Escalonamento de clientes.
- Dependência de clientes.
- Escalonamento de grupos de clientes.

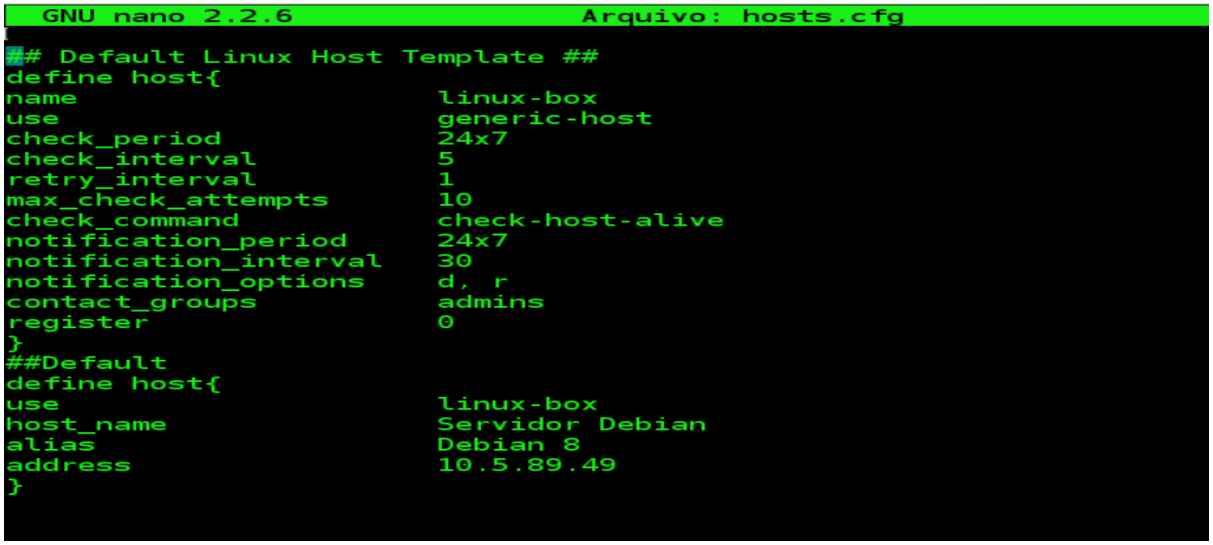
Cria-se um arquivo de configuração para o host que se deseja fazer o monitoramento. Na Figura 08 está o exemplo do arquivo com as configurações do host que foi monitorado.

O comando “define host” é para definir as propriedades do host que será monitorado e cada definição atribuída a seguir:

- host_name: utilizado para estabelecer o nome abreviado que será fundamental para identificar o cliente.
- alias: usado para fixar um nome completo do cliente.
- address: usado para definir o endereço IP do cliente.

- check_period: utilizado para definir qual o período de tempo em que a Nagios irá ter a responsabilidade de monitorar e alertar sobre qualquer problema na rede.
- max_checks_attempts: usado para estipula a quantidade de vezes que a Nagios irá tentar checar novamente os clientes que voltarem de qualquer estado além do OK.

Figura 08 - Arquivo para a configuração do host



Fonte: do Autor.

É necessário criar outro arquivo para configurar quais serviços vão ser monitorados conforme o exemplo exibido na Figura 09.

A sintaxe de cada serviço é definida no arquivo “services.cfg”, onde cada comando utilizado tem uma função a ser feita.

- use: faz utilizar o serviço genérico.
- host_name: utiliza o host configurado no arquivo anterior.
- service_description: a descrição do serviço.
- check_command: o comando que terá a função principal de fazer a checagem do serviço.

Figura 09 - Configuração dos serviços monitorados

Fonte: do Autor.

3.1.2.2 RELATORIO COM NAGIOS

Para ter uma forma de visualizar o que acontece entre os serviços, de uma forma mais clara é preciso ter uma certa didática e analisar o relatório do que acontece dentro do gerenciamento de redes de computadores.

Existem quatro tipos de saídas em cada serviço de rede, sendo eles:

- **OK**: Serviço funcionando em perfeito estado.
- **WARNING**: Requer uma atenção e olha analisada mais detalhada no serviço, pois, pode ser que algo na hora da configuração foi esquecido algo e o serviço não está 100 % funcional.
- **UNKNOWN**: Acontece quando a ferramenta não consegue captar os dados sobre o serviço resultando como serviço desconhecido.
- **CRITICAL**: Quando o serviço precisa de manutenção e um cuidado especial voltado a ele.

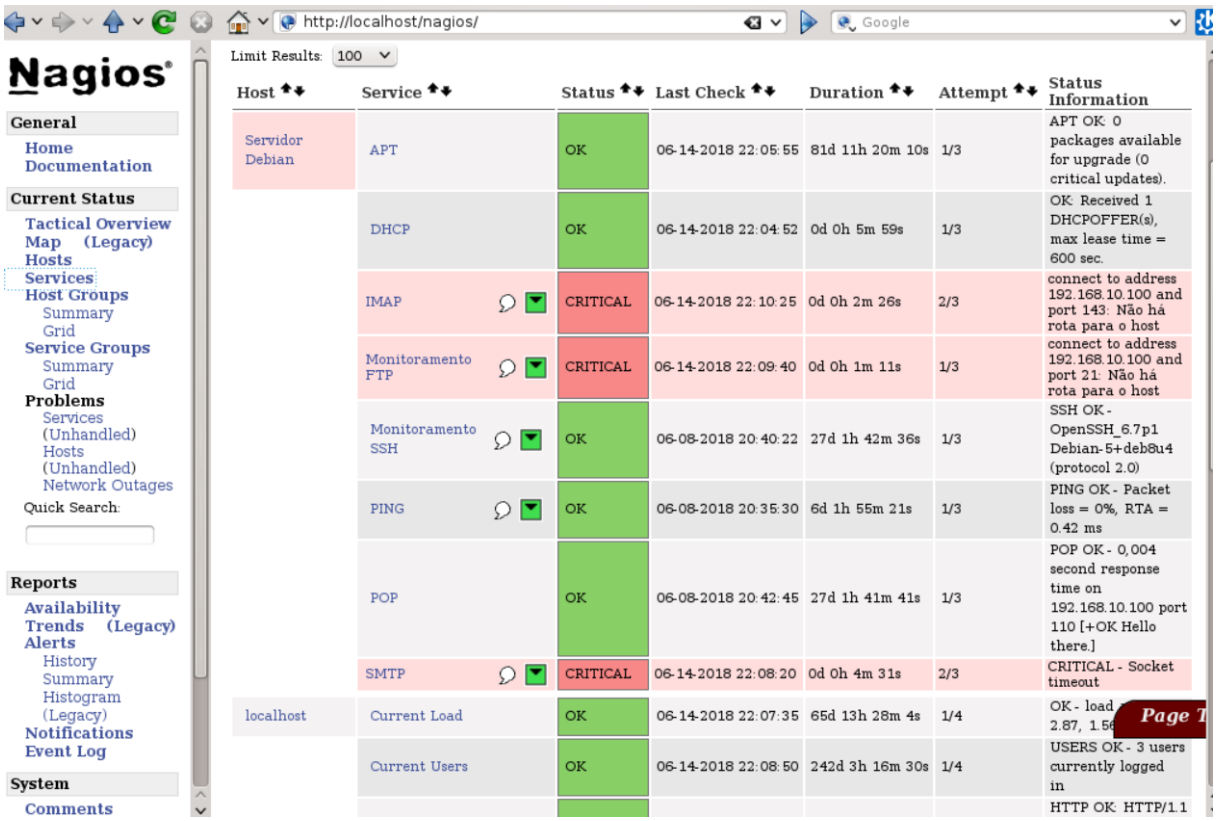
Essas saídas são o retorno dos estados dos serviços, podendo o administrador de redes saber o real estado dos serviços e tornando-se mais atento ao configurar serviços e também sendo mais ágil na hora em que houver algum problema em um determinado serviço, conforme a Figura 10. Retorna a informações dos estados dos serviços e informa o dia e a hora da última checagem que a ferramenta fez no servidor. Aparece o tempo de duração que o processo é executado e quantas tentativas foi necessária fazer.

Para ter um relatório como base é necessário fazer os passos a seguir:

- Seleciona-se no menu a opção REPORTS.
- Seleciona-se o tipo de relatório, pois a ferramenta possui quatro tipos: HOST GROUP, HOSTS, SERVICEGROUP, SERVICE.
- Seleciona-se as opções como: o período de tempo, data inicial e data final.

Após ter executado os passos citados acima vai aparecer na mesma guia o relatório geral com todas as saídas, exibindo a porcentagem do tempo em que um determinado serviço está sendo monitorado.

Figura 10 - Status dos serviços monitorados



Fonte: do Autor.

3.2 FERRAMENTAS DE DETECÇÃO DE VULNERABILIDADES

Nessa seção serão apresentadas as ferramentas OpenVAS e Nessus que fazem o monitoramento de serviços instalados em um determinado servidor.

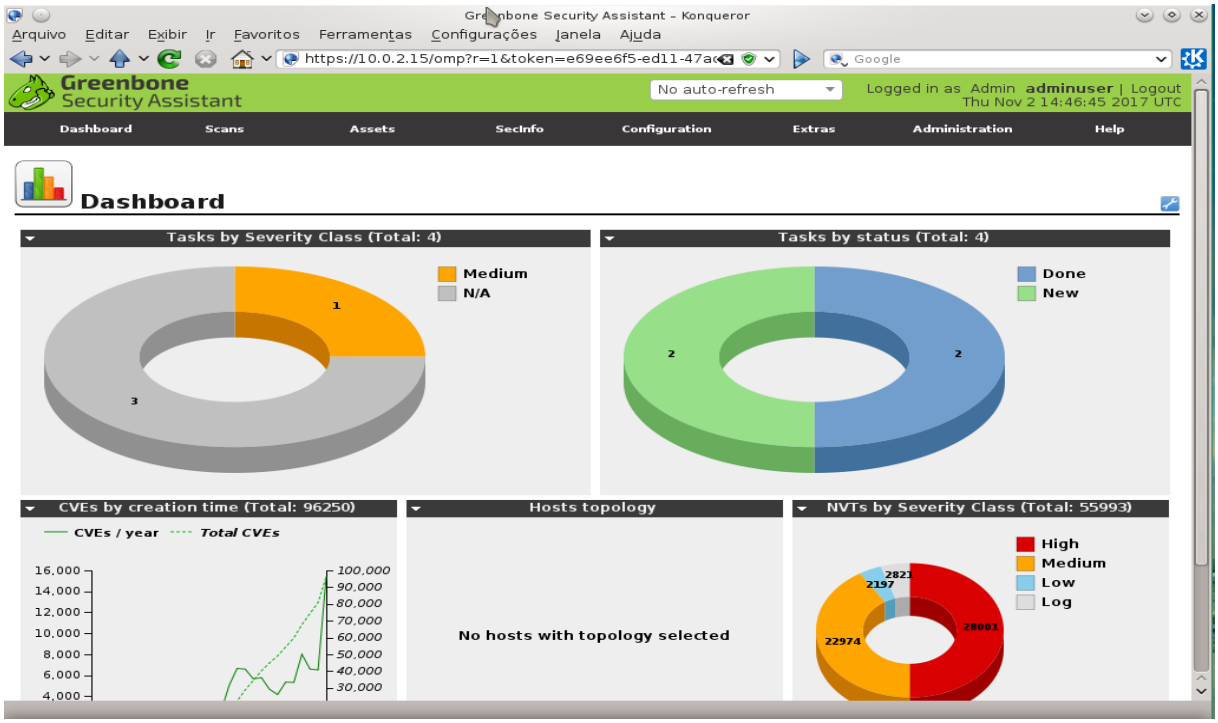
3.2.1 OpenVAS

É um framework para a detecção de vulnerabilidades, open source e gratuito que possui vários serviços e ferramentas segundo a sua documentação. Disponibiliza um scanner completo e possui uma coleção de scripts que estão capacitados a descobrir diversas vulnerabilidades.

OpenVAS oferece um ambiente completo de avaliação de segurança, com uma série de serviços e componentes que podem ser organizados em diversas formas para construir um ambiente de avaliação adequado a rede, segundo Schwarzer (2011)

Por intermédio de uma análise frequente da rede e a verificação da segurança, um administrador de redes de computadores é capaz o suficiente para qualificar o grau da segurança da rede e aderir regras de segurança em um tempo rápido. A interface inicial é exibida na Figura 11, mostra como a ferramenta apresenta os relatórios das máquinas que a mesma faz o escaneamento.

Figura 11 - Página inicial da interface web da ferramenta OpenVAS



Fonte: do Autor.

3.2.1.1 INSTALAÇÃO DA FERRAMENTA OpenVAS

Primeiramente iremos fazer a instalação no sistema operacional Kali Linux que é uma distribuição *open source* para fazer testes de *Pentest*.

O próximo passo que foi executado, inicia-se a instalação da ferramenta.

- apt-get install openvas

Com o comando executado, é indispensável a execução do seguinte comando.

- openvas-setup

Pois este comando faz o download das regras atuais, fazendo a criação de um usuário administrador e irá iniciar os serviços utilizados pela ferramenta. O processo é bastante demorado, dependendo da velocidade da banda da internet. Quando o processo termina é gerada uma senha para poder utilizar a ferramenta, no entanto é necessário fazer uma cópia da senha em algum lugar do seu computador para poder utilizar a ferramenta.

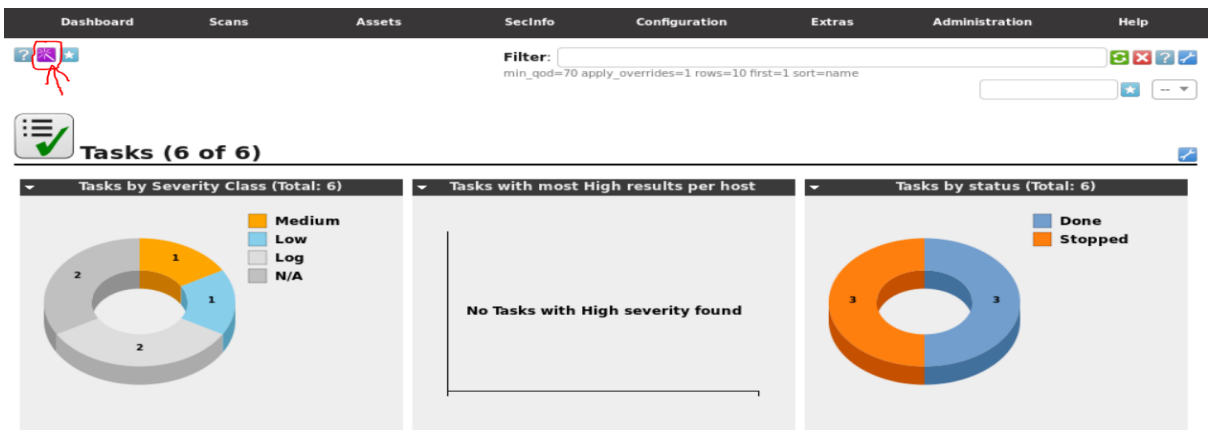
Inicializa-se o serviço com o seguinte comando.

- openvas-start

Para acessá-la, digita-se no navegador o seguinte endereço “https://localhost:9392”, é faz-se o “login” para utilizar a ferramenta.

Para configurar escaneamento em um host, possuímos duas formas de fazê-lo; - O primeiro a ser executado, vai ser o escaneamento imediato; - Seleciona-se a opção “Scans” e sua sub-opção “Task”, no canto superior esquerdo há um ícone circulado conforme na Figura 12, para fazer o escaneamento do servidor mais ágil.

Figura 12 - Configuração do host para o escaneamento imediato



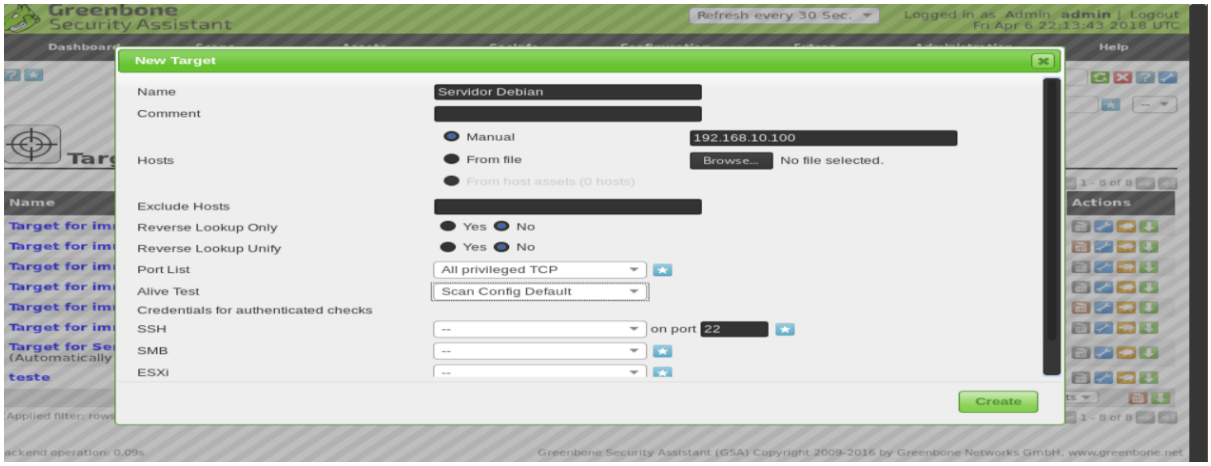
Fonte: do Autor.

Seleciona-se “Task Wizard”, que vai abrir o modal para informar as opções do servidor, isto é, só é necessário inserir o endereço IP do servidor e seleciona-se o botão “Start Scan”, para iniciar o processo de varredura. O escaneamento é bem demorado, pois ele faz uma varredura no servidor e busca as vulnerabilidades em cada serviço instalado na máquina.

A segunda forma para fazer o processo de escanear é diferente, porém, é mais trabalhosa de configurar. Primeiramente seleciona-se no menu “*Configuration*” e faz-se a escolha da opção “*Targets*”, que são os computadores alvos; - No canto superior esquerdo, há um ícone com uma estrela, clica-se nele; - No campo “*Name*” informa-se o nome para o alvo; - Em “*Comment*” não é obrigatório inserir alguma informação;- Em “*Hosts*”, seleciona-se a opção Manual e informa-se o endereço IP do servidor.;- Em “Port *List*” e escolhe-se o tipo de privilégio que o scanner vai ter sobre a máquina;- O que está selecionado passa todos os privilégios para a camada TCP/IP;- No “*Alive Teste*” seleciona-se o tipo de escaneamento, pois existem vários tipos de escaneamentos. Após isso clica-se em “*Create*” e o *Target* é criado.

Seleciona-se no menu a opção “*Scans*” e sua sub-opção “*Tasks*”, no canto superior esquerdo há também um ícone com uma estrela, clica-se e seleciona-se a alternativa “*New Task*”, que exibe o modal para criar uma nova tarefa de acordo com a Figura 14; - Nos campos “*Name*” e “*Comment*” faz-se o mesmo processo que foi feito na configuração do alvo; - Em *Scans Targets*, o escaneamento do alvo é preciso que seleciona-se o target criado na etapa anterior, com o nome do servidor; - Após em *Scanner* e seleciona-se um dos dois scanners instalados junto a ferramenta; - Seleciona-se OpenVAS *Default*.

Figura 13 - Modal para a criação de um Target

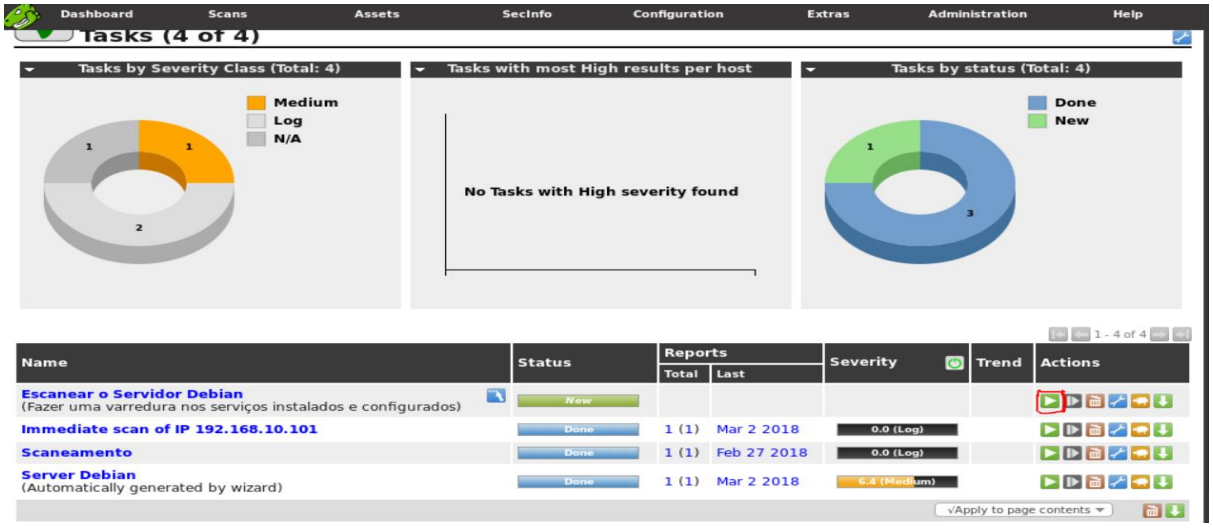


Fonte: do Autor.

Possuímos uma configuração importante abaixo de Scanner, nomeado de “Scan Config”, seleciona-se a configuração mais apropriada, pois tem sete tipos de varreduras, sendo eles: “Discovery”, “Full and fast”, “Full and fast ultimate”, “Full and very deep”, “Full and very deep ultimate”, “Host Discovery” e “System Discovery”. Faz-se uma varredura mais aprofundada selecionando a opção “Full and very deep” e clica-se em “Create” para criar a tarefa.

Na Figura 14, é exibido os gráficos a quantidade de varreduras que foram criadas e não executadas. Para executar a varredura que foi criada, clica-se no ícone “play” no canto inferior esquerdo, que está demarcado com a cor vermelha. Quando foi clicado no ícone a ferramenta fez uma requisição para o servidor, fazendo a varredura das vulnerabilidades dos serviços.

Figura 14 - Gráfico dos escaneamentos



Fonte: do Autor.

3.2.2.2 RELATÓRIO COM OPENVAS

O relatório desta ferramenta traz informações bem detalhadas sobre cada serviço. Para gerá-lo, após ter sido configurado e executado uma varredura. Existem cinco tipos de saídas ou gravidades, sendo elas:

- **HIGH**: serviço totalmente desprotegido.
- **MEDIUM**: existe alguma configuração errada ou está tendo muitas requisições para um servidor estabelecido.

- **LOW**: Serviço está bem configurado, mas pode ter algo que o comprometa.
- **LOG**: informa se há muitos logs de erros sobre o serviço.
- **FALSE POSITIVO**: quando o serviço possui alguma vulnerabilidade escondida.

É retornado o nome do serviço seguido de sua gravidade, o endereço IP, em qual porta está sendo executado, o tipo de protocolo é usado e quando foi gerado um arquivo de log. Após ter feito o escaneamento deve-se seguir os seguintes passos:

- Clica-se em **REPORTS**.
- Selecionar qual **HOST**.
- Seleciona-se o formato que deseja o relatório, tendo vários formatos: **XML**, **TXT**, **HTML**, **PDF**, **NBE**, **Topology SVG**.
- Clica-se no ícone de download.

Com o relatório em mãos o administrador irá analisar cada serviço detalhadamente, pois, a informação contida neste documento faz com que o administrador de redes possa detectar alguma anormalidade dentro do gerenciamento de sua rede, conforme a Figura 15, que exibe um relatório do servidor 192.168.10.100 que foi executado uma varredura com ferramenta.

Figura 15 - Relatório com a ferramenta OpenVAS

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.10.100	0	18	1	0	0
Total: 1	0	18	1	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 19 results selected by the filtering described above. Before filtering there were 150 results.

2 Results per Host

2.1 192.168.10.100

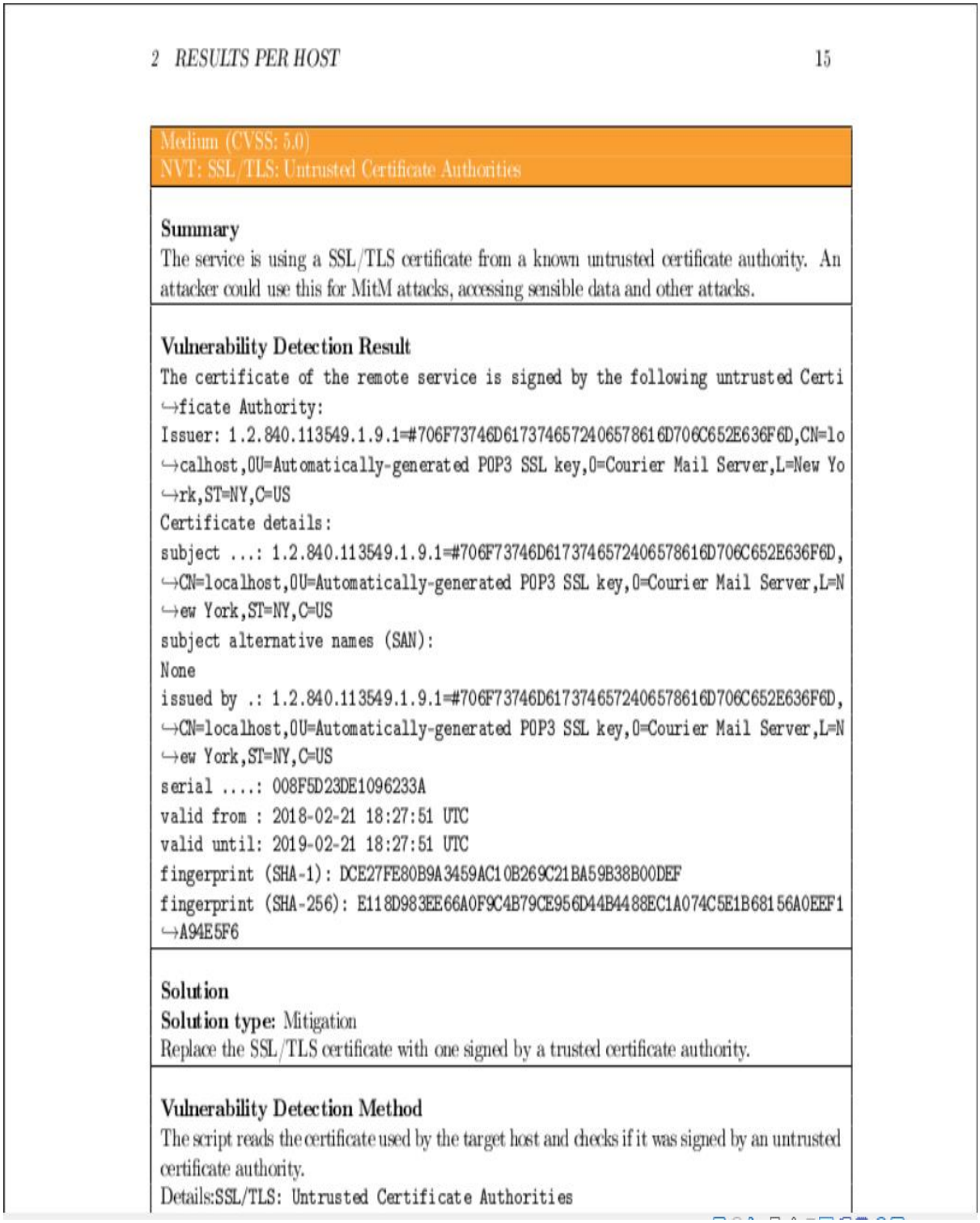
Host scan start Sat May 19 00:07:48 2018 UTC
Host scan end Sat May 19 01:02:20 2018 UTC

Service (Port)	Threat Level
993/tcp	Medium
465/tcp	Medium
21/tcp	Medium
995/tcp	Medium
25/tcp	Medium
110/tcp	Medium
143/tcp	Medium
general/tcp	Low

Fonte: do Autor.

Os dados que possuem as vulnerabilidades mais detalhadas são exibidos na Figura 16, pois para cada vulnerabilidade é informado uma solução para o problema.

Figura 16 - Detalhamento da vulnerabilidade



2 RESULTS PER HOST 15

Medium (CVSS: 5.0)
NVT: SSL/TLS: Untrusted Certificate Authorities

Summary
The service is using a SSL/TLS certificate from a known untrusted certificate authority. An attacker could use this for MitM attacks, accessing sensible data and other attacks.

Vulnerability Detection Result
The certificate of the remote service is signed by the following untrusted Certi
↪ficate Authority:
Issuer: 1.2.840.113549.1.9.1=#706F73746D617374657240657861 6D706C652E636F6D,CN=lo
↪calhost,OU=Automatically-generated POP3 SSL key,O=Courier Mail Server,L=New Yo
↪rk,ST=NY,C=US
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#706F73746D617374657240657861 6D706C652E636F6D,
↪CN=localhost,OU=Automatically-generated POP3 SSL key,O=Courier Mail Server,L=N
↪ew York,ST=NY,C=US
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#706F73746D617374657240657861 6D706C652E636F6D,
↪CN=localhost,OU=Automatically-generated POP3 SSL key,O=Courier Mail Server,L=N
↪ew York,ST=NY,C=US
serial ....: 008F5D23DE1096233A
valid from : 2018-02-21 18:27:51 UTC
valid until: 2019-02-21 18:27:51 UTC
fingerprint (SHA-1): DCE27FE80B9A3459AC10B269C21BA59B38B00DEF
fingerprint (SHA-256): E118D983EE66A0F9C4B79CE956D44B4488EC1A074C5E1B68156A0EEF1
↪A94E5F6

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted certificate authority.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by an untrusted certificate authority.
Details:SSL/TLS: Untrusted Certificate Authorities

Fonte: do Autor.

Com o relatório em mãos foi possível analisar e descobrir que alguns dos serviços que estavam no servidor possuíam algumas vulnerabilidades.

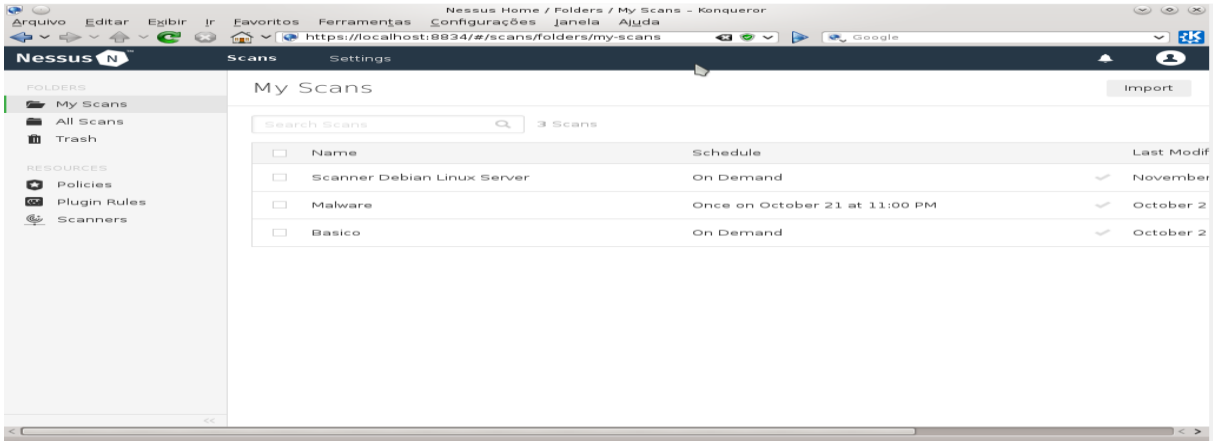
3.2.2.3 NESSUS

Segundo (TENABLE) é uma ferramenta de auditoria que é utilizada para verificar e reparar vulnerabilidades nos computadores da rede local desenvolvido pela Tenable Network Security. Ela faz a varredura das portas ativas, buscando acontecimentos anormais na máquina. É uma tecnologia que pode ser utilizada por qualquer administrador de redes, mas, não possui seu código aberto. A partir da versão 2.2 a empresa mantenedora do Nessus resolveu deixar o código fechado porque várias empresas estavam copiando sua lógica estrutural e criando aplicações que competiam com eles.

Nos dias de hoje o Nessus utiliza mais de 10.000 plug-ins para proteger contra falhas. A função do Nessus é auxiliar a detectar falhas antes que alguma pessoa utilize essas falhas e encontre uma maneira de prejudicar o sistema. É baseado em plug-ins que são softwares que possuem funcionalidades específicas capaz de analisar a existência de alguma vulnerabilidade.

A Nessus possui um processo simples de instalação e de fácil manuseio. Sua interface conforme a Figura 17, necessita de plug-ins que são instalados após a instalação da ferramenta. Para fazer uma análise na rede de um cliente apenas é necessário criar um host com o endereço do computador que será escaneado, e definir o tipo de análise que irá fazer.

Figura 17 - Interface web da ferramenta Nessus



Fonte: do Autor.

3.2.2.4 INSTALAÇÃO DA FERRAMENTA NESSUS

Para fazer a instalação dessa ferramenta faz-se necessário seguir os seguintes passos. Primeiro vá até o site “https://www.tenable.com/downloads/nessus” e procure a versão para sistema operacional correspondente, no caso, será detalhado este processo com o sistema operacional Windows. Para iniciar, entra-se no seguinte site e fazer o download:

- https://www.tenable.com/downloads/nessus

Seleciona-se a plataforma que a ferramenta vai ser instalada; - Após efetua-se o download, execute o arquivo “.exe” e apenas clica-se em todos os “next” até que a ferramenta finalize a instalação.

Após esse processo ser feito é necessária a chave de ativação, que o Nessus Core na versão gratuita vai ser ativado e poderá ser utilizado. No site “https://www.tenable.com/products/nessus/activation-code” seleciona-se a ferramenta “free” e clica em “Register Now”, vai ser necessário passar por um registro para obter a chave de ativação. O código da chave vai ser enviado ao e-mail cadastrado no registro. Para iniciar a instalação basta acessar ao endereço “http://localhost:8834” e inicia-se o processo de configuração manual da ferramenta.

Aparece a tela inicial da ferramenta, clica-se em “Get Started” e inicia-se a configuração. Na próxima tela faz-se o cadastro onde o usuário insere o nome e a senha para utilizar a interface gráfica da ferramenta. Clica-se em “next”, é exibida a tela para inserir o código da licença que foi enviado ao e-mail cadastrado.

Após essas etapas acimas serem concluídas, faz-se o download dos plug-ins que a mesma utiliza para fazer as varreduras e esse processo é bem demorado, pois caso haja alguma interferência na metade desse processo é preciso fazer todos os passos iniciais novamente.

3.2.2.5 RELATÓRIO COM NESSUS

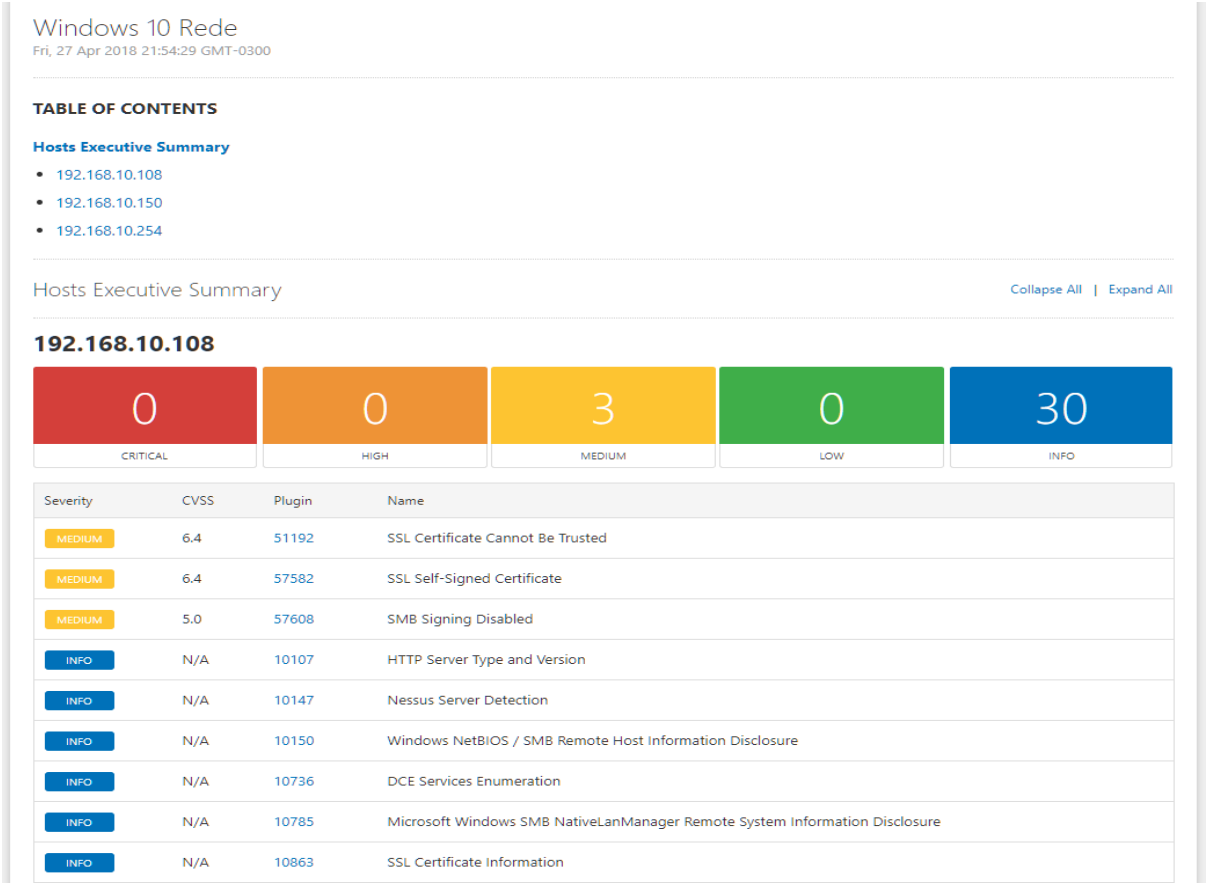
O relatório gerado com essa ferramenta é bem fácil de entender e as informações que a mesma traz são bem relevantes para o administrador de redes. O retorno dos serviços são os seguintes:

- **CRITICAL**: estado crítico, precisa ser reparado o mais urgente;

- **HIGH**: estado grave, alguma vulnerabilidade foi detectada;
- **MEDIUM**: estado de nível não tão grave;
- **LOW**: estado de nível baixo;
- **INFO**: informações detalhadas sobre o serviço;

Em cada retorno das saídas acima é exibido a descrição do serviço e caso encontre alguma vulnerabilidade, a ferramenta retorna uma solução de como o problema pode ser corrigido. É exibida a porta, o protocolo que serviço utiliza e o endereço IP do HOST que foi escaneado. Após fazer o escaneamento faz-se necessário clicar no escaneamento que foi efetuado e vai aparecer todas as vulnerabilidades encontradas. No canto superior direito, tem o botão com o nome de EXPORT, que é escolhido qual tipo de relatório desejasse. Existem quatro tipos de formatos que o relatório pode ser exportado, sendo eles: “Nessus”, “HTML”, “CSV”, “NessusDB”. Na Figura 18 é exibido o relatório que a foi gerado no formato “HTML”.

Figura 18 - Relatório da ferramenta Nessus



Fonte: do Autor.

4 VERIFICAÇÃO DA USABILIDADE

Esta seção descreve a metodologia utilizada para realizar as avaliações propostas nesse trabalho que versa sobre a verificação da usabilidade e da eficácia das ferramentas de detecção de vulnerabilidades, bem como os benefícios que cada ferramenta possui.

4.1 ARQUITETURA DOS TESTES

Para realizar os testes com as ferramentas foi criado um ambiente no qual foram virtualizadas duas máquinas Debian/Linux, sendo uma delas o servidor que vai possuir alguns serviços instalados e a outra a máquina cliente na qual estão instaladas as ferramentas que serão avaliadas. Também será virtualizada uma máquina com o sistema operacional Windows. A escolha desses sistemas operacionais deve-se ao fato destes, permitirem estabelecer um estudo comparativo entre os sistemas mais utilizados nas redes de computadores e avaliar as vulnerabilidades que cada sistema possui. A escolha do sistema operacional Debian/Linux baseou-se no fato que esse sistema possui código aberto e recursos que permitirão realizar os testes propostos neste trabalho.

No servidor Debian forma instalados os seguintes serviços:

- **DHCP:** Segundo Morimoto (2009), atualmente quase todas as redes utilizam algum tipo de serviço DHCP (*Dynamic Host Configuration Protocol*), que é um Protocolo de Configuração Dinâmica de Endereços de Rede. É um serviço configurado manualmente para a obtenção de um endereço IP (*Internet Protocol*). O trabalho desse servidor é bem simples, de certa maneira. Ele responde aos pacotes broadcast das máquinas, destinando um pacote com um dos endereços disponíveis e os demais dados da rede. Pacotes de broadcast são enviados aos IP's que estão com o endereço IP em uma faixa e são reenviados pelo switch da rede para todas as portas.
- **DNS:** Servidores DNS (Domain Name Server ou Sistema de nomes de domínios) são responsáveis em encontrar e traduzir para endereços IP's os endereços dos sites. No pico da rede temos os roots servers, que são 13

servidores espalhados pelo mundo que tem como finalidade enviar todas as requisições de respostas de domínios.

- **SSH (*Secure Shell*):** Um dos benefícios do Linux, indicada por muitos administradores de rede é a clareza em gerenciar o sistema remotamente. Poucas empresas hospedam websites dentro da própria empresa. Na maioria das vezes os servidores ficam em data centers, que oferecem uma estrutura necessária para que os mesmos fiquem no ar de forma transparente.
- **FTP (*File Transfer Protocol*)**: Segundo Morimoto (2009), o funcionamento do serviço FTP é bem mais simplificado que o SSH, visto que ele é utilizado de forma a liberar arquivos na Internet ou na própria rede local sem nenhuma segurança.
- **SMTP (*Simple Mail Transfer Protocol*):** estabelecido no RFC 2821, está no centro do correio eletrônico da Internet. O serviço de e-mail é um instrumento de comunicação assíncrono, dado que, usuários enviam mensagens quando for necessário para os mesmos, sem precisar saber se quem vai receber a mensagem esteja conectado no servidor de e-mail.
- **POP3:** Segundo Morimoto (2009), é um protocolo de acesso ao correio de extrema facilidade, por ser muito simples a sua finalidade é muito reduzida. O serviço inicia quando um agente de usuário realiza uma conexão TCP com o servidor de correio, normalmente utilizado na porta 110. Com a conexão funcionando em perfeito estado, esse serviço se submete por três fases: autorização, transação e atualização.
- **IMAP:** Segundo Morimoto (2009), distribui vários recursos parecidos com o POP3. É um protocolo que o cliente de e-mail pode utilizar para fazer downloads dos e-mails em um servidor de e-mail. Mas traz mais recursos que o POP3, visto que, foi desenvolvido para conceder que seus utilizadores preservarem seus e-mails no servidor.
- **APACHE:** Segundo Morimoto (2009), os servidores web são a espinha dorsal da Internet, são eles que hospedam todas as páginas incluindo os mecanismos de busca e servem como base para todo o tipo de aplicativa via web. O serviço APACHE oferta um sustento apenas a recursos básicos, mas pode ser expandido pelo meio de módulos, suportando scripts em PHP (Hypertext Preprocessor), acessando banco de dados, e mais outros recursos.

- **SNMP (Simple Network Management Protocol):** É o protocolo mais utilizado para o gerenciamento de redes e autoriza que uma ou mais estações sejam apontadas como gerentes de rede. A estação gerente de rede recebe as informações de todos os hosts, que são denominados como agentes através do tratamento das informações e pode gerenciar toda a rede e detectar os problemas ocorridos. Os dados recolhidos pela máquina que faz o controle da rede ficam memorizadas nas próprias máquinas da rede (MIB). Encontram-se gravadas esses dados em uma base que são fundamentais para o gerenciamento do dispositivo pelo meio de variáveis que são requisitadas pelo host gerente.

No servidor Kali/Linux foi instalado o pacote T50, para poder simular um ataque DOS (*Denial-of-Service*), que faz testes de stress em redes ou servidores. Utiliza o método de injeção de pacotes misturando até 15 tipos de protocolos diferentes. Tem seu código aberto e está disponível em vários formatos pré-compilados para algumas distribuições GNU/Linux. É possível enviar um valor muito alto de requisições de pacotes, fazendo com que o sistema não suporte, deixando alguns serviços indisponíveis. Um dos comandos que a ferramenta utiliza é o “hping3” que faz vários tipos de requisições através do “ping”, fazendo com que os serviços em um determinado servidor fiquem indisponíveis.

Esta ferramenta foi utilizada para fazer os ataques de DOS em um host, tentando deixar a máquina indisponível para as ferramentas de detecção de vulnerabilidades

O DOS é uma técnica utilizada por hackers para fazer com que uma máquina ou algum recurso de rede fique indisponível para os usuários, derrubando os serviços do maquina conectada na internet.

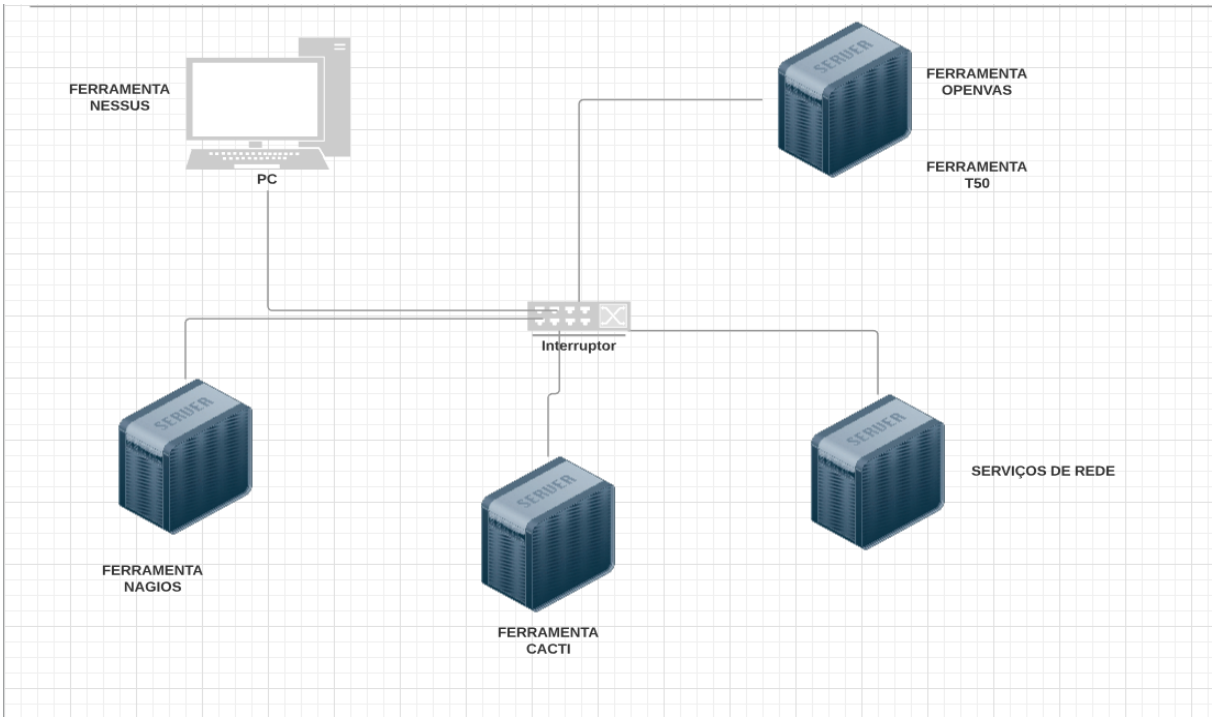
Segundo CORREA, MARTINS:

> “O Denial-of-Service (DOS) ou ataque de negação de serviços tem como objetivo impedir um serviço de funcionar corretamente e assim impedir que os usuários utilizem esses serviços. O ataque de negação de serviços é muito utilizado para atacar servidores de hospedagem de sites na Internet. O DOS normalmente é feito através de múltiplas requisições feitas a um servidor. O atacante, que no caso seria o hacker que está tentando parar o serviço, utiliza de softwares e técnicas para

> fazer múltiplas requisições automaticamente para o alvo, que é o serviço que o hacker deseja afetar.”

As ferramentas de detecção de vulnerabilidades de segurança de redes de computadores fazem uma análise do tráfego da rede e também faz uma varredura na máquina, verificando os softwares que estão vulneráveis e que abrem portas para possíveis ataques. As ferramentas de monitoramento e detecção de vulnerabilidades foram instaladas em um servidor específico nas quais serão realizados os testes, conforme descreve a Figura 19.

Figura 19 - Arquitetura das máquinas virtualizadas



Fonte: do Autor.

Após a criação das máquinas foram instaladas as ferramentas de monitoramento, sendo elas: CACTI e NAGIOS, e as ferramentas de varredura, sendo elas: NESSUS e OPENVAS. Em seguida serão avaliados alguns critérios de análise:

- Instalação/Configuração: modo de instalar e configurar.
- Documentação: se a mesma auxilia o administrador de redes a entender o funcionamento da ferramenta.
- Recursos: se possui vários recursos para ser utilizado.

- Respostas geradas: que tipos de respostas a ferramenta de detecção apresenta para o administrador de redes.
- Detecção: se a mesma apresenta de fato alguma mensagem em tempo real, no momento em que detecta algum acontecimento anormal na máquina.

E serão também avaliados os critérios de usabilidades sendo eles: a facilidade do aprendizado, facilidade em memorizar, maximização da produtividade, minimização da taxa de erros e maximizar da satisfação do usuário.

Foi criada uma máquina virtual para cada ferramenta, para que não ocorresse alguma interrupção entre uma ferramenta e outra. Todas as ferramentas são acessadas pelo navegador para poderem ser utilizadas.

O teste de usabilidade com dois usuários foi dividido em duas etapas, na primeira etapa com as ferramentas de monitoramento e na segunda etapa com as ferramentas de varredura. Sem o conhecimento do usuário foi disparado um comando hping3 que é disponibilizado pela ferramenta T50. Na medida em que o ataque ocorria, o usuário poderia observar o estado dos serviços.

É importante ressaltar que nenhum dos usuários possuía experiência prévia com nenhuma das ferramentas.

Foi feito a apresentação das ferramentas de monitoramento, explicando a sua funcionalidade e o que ela detectava. A seguir o usuário iniciou a utilização das ferramentas verificando os status dos serviços, sem que os mesmos soubessem que a ferramenta T50 estava simulando o ataque de negação de serviço. Ao detectar alguma anormalidade no servidor, foi sugerido que o usuário utilizasse as ferramentas de detecção de vulnerabilidades. Apresentou-se as ferramentas de vulnerabilidades e foi explicado o funcionamento das mesmas. Pediu-se ao usuário que fizesse uma varredura no servidor que aparentava estar com anormalidades. Após feita a varredura, foi sugerido que o usuário verificasse o relatório que a ferramenta gerou. Após foi entregue o questionário avaliativo para a verificação da usabilidade das ferramentas.

4.2 VALIDAÇÃO DA USABILIDADE COM OS USUÁRIOS

A identificação dos usuários ficou estabelecida da seguinte forma, um usuário definido como A1 que é um aluno do curso superior na área de informática, e tem um alto conhecimento em redes de computadores, e o outro usuário definido como

A2 já formado na área, cursando mestrado na área de informática, que trabalha com o desenvolvimento de software e possui conhecimento limitado na área de redes. Para a avaliação de usabilidade foi definido um questionário conforme o ANEXO 1. No teste com as com as ferramentas de monitoramento foi solicitado aos usuários para que buscassem informações sobre o estado dos serviços instalados no servidor

Com relação as ferramentas de monitoramento os usuários se posicionaram da seguinte forma. Na ferramenta CACTI, o usuário A1 concordou que as informações disponibilizadas são coerentes e estão de acordo o estado real dos serviços, e as informações também o auxiliaram no diagnóstico. As informações foram suficientes para o mesmo, que concorda que a forma com que os dados são transmitidos são eficientes e a organizações da tela é clara. Em relação a interface o mesmo opinou de forma neutra, discordou de que são necessários conhecimentos adicionais para utilizar a ferramenta e avaliou de forma positiva que foi fácil encontrar a informação que precisava. Para o usuário A2 as informações disponibilizadas não foram coerentes e não o auxiliaram no diagnóstico, por que o mesmo não possuía conhecimentos suficientes sobre a ferramenta e também não foram suficientes para detectar o que estava acontecendo nos serviços. Avaliou de forma neutra que a forma que os dados são transmitidos são eficientes, discordou totalmente que as organizações das informações na tela sejam claras e que a interface do sistema é agradável. Considerou de modo neutro que foram necessários conhecimentos adicionais para conseguir utilizar a ferramenta, afirmou que achou o sistema muito complicado e discordou que foi fácil encontrar o que precisava.

Na ferramenta NAGIOS, o usuário A1 avaliou que as informações disponibilizadas são coerentes, o ajudaram no diagnóstico e foram suficientes. Concordou com a forma em que os dados são transmitidos são eficientes, também que a organização das informações é clara e a interface do sistema é agradável e que foi fácil encontrar a informação que precisava. Entretanto, discordou de que foram necessários conhecimentos adicionais para utilizar a ferramenta e não achou a mesma muito complicada. O usuário A2 avaliou que não possuía conhecimentos suficientes para verificar se as informações disponibilizadas eram coerentes, não o auxiliando no diagnóstico e que não foram suficientes. Considerou de forma neutra a forma que os dados são transmitidos e de que foi necessário conhecimento adicional para o mesmo utilizar a ferramenta. Discordou que as informações na tela sejam

claras, que a interface é agradável e que foi fácil de encontrar o que precisava. Achou o sistema muito complicado.

Com relação as ferramentas de detecção de falhas, os usuários se posicionaram da seguinte forma. Na ferramenta NESSUS, o usuário A1, avaliou de forma positiva que as informações são coerentes, também o auxiliaram no diagnóstico e que as informações foram suficientes para o mesmo, mas, afirmou que a ferramenta não disponibiliza escaneamentos suficientes para problemas que venham a ocorrer no servidor. Considerou de forma neutra, que a forma que os dados são transmitidos são eficientes e para encontrar a informação que precisava. Concordou que a organização das informações da tela é clara e que foram necessários conhecimentos adicionais para utilizar a ferramenta. Discordou que a interface seja agradável e concordou totalmente que o sistema é muito complicado. Para o usuário A2, as informações disponibilizadas foram coerentes, e o auxiliaram no diagnóstico, mas, poderia ter mais opções e as informações não foram suficientes. Também afirmou que a ferramenta não possui escaneamentos suficientes. Concordou que a forma em que os dados são transmitidos são eficientes. A organização das informações na tela do sistema é clara e a interface é agradável. Não foram necessários conhecimentos adicionais para utilizar a ferramenta e no mesmo não achou o sistema complicado. E avaliou de forma neutra se foi fácil encontrar a informação que precisava.

Na ferramenta OPENVAS, o usuário A1, as informações disponibilizadas foram coerentes, o ajudaram no diagnóstico de forma suficientes. A ferramenta disponibiliza escaneamentos suficientes, segundo A1 “Excelente ferramenta, muito completa, demora um pouco, mas é compreensível devido ao grande número de informações que traz”. A forma com que os dados são transmitidos foram eficientes, a organização das informações na tela do sistema foi clara a interface agradável e foi fácil encontrar a informação que precisava. Não foram necessários conhecimentos adicionais o não achou o sistema muito complicado. Para o usuário A2, as informações disponibilizadas não foram coerentes, as informações o ajudaram no diagnostico, e foram suficientes, também afirmou que a ferramenta disponibiliza escaneamentos suficientes para problemas que possam vir a ocorrer no servidor.

Após o experimento também foi solicitado ao usuário que buscasse informações adicionais com relação aos estados dos serviços. O usuário A1 foi diretamente

buscar nos arquivos de log da ferramenta, entretanto, o usuário A2 achou bastante complicado buscar informações adicionais, pelo fato, de as ferramentas estarem no idioma inglês.

Após os testes foi possível analisar que os dois usuários tiveram algumas dificuldades ao tentar utilizar um software que não conheciam. A duas ferramentas de monitoramento cumpriram seus objetivos, que foi detectar o que estava acontecendo no servidor. Houve problemas em relação a rede, pois estava com dificuldades na conexão das máquinas virtuais durante um dos testes.

Para cada marcação no questionário de avaliação de usabilidade, foi definido uma pontuação, onde após foi feito o somatório, sendo possível verificar as ferramentas mais bem avaliadas pelos usuários.

Figura 20 – Questionário avaliativo

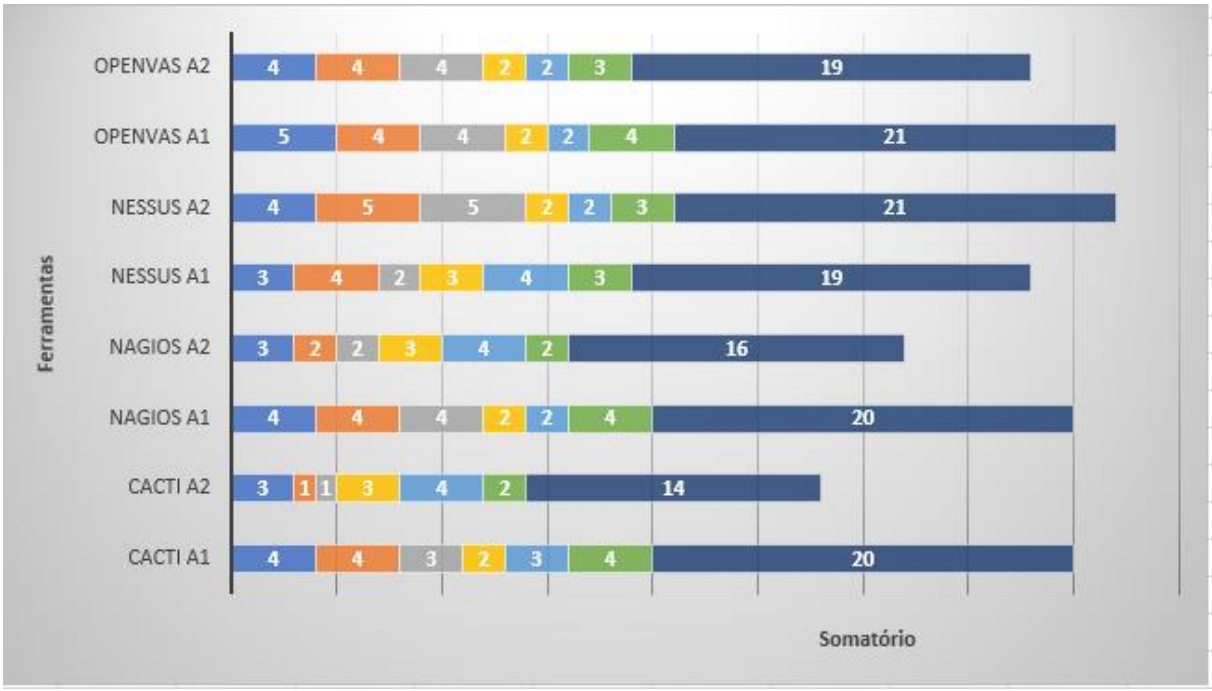
Questionário de avaliação de usabilidade

	Discordo Totalmente	Discordo	Neutro	Concordo	Concordo Totalmente
A forma em que os dados são transmitidos são eficientes?			X		
A organização das informações na tela do sistema é clara?				X	
A interface é agradável?					X
Foram necessários conhecimentos adicionais para utilizar a ferramenta?		X			
Achei o sistema muito complicado?				X	
Foi fácil encontrar a informação que precisava?			X		
Pontuação =>	1	2	3	4	5

Fonte: do Autor.

Conforme o gráfico apresentado na Figura 21, é possível analisar qual ferramenta teve a melhor usabilidade para cada usuário. Com isto, cada ferramenta terá uma nota final, onde será concluída qual a melhor a ser utilizada.

Figura 21 – Gráfico do somatório das notas atribuídas a cada ferramenta.



Fonte: do Autor.

Aparentemente as ferramentas Nagios e OpenVAS obtiveram um melhor resultado, pode-se analisar que de fato a OpenVAS empatou pelo somatório, mas nas questões respondidas obteve menos pontuação. Com isso pode-se definir que as melhores ferramentas a serem utilizadas são as que obtiveram um melhor resultado no somatório das notas são Nagios e OpenVAS.

5 CONCLUSÃO

O presente trabalho teve como objetivo avaliar a usabilidade das ferramentas de detecção de redes de computadores. Para tanto, foi necessário fazer a instalação e a configuração das ferramentas e também de alguns serviços de redes para serem monitorados e escaneados.

Com relação a instalação das ferramentas de monitoramento, estas possuem uma maior complexidade ao configurar os arquivos necessários para então conseguir utiliza-las. As ferramentas de varreduras são mais fáceis de serem instaladas e configuradas, pois a documentação das mesmas é acessível.

Em relação a utilização das ferramentas pode-se avaliar que todas auxiliam o administrador de redes, pois as de monitoramentos irão acusar que há alguma anormalidade na rede, e as de varreduras para fazer um escaneamento mais aprofundado, podendo saber como corrigir tal vulnerabilidade.

A partir dos testes realizados com os usuários pode-se ter uma ideia melhor sobre a usabilidade das ferramentas. Observou-se que para conseguir utilizar as ferramentas de detecção de vulnerabilidades, é necessário um conhecimento intermediário na área de redes de computadores, pois, como foi avaliado nos testes.

Algumas ferramentas como a Nagios obtiveram melhor resultado em determinado aspecto em exibir o estado dos serviços, auxiliando ao administrador poder fazer algo cara a correção de alguma anormalidade na rede. A ferramenta Cacti obteve um resultado melhor em exibir para o usuário através dos gráficos o funcionamento dos serviços. A OpenVas fez varreduras, estas que demonstraram que alguns serviços possuíam vulnerabilidades e com um relatório fácil de entender, trazendo uma solução de como resolver tais vulnerabilidades A ferramenta Nessus obteve um resultado razoável na questão do relatório que a mesma gerava.

Com o somatório das avaliações feitas pelos usuários é possível definir que a ferramenta de monitoramento com melhor usabilidade é a Nagios. A ferramenta de varredura com melhor usabilidade é a OpenVAS para usuários com alto conhecimento em redes e a Nessus para usuários com pouco conhecimento.

Como trabalho futuro pensa-se avaliar o as ferramentas e em um contexto de testes de penetração, onde se utilizaria métodos da segurança da informação para impedir que um determinado servidor seja invadido.

Por fim, buscou-se contribuir para que novas pesquisas da área de segurança de redes possam realizada a partir dos resultados obtidos.

REFERÊNCIAS

ALERTA SECURITY. ***A importância da Análise de vulnerabilidade*** - Disponível em:<https://www.alertasecurity.com.br/blog/82-a-importancia-da-analise-de-vulnerabilidade> Acesso em: 23 de outubro de 2017.

ALERTA SECURITY. **O que é risco, vulnerabilidade e ameaça.** Disponível em: <https://www.alertasecurity.com.br/blog/75-o-que-e-risco-vulnerabilidade-e-ameaca> Acesso em 25 de outubro de 2017.

BORGES, Alighieri Miguel, VALENTIM, Tainan dos Santos, LIMAS, Jeferson Mendonça, ANTUNES, Alexssandro Cardoso, 2015. **Estudo comparativo entre Nagios e Zabbix.**

BUZZATTE, Patrícia Monego, ***Análise de Vulnerabilidades através de scanners detectores****. Disponível em:* <http://www.redes.ufsm.br/docs/tccs/TCC_Final_Patricia.pdf> Acesso em: 16 de agosto de 2017.

CORRÊA, A.L.R, MARTINS, H.P, **Monitoramento De Ataques De Negação De Serviço: Um caso Prático Utilizando Slowloris.** Disponível em: <http://www.fatecbauru.edu.br/mtg/source/Monitoramento%20de%20ataques%20de%20nega%C3%A7%C3%A3o%20em%20servi%C3%A7o.pdf> Acesso em: 02/05/2018.

FERREIRA, F.N.F.; ARAÚJO, M. T. **Políticas de Segurança da Informação: Guia Prático para Embalagem e Implementação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

LAUREANO**,** Marcos Aurelio Pchek**. Gestão de Segurança da Informação. Disponível em.** Acesso em: 08 de novembro de 2017.

KUROSE, James F. **Redes de Computadores e a Internet: uma abordagem top-down**. 6. ed. - São Paulo: Pearson Education do Brasil, 2013.

MICROFOCUS. **Cyber Risk Report 2016**. Disponível em: <http://files.asset.microfocus.com/4aa6-4617/en/4aa6-4617.pdf> Acesso em: 01 de novembro de 2017.

MORIMOTO, Carlos Eduardo. **Servidores Linux: guia prático**. Porto Alegre: Sul Editores, 2008.

MONOLITONIMBUS. **Cacti**. Disponível em <https://www.monolitonimbus.com.br/cacti/> Acesso em: 03 de abril de 2018.

NAGIOS BR. **Nagios Core.** Disponível em <http://nagios-br.com/nagios-core> Acesso em: 27 de agosto de 2017.

NAGIOS BRAZILIAN COMMUNITY SITE. **Nagios core.** Disponível em: <http://nagios-br.com/nagios-core> Acesso em 25 de agosto de 2017.

NAKAMURA, E.T.; GEUS, P.L de. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec Editora, 2007.

NETO, A.F, UCHÔA, J.Q. **Ferramentas Livres para Monitoração de Servidores**. Disponível em: <http://repositorio.ufla.br/bitstream/1/9641/1/ARTIGO_Ferramentas_livres_para_monitora%C3%A7%C3%A3o_de_servidores.pdf> Acesso em: 18 de abril de 2018.

NIELSEN, Jakob; LORANGER, Hoa. Usabilidade na Web: Projetando Websites com qualidade. Rio de Janeiro: Elsevier, 2007.

OPENVAS. **The world's most advanced Open Source vulnerability scanner and manager.** *Disponível em:* <http://www.openvas.org/> Acesso em: 24 de agosto de 2017.

PESSOA, Marcio. **SNMP: Instalação e configuração no Linux.** Disponível em: <https://pessoa.eti.br/main/2011/10/18/snmp-instalacao-e-configuracao-no-linux/> Acesso em: 12 de abril de 2018.

TABLELESS. **O que é usabilidade?** Disponível em: <https://tableless.com.br/o-que-e-usabilidade/> Acesso em: 08 de dezembro de 2017.

TANENBAUM, A. S. ***Redes de Computadores***. 4. ed. Rio de Janeiro: Elsevier, 2003.

TENABLE. **Baixe Nessus.** Disponível em: <https://www.tenable.com/products/nessus/select-your-operating-system> Acesso em: 26 de outubro de 2017.

ANEXOS

ANEXO 1 – Questionário avaliativo das ferramentas

Questionário sobre as ferramentas de segurança de rede de computadores

1. As informações disponibilizadas são coerentes e estão de acordo com o real estado dos serviços?

2. As informações auxiliaram no diagnóstico? Por que?

3. As informações foram suficientes? Justifique?

4. A ferramenta disponibiliza escaneamentos suficientes para problemas que vieram ocorrer no servidor?

Questionário de avaliação de usabilidade

	Discordo Totalmente	Discordo	Neutro	Concordo	Concordo Totalmente
A forma em que os dados são transmitidos são eficientes?					
A organização das informações na tela do sistema é clara?					
A interface é agradável?					
Foram necessários conhecimentos adicionais para utilizar a ferramenta?					
Achei o sistema muito complicado?					
Foi fácil encontrar a informação que precisava?					

Fonte: do Autor.