CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Gustavo Defávori

Detectando Falhas e Vulnerabilidades em redes IPv4 usando Nessus e NMAP

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Gustavo Defávori

Detectando Falhas e Vulnerabilidades em redes IPv4 usando Nessus e NMAP

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação sob a orientação do (a) Prof.(a) Me. Clerivaldo Jose Roccia.

Área de concentração: Segurança da Informação.

Americana, SP

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Defávori, Gustavo
D498d Detectando falhas e vulnerabilidades em redes IPv4 usando Nessus e NMAP. / Gustavo Defávori. – Americana: 2015.
81f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Clerivaldo José Roccia

1. Segurança em sistemas de informação I. Roccia, Clerivaldo JoséII. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518

Gustavo Defávori

Detectando Falhas e Vulnerabilidades em redes IPv4 usando Nessus e NMAP

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana 25 de junho de 2015.

Banca Examinadora:

Clerivaldo Jose Roccia (Presidente)
Mestre
Fatec Americana

Maria Cristina Luz Fraga Moreira Aranha (Membro)
Mestre
Fatec Americana

Henri Alves de Godoy (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar a Deus, por estar concluindo mais uma etapa de estudos.

Ao professor Clerivaldo, por ter dado todo o auxilio e apoio para este trabalho se concretizar.

A minha família por total apoio, e paciência para a concretização desta fase.

Ao parceiro de serviço Danilo, pelas dicas, ideias e correções ao longo desta fase.

DEDICATÓRIA

Aos meus familiares, amigos, e a todos que atuam na área de Segurança da Informação.

RESUMO

O presente trabalho é uma monografia, que apresenta dois softwares que auxiliam no processo de Segurança da Informação, sendo eles, o NMAP e o Nessus. É apresentado o conceito da Segurança da Informação, seu surgimento, bem como alguns aspectos importantes como, por exemplo, a constituição dos seus pilares de sustentação e o protocolo usado no processo de comunicação. Este trabalho ainda aborda a diferença entre as versões desse protocolo que estão sendo usados atualmente. Ao longo do trabalho, será mostrado um estudo de campo através de vários cenários que foram previamente construídos. Os testes que foram usados no estudo de campo, utilizam como ferramentas, o Nessus e o NMAP. O objetivo principal desse estudo é mostrar que uma máquina, com a configuração padrão do sistema operacional ou com pequenas mudanças simples, que aparentemente apresentam mais segurança, ainda possuem vulnerabilidades e falhas que, se não forem resolvidas, podem virar alvos de atacantes.
.

Palavras Chave: Segurança da Informação; Nessus; Vulnerabilidades.

ABSTRACT

This work is a monograph, which features two softwares that help in the Information Security process, namely, the NMAP and Nessus. It presented the concept of information security, its appearance as well as some important aspects such as the constitution of the supporting pillars and the protocol used in the communication process. This paper also discusses the difference between the versions of this protocol being used today. Throughout the work, it will be shown a field study through various scenarios that were previously built. The tests that were used in the field study, using as tools, Nessus and NMAP. The main objective of this study is to show that a machine with the default configuration of the operating system or with small simple changes that appear to have more security, still have vulnerabilities and flaws which, if unresolved, can become targets of attackers.

Keywords: Information Security, Nessus, Vulnerabilities.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARP – Address Resolution Protocol

Cert.br – Centro de Estudos, e Resposta e Tratamento de Incidentes de Segurança no Brasil

CGI.br – Comitê Gestor da Internet da Internet no Brasil

CVE – *Common Vulnerabilitiesand Exposures*

DHCP – *Dynamic Host Configuration Protocol*

DoS – *Denial of Service*

DNS – *Domain Name System*

GB – Gigabyte

HTML – *Hyper Text Markup Language*

HTTPS – *Hyper Text Transfer Protocol Secure*

ICMP – *Internet Control Message Protocol*

IP – *Internet Protocol*

IPv4 – *Internet Protocol version* 4

IPv6 – *Internet Protocol version* 6

ISO – *International Standards Organization*

JDK – Java *Development Kit*

JRE – Java *Runtime Environment*

MB – *Megabyte*

NASL – Nessus *Attack Scripting Language*

OSI – *Open Systems Interconnection*

PDF – *Portable Documente Format*

RSTP – *Rapid Spanning Tree Protocol*

SI – Segurança da Informação

SMS – *Short Message Service*

SO – Sistema Operacional

SSL – *Secure Socket Layer*

TCP – *Transmisson Control Protocol*

TCP/IP – *Transmission Control Protoco l Internet Protocol*

TCJ – Tribunal de Contas da União.

UDP – *User Datagram Protocol*

VLAN – *Virtual Local Area Network*

SUMÁRIO

1 INTRODUÇÃO

Nos tempos atuais, as informações armazenadas precisam de muita segurança. Para isto, existe um campo da computação denominado de Segurança da Informação (SI). Dentre os objetivos deste campo, está a redução das chances de informações de acesso restrito (secretas) cair em mãos erradas.

"Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional" (FONTES, 2006, p.3).

"A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa" (PEIXOTO, 2006, p.37).

"A segurança da informação existe para minimizar os riscos em relação à dependência do uso dos recursos de informação para o funcionamento da organização." (FONTES, 2006, p.11).

Um ambiente idealmente seguro, tem as seguintes características: possuir política para usuários e funcionários; possuir política de serviço, política de *backup*, *firewall*, Proxy, equipe bem treinada para suporte, usuários conscientes, VLAN[1] e softwares para auxiliarem a SI. Para que estas características sejam seguidas, alguns softwares são utilizados, como, por exemplo: o Zabbix (software usado para monitorar o desempenho de toda a infraestrutura de uma rede, além de aplicações); Wireshark (software usado para capturas de pacotes de uma determinada rede que, através desta captura, é feito uma análise detalhada de cada campo do protocolo no pacote em questão); Packet Tracer (programa usado para monitorar e simular virtualmente como um ambiente de rede irá se comportar ou como se comporta), Nessus (software usado para detectar falhas na rede através de escaneamentos feitos a partir de políticas montadas com recursos do próprio programa), dentre outros.

Para um ambiente seguro, não basta o melhor sistema de segurança, como citado, também é necessário que os usuários sigam as orientações dadas

1 Vlan: *Virtual Private Network* - Rede Virtual Privada

pelos responsáveis do ambiente computacional ou de rede e, além disso, eles precisam estar atentos às dicas dadas por pessoas atuantes na área de SI.

Entretanto, não existem somente pessoas especializadas em SI, têm-se, também, muitas empresas e instituições governamentais e não governamentais, que auxiliam, não somente os profissionais da área, mas também, usuários que estão preocupados em zelar pela segurança no ambiente virtual. Muitas dessas instituições e empresas são respeitáveis, podendo-se citar: CGI.br (Comitê Gestor da Internet da Internet no Brasil), Cert.br (Centro de Estudos, e Resposta e Tratamento de Incidentes de Segurança da Informação), Internet Segura.br, entre outros.

A importância dos usuários estarem conscientizados, mesmo não sendo da área de SI, é porque são cada vez mais comuns ataques em ambientes computacionais de pequeno a grande porte, podendo ser citados: spam, vírus, *Internet Banking*, *phishing*, ataques a empresas e a pessoas de modo geral, além de, também, os crimes cibernéticos, como: *Hackers* que atacam servidores, manipulação de dados, dentre outros.

Tendo isso em mente, nota-se que nenhum sistema é completamente infalível, muito menos completamente seguro. Com isso, é necessário buscar formas de evitar ataques que explorem as falhas e as vulnerabilidades no ambiente de SI.

Porém, graças a essa área, existem técnicas de defesa e softwares que indicam as falhas no ambiente em questão, como os antivírus e os scanners de rede.

Para a administração de redes, existem ferramentas que auxiliam nesse processo. As ferramentas utilizadas nos dias de hoje, mostram falhas e vulnerabilidades de uma rede, permitindo ao administrador, em tempo hábil, fazer as correções necessárias para manter o ambiente seguro. Dentre elas, elenca-se: o Nessus e o NMAP, que, em conjunto, serão utilizados para o estudo de campo.

O Objetivo geral deste trabalho é a utilização de ferramentas de escaneamento de rede (*scanners de rede*), em que será possível observar a detecção de vulnerabilidades e falhas de rede.

Os objetivos específicos, ao longo deste trabalho, se basearão em conhecer algumas características do protocolo TCP/IP, focando na versão 4 do protocolo IP; montar uma rede para usar os softwares Nessus e NMAP, usando 2

hosts virtualizados através do programa VirtualBox; preparar um ambiente com uma rede configurada via DHCP, utilizando IPv4; instalar um servidor e configurá-lo com o Nessus e NMAP, para realizar os escaneamentos; prever qual é o melhor tipo de política a ser adota nos escaneamentos da rede; escolher qual é o melhor conjunto de *flags* para a realização dos testes usando o NMAP; preparar um cliente onde serão realizados os testes com o Nessus e o NMAP; Executar os escaneamentos com o *softwares* Nessus e NMAP; e analisar os resultados obtidos.

O trabalho resume-se em mostrar a importância da SI nos tempos atuais, ainda mais em ambientes computacionais, além de mostrar que o campo de SI possui *softwares* e recursos que auxiliam na tarefa de manter o ambiente seguro. Para um ambiente mais seguro, é importante que se faça uso de softwares que colaborem com a segurança, porém sozinhos não garantem a plena segurança. É necessário também, que os administradores saibam usar e interpretar os relatórios gerados pelas ferramentas, tendo sempre que estar atualizado em relação às inovações e problemas do campo de Tecnologia da Informação, caso não estejam preparados, apenas um software não atualizado poderá gerar falhas, vulnerabilidades e incidentes na rede.

Neste trabalho, serão observadas inicialmente, informações importantes sobre o vasto campo de SI, juntamente com a apresentação das ferramentas que serão utilizadas no estudo de campo (Nessus e NMAP); seguindo-se para o modo com que foi feito o estudo de campo, através de um fluxograma (imagem que mostra os passos a ser realizados para uma determinada tarefa); posteriormente serão observados, os resultados obtidos e algumas explicações provenientes da coleta dos resultados dos testes gerados pelos programas Nessus e NMAP. Também será feito um “manual” do passo a passo, de como foi feito o uso dos *softwares* Nessus e NMAP.

2 SEGURANÇA DA INFORMAÇÃO

Atualmente, todas as pessoas têm informações, como fotos, documentos, músicas, entre outros; que precisam ser armazenadas com certa segurança. Para isso, é utilizado o ambiente computacional e alguns quesitos de SI.

A informação é um recurso que tem valor para a organização e deve ser bem gerenciada e utilizada. Para tanto é necessário garantir que ela esteja disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais na organização. (FONTES, 2006, p. 38).

2.1 DEFINIÇÃO DE SI

Com essas necessidades, torna-se necessário utilizar alguns recursos da área de Segurança da Informação (SI).

> Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada. (FONTES, 2006, p. 11).

O campo de SI é utilizado para auxiliar os usuários e os administradores de rede a evitar incidentes e falhas relacionadas à segurança, que podem prejudicar o usuário em si e, até mesmo, causar grandes prejuízos a empresas e órgãos governamentais e não governamentais.

2.2 SERVIÇO DE DISPONIBILIDADE

Muitos fatores estão ligados a informação, principalmente quando é levada em consideração a SI. Observando a cartilha do Tribunal de Contas da União – TCJ, tem se a definição da disponibilidade de Informação.

> [...] Disponibilidade da Informação consiste na garantia de que as informações estejam acessíveis ás pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõem garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem de direito. (BRASIL, 2007, p. 26).

Pode-se concluir então que a disponibilidade de serviço é a informação ficar sempre disponível para os usuários e componentes que a utilizam, sem qualquer problema com interrupções ou atrasos para acessá-la.

2.3 PILAR DE SEGURANÇA DA INFORMAÇÃO

Nos dias de hoje o campo de SI é constituído em alguns pilares bases que a sustentam. Para Peixoto (2006, p.38-39) este pilar é constituído de 3 componentes que são: a Confidencialidade, a Integridade e a Disponibilidade.

A Confidencialidade tem como característica.

> [...] A tramitação das informações deve contar com a segurança de que elas cheguem sem que dissipem para outros meios ou lugares onde não deveriam passar. Recursos como criptografar as informações enviadas, autenticações, dentre outros, são válidos desde que mantenham também a integridade destas informações; (Peixoto, 2006, p. 38-39).

Depois da Confidencialidade o segundo componente é a Integridade que para tem como característica.

> [...] Após a certeza de uma chegada confiável das informações, ou seja, recebidas pela pessoa correta e enviadas pela que realmente se esperava ter enviado, deve-se esperar também que as informações não tenham sofrido nenhum tipo de modificação ou alteração comprometendo sua real veracidade, levando á perda da integridade que continham quando partiram da origem; (PEIXOTO, 2006, p. 38-39).

O último componente é a Disponibilidade, que possui a seguinte característica.

> [...] De nada adiantaria termos a confidencialidade e a integridade se tais informações não estiverem disponíveis para serem acessadas. Talvez um dos grandes desafios seja justamente conseguir manter essa estrutura da passagem destas informações de forma confiável e íntegra sem que haja a enorme dificuldade ou até mesmo a impossibilidade de captar de forma viável tais informações. (Peixoto, 2006, p. 38-39).

Já para Fontes (2006, p.12) o pilar é composto por mais componentes dos quais pode-se citar: Auditabilidade e o Não repúdio de autoria. Segundo ele, a Auditabilidade é: "[...] o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação." (FONTES, 2006, p. 12).

Já o Não repúdio de auditoria tem como característica: "[...] o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria." (FONTES, 2006, p. 12).

2.4 CONCEITOS DE SEGURANÇA

Quando se fala em SI, em específico a própria informação, verifica-se que elas estão dispostas a uma série de perigos, desde seu armazenamento até o momento do transporte de um ponto a outro. Esses perigos são detectados em diferentes momentos e podem resultar em uma pequena perda ou, até mesmo, um roubo de enormes proporções. Para isso, é necessário conhecer os fatores perigosos aos quais as informações estão submetidas.

2.4.1 Ameaças

O primeiro desses fatores são as ameaças que são: "Potencial para violação da segurança quando há circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade." (STALLINGS, 2008, p. 6).

Deste modo pode- se entender que uma ameaça é uma brecha aberta para um possível ataque acontecer (explorando a vulnerabilidade), o que pode causar impactos nos *hosts*[2] ou em ambientes de rede.

2.4.2 Vulnerabilidades

A vulnerabilidade pode ser um fator que colabore com outros problemas aos quais as informações estão dispostas.

> Vulnerabilidade é a condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. (Cert.BR, 2012, p. 122).

A vulnerabilidade acontece por meio de brechas deixadas abertas por usuários e administradores de rede que não atualizaram e/ou configuraram serviços ou equipamentos de rede da maneira correta.

2.4.3 Riscos

Os riscos podem ser considerados como a junção das vulnerabilidades com as ameaças. “Risco é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização.” (FONTES, 2010).

Pode-se dizer então que o risco acontece por meio de brechas que não estavam protegidas, podendo assim causar falhas e, até mesmo, incidentes de segurança.

2*Host*: é qualquer dispositivo que pode se conectar numa rede, como exemplo pode-se citar: impressoras de rede, computadores, celulares, *tablets*, dentre outros.

2.4.4 Falhas

As falhas estão ligadas a etapa de alguma transição ao qual a informação passa. “É qualquer erro que redunde em interrupção do processamento.” (GENARI 2003, p. 141).

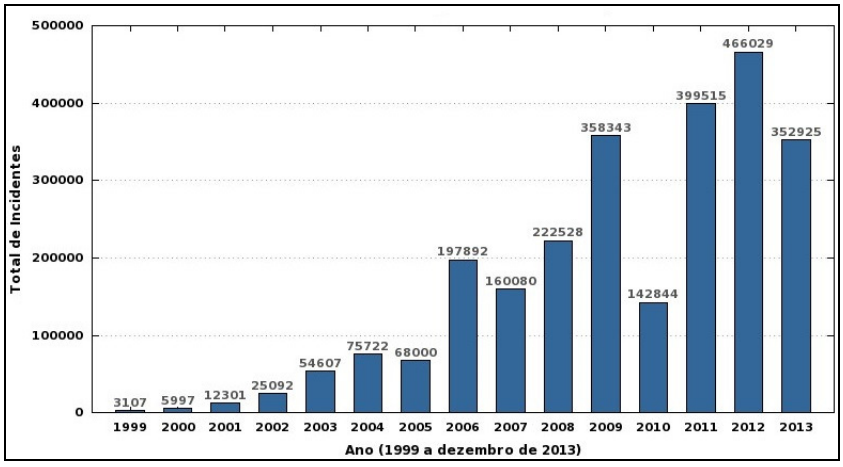
A falha pode acontecer no momento que algo diferente acontece durante algum processamento, podendo ser visto em *downloads*, no qual em certo momento o transporte de algum dado ou informação falha e compromete o resultado final do mesmo.

2.4.5 Incidentes de segurança

Os incidentes abrangem diversos aspectos, que “[...] é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.” (Cert.BR, 2012, p. 116).

A Figura 1 apresenta um gráfico onde pode-se observar que o número de incidentes vem aumentando conforme o passar dos anos, devido a diversos fatores. Esse número teve grande aumento a partir do ano de 2010, mantendo-se acima da casa dos 300 mil, levando somente em consideração o Brasil.

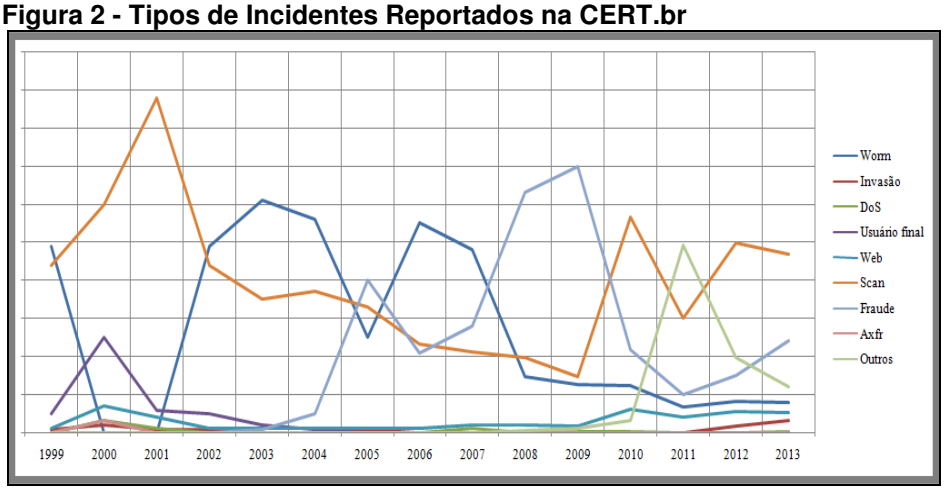
Figura 1 - Total de Incidentes Reportados ao CERT.br por Ano



Fonte: CERT.BR (2015)

Os aumentos de incidentes ocorrem também devido ao aumento no número de tipos de incidentes. Foram reportados a CERT.BR diferentes tipos de incidentes que por eles foram publicados no ano de 2014, conforme pode ser visto na Figura 2.

Figura 2 - Tipos de Incidentes Reportados na CERT.br



Fonte: CERT.br (2014)

Alguns tipos de incidentes são muitos conhecidos, sendo eles o DoS, Invasão e o *Scan*. O DoS"[...] (DoS – *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede." (Cert.BR, 2014). Já a Invasão, é "[...] um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede." (CERT.BR, 2014).

O *Scan se caracteriza* como:

> [...] notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. (Cert.BR, p.135, 2014).

Não existem somente estes tipos de incidentes. Estes são apenas alguns tipos, existem muitos outros que estão ligados à infraestrutura, ao hardware, ao software e a outros fatores além da própria SI.

Com isso pode-se observar que qualquer usuário possui riscos que necessitam de cuidados especiais utilizando a Segurança da Informação. Caso o usuário não cuide das falhas abertas em seu *host* ou em um ambiente de rede gerenciado por ele, através de atualizações, configurações de segurança e configurações de seu Sistema Operacional (SO), qualquer pessoa que possua más intenções poderá explorar as vulnerabilidades geradas pelas falhas existentes, podendo causar uma ameaça que poderá virar até mesmo um ataque.

2.5 ATAQUES

Os ataques tem como características:

> Um ataque á segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança e violar a política de segurança de um sistema. (STALLINGS, 2008, p. 6).

Os ataques se caracterizam de diferentes formas e podem ocorrer em diferentes meios, os exemplos de ataque são: os de Demonstração de poder, os de Prestígio, os de Motivações Financeiras, os de Motivações Ideológicas e Motivações Comerciais.

Os ataques de Demonstração de poder se caracterizam por "[...] mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente." (Cert.BR, 2012, p. 17-18).

Já os ataques de Prestígio, ocorrem pelo atacante que quer se:

> [...] vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo. (Cert.BR, 2012, p. 17-18).

Os ataques de Motivações Financeiras se caracterizam por: “coletar e utilizar informações confidenciais de usuários para aplicar golpes [...]” (Cert.BR, 2012, p. 17-18). Já os de Motivações Ideológicas “[...] tornar inacessível ou invadir sites que divulguem conteúdo à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.” (Cert.BR, 2012, p. 17-18). E os de Motivações Comerciais, por “tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.” (Cert.BR, p. 17-18).

Esses ataques se dividem em dois tipos diferentes, os ataques ativos e os ataques passivos.

2.5.1 Ataques passivos

Os ataques passivos “[...] possuem a natureza de bisbilhotar ou monitorar transmissões. O objetivo é obter informações que estão sendo transmitidas. Dois tipos de ataques passivos são liberação do conteúdo da mensagem e análise de tráfego.” (STALLINGS, 2008, p. 7).

> [...] são muitos difíceis de detectar, pois não envolvem alteração dos dados. [...] Porém, normalmente, é viável impedir o sucesso desses ataques por meio da criptografia. Assim, a ênfase em lidar com ataques passivos está na prevenção, em vez de na detecção. (STALLINGS, 2008, p. 7).

Um exemplo deste ataque é quando um “atacante” fica bisbilhotando o usuário digitar a senha no computador ou na maquina de cartão de credito. Para evitar este tipo de inconveniente, o usuário tem que ser o mais discreto possível para digitar sua senha, evitando ter escrita em papeis, agendas, dentre outros lugares que fique exposto.

2.5.2 Ataques ativos

Os ataques ativos “[...] envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso [...]” (STALLINGS 2008, p.7).

Esses ataques:

> [...] apresentam as características opostas dos ataques passivos. Embora os ataques passivos sejam difíceis de detectar, existem medidas para impedir seu sucesso. Por outro lado, é muito difícil impedir ataques ativos absolutamente devido à grande variedade de vulnerabilidades físicas, de software e de rede em potencial. Em vez disso, o objetivo é detectar ataques ativos e recuperar-se de qualquer interrupção ou atrasos causados por eles. [...] (STALLINGS, 2008, p. 8).

2.5.3 Atacantes

“A intrusão não autorizada em um sistema ou rede de computadores é uma das ameaças mais sérias à segurança de computadores.” (STALLINGS, 2008, p. 7).

Atualmente, as pessoas que efetuam os ataques são conhecidas como *hackers*, mas no passado eles eram apenas pessoas que possuíam grande conhecimento sobre o ambiente computacional.

> [...] Os verdadeiros “Hackers” eram especializados em informática que estudavam ou trabalhavam com computadores, em especial nos Estados Unidos. Hoje, grande parte dos “Hackers” originais trabalha na área de segurança de computadores para grandes empresas e até para governos. [...] o “Carder”, que é aquele que falsifica e opera com cartões de crédito, o “Phreaker”, especializado em delitos envolvendo telefonia e muitos outros, identificados de acordo com sua área de atuação. [...]. (GONÇALVES, 2003, p.1).

Além desses termos alguns outros surgiram, sendo um dos mais conhecidos na área o *cracker.* “Os crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos.” (MARTINS, 2012).

Em alguns países ao redor do mundo os atacantes, mais especificamente os intrusos, trabalham para o governo. Caso algum deles se recuse, vai para a cadeia cumprir sua pena.

2.6 PROTOCOLO TCP/IP

Nos tempos atuais, as redes de computadores trabalham usando protocolos baseados no Modelo ISO/OSI, este que é constituído de 7 camadas. Cada camada tem sua função no processo de comunicação numa rede e vários protocolos atuando em cada camada, sendo responsáveis por uma função ou serviços na rede.

> Para facilitar a interconexão de sistemas de computadores, a ISO (International Standards Organization), desenvolveu um modelo de referência chamado OSI (Open Systems Interconnection) para que os fabricantes pudessem criar protocolos a partir deste modelo. (TORRES, 2007).

Dentre os vários protocolos existentes um dos que mais conhecidos são o TCP e o IP, popularmente conhecidos também por TCP/IP. Ambos trabalham lado a lado, só que em camadas diferentes e com funções diferentes, mais um auxilia o outro.

O protocolo IP – *Internet Protocol* – Protocolo de Internet, é responsável pelo endereçamento dos *hosts* na rede. Este protocolo possui várias versões, as mais conhecidas são a IPV4 e o IPV6 (versão 4 e 6).A versão 4 foi substituída pela versão 6 por ocorrer o esgotamento dos endereços IP disponíveis.

Para IPv6.br [s.d.] A versão 4 do protocolo IP, foco deste trabalho, ainda está em uso. Ela possui cerca de 4 bilhões de endereços disponíveis. Mais com o aumento das redes, celulares e a Internet das Coisas, foi preciso criar uma nova versão do protocolo para atender a demanda. A nova versão foi a 6 (IPv6).

Segundo IPv6.br [s.d.] Já a versão 6 deste protocolo, apresenta uma grande diferença na quantidade de endereços possíveis, que chegam em torno de 340 undecilhões de endereços.

Já o protocolo TCP –*Transmisson Control Protocol* – Protocolo de Controle de Transmissão, tem como responsabilidade estabelecer uma conexão e verificar se a mensagem chegou corretamente no seu destino. Caso algum pacote tenha sido extraviado no caminho o mesmo é enviado novamente, ou seja, o TCP tem transmissão confiável.

"O TCP/IP é o padrão mais aceito hoje pelos sistemas operacionais e redes, além de ser através desses conjuntos de protocolos que é possível se conectar à internet." (RASMUSSEN, 2003).

2.6.1 Portas TCP

O protocolo TCP/IP, dá suporte a vários serviços de rede e estes serviços, precisam de uma ou mais portas para ser executados.

A Tabela 1 representa alguns serviços que o TCP/IP dá suporte, acompanhado da descrição do serviço e o protocolo responsável pelo serviço.

Tabela 1 - Algumas portas atribuídas

Porta	Protocolo	Uso
21	FTP	*File Transfer* (Transferência de Arquivos)
23	Telnet	*Login* remoto
25	SMTP	Correio eletrônico
69	TFTP	*Trivial File Transfer Protocol*(Protocolo Trivial de Transferência de Arquivos)
79	Finger	Pesquisa de informações sobre um usuário
80	HTTP	*World Wide Web*
110	POP-3	Acesso remoto a correio eletrônico
119	NNTP	Notícias da USENET

Fonte: TANENBAUM (2003, p.568)

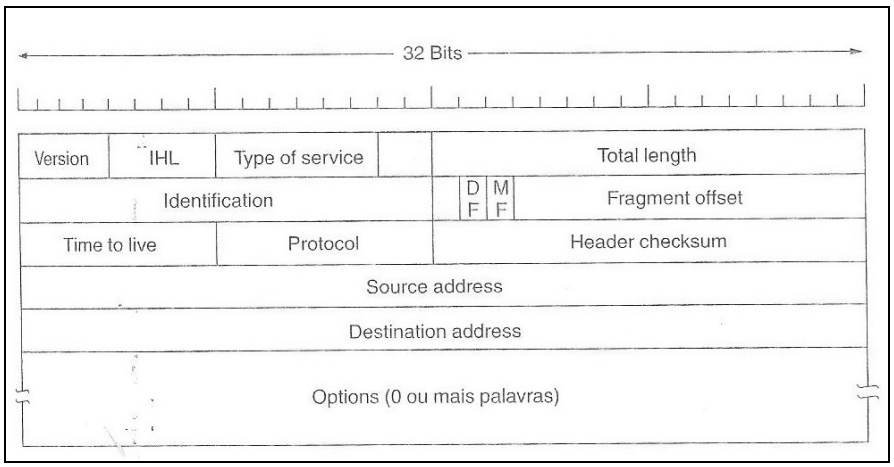
2.6.2 Flags

Os protocolos de comunicação de rede usam pacotes de dados para poder trocar informações. Os pacotes de dados além de possuir os próprios dados, possuem cabeçalho. Este cabeçalho traz várias informações importantes para o processo de comunicação. Além do cabeçalho, os protocolos utilizam o datagrama[3]. Um datagrama possui dois endereços: o endereço de origem do remetente e o endereço de destino (destinatário).

Para uma mensagem chegar ao seu destinatário, a mesma fica sujeita ao seu tamanho. Caso seja muito grande será dividida em vários pedaços denominados de fragmentos.

Na Figura 3 pode-se observar o formato do cabeçalho protocolo IPV4.

Figura 3 - O cabeçalho IPV4 (Internet Protocol)



Fonte: Tanenbaum (2003, p.461)

Para Tanenbaum (2003, p.461) o campo *Version* é usado para determinar a versão do protocolo a qual o cabeçalho pertence. Já, segundo ele, o campo IHL informa o tamanho do cabeçalho, pois o cabeçalho não tem tamanho fixo, na Figura 3 é apresentado um cabeçalho IPv4 com 32 bits e o campo *Type of service* foi um dos que sofreu mais modificações ao longo dos anos. Sua função é diferenciar as classes de serviços.

3 Datagrama: "É [...] Cada pacote de entrada ou saída é chamado de datagrama IP. [...]." (MICROSOFT [s.d.]).

Em seu livro, mostra que “O campo Total *lenght* inclui tudo que há no datagrama – cabeçalho e dados, mostrando seu tamanho. [...] (TANENBAUM, 2003, p.462)” e que “O campo *Identification* é necessário para permitir que o host de destino determine a qual datagrama pertence um fragmento recém-chegado.” Todos os fragmentos de um datagrama contêm o mesmo valor de *Identification*.(TANENBAUM, 2003, p. 462), ou seja, se uma mensagem for dividida em vários fragmentos, todos os fragmentos desta mensagem vão receber o mesmo valor neste campo. Também segundo ele “O campo Fragment offset informa a que ponto do datagrama atual o fragmento pertence. [...]”.

Já o campo *Time to live*, serve como um contador que é usado para definir o limite de vida do pacote. O objetivo deste campo é evitar que o pacote fique eternamente trafegando na rede, causando loops que deixam a rede lenta e podendo até causar perdas de pacotes. A vida vai sendo decrementada de acordo com o trafego do pacote pelos nós da rede. (TANENBAUM, 2003, p.462)

“[...] O campo Protocol informa a que processo de transporte o datagrama deve ser entregue. [...]” (TANENBAUM 2003, p.463), ou seja, este campo é pra identificar qual protocolo vai fazer a entrega do pacote, dentre as possibilidades está o TCP e o UDP (*User Datagram Protocol*- Protocolo de datagrama de usuário). “O campo Header checksum confere apenas o cabeçalho. [...]”. (TANENBAUM, 2003, p.463)

“Os campos Source address e Destination address indicam o número do host. [...]”, (TANENBAUM, 2003, p.463), e o campo *Options* é usado para colocar opções que o projeto original do protocolo não contém.

Os pacotes podem possuir *flags*, que são usadas para operação de controle do pacote em questão. A Tabela 2 mostra cada uma das *flags*, e sua função no protocolo TCP/IP.

Tabela 2 - *Flags* do protocolo TCP/IP

URG	É um ponteiro apontando que este pacote possui dados importantes;
ACK	É um número que identifica a confirmação que recebeu o último pacote ou outro tipo de resposta;
PSH	Envia imediatamente ignorando a capacidade do *buffer*;
RST	Inicia novamente a conexão;
SYS	Inicio de conexão;
FIN	Finaliza a conexão.

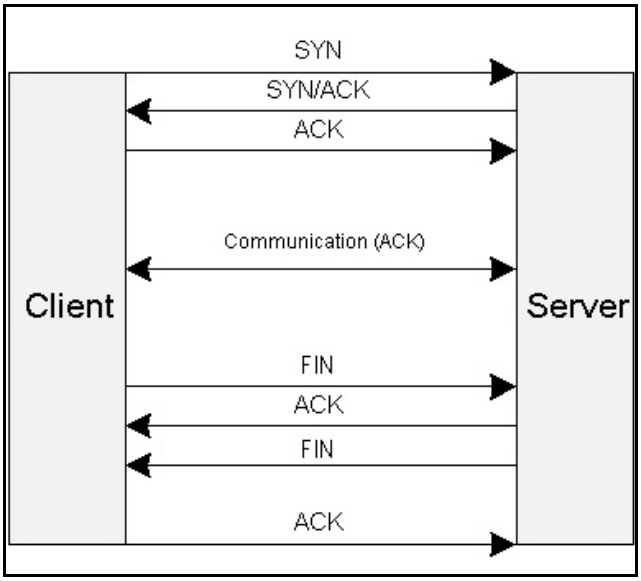
Fonte: Adaptado de Forouzan (2008, p. 722)

Pode-se então observar que a *flag* URG é usada quando o pacote contém dados importantes; a *flag* ACK é usada para avisar que o último pacote chegou ao seu destino; o PSH é usado para envio imediato, ignorando o estado de *buffer*; a *flag* RST inicia a conexão novamente; a *flag* SYN inicia a conexão; e a *flag* FIN finaliza o processo de comunicação entre o emissor e receptor.

2.6.3 Processo de comunicação do TCP/IP

O protocolo TCP é um protocolo de transporte e possui conexão garantida, devido a um processo de conexão que ocorre no momento da comunicação entre emissor e receptor, denominado como *3wayhandshakeconnection*. Este processo monitora desde o primeiro pacote, que começa a trafegar pela rede para ir ao seu destino, até o último que realizará esse processo. Este processo de comunicação entre cliente (*client*) e servidor (*Server)* pode ser observado na Figura 4.

Figura 4 - Processo de Comunicação TCP/IP



Fonte: InformaBR (2015)

O cliente (Client) inicia o processo enviando uma solicitação de comunicação ao servidor (Server) com a *flag* syn para iniciar a comunicação. O servidor retorna com as flags syn/ack, respondendo a solicitação de comunicação. Após isso, ambos (cliente e servidor) trocam mensagens com a *flag* ack. Quando é encerrada a troca de mensagens o cliente manda a *flag* fin para o servidor encerrar a conexão. O servidor entende isso e responde com a *flag* ack, retornando com a *flag* fin finalizando a conexão, para encerrar o cliente confirma o fechamento de conexão com a *flag* ack.

A modificação da ordem das flags dentro do pacote TCP/IP faz com que o protocolo se comporte de maneira diferente em relação ao comportamento padrão. Essa característica do protocolo é explorada pelas técnicas de invasão em programas do tipo *scanner* de rede e de vulnerabilidades.

2.7 PORTAS x *FLAGS* x ATAQUES x TÉCNICAS DE INVASÃO

Os ataques acontecem por meio de técnicas de invasão. O processo de ataque é feito por um ou mais atacantes, escolhendo um alvo. Depois de ter feita a escolha do alvo, é preciso conhecer o ambiente de rede do alvo, para isto é

usado ferramentas que fazem a verificação do ambiente. Uma ferramenta muito útil neste processo é o NMAP (considerado como ataque ativo), pois o usuário escolhe um endereço IP ou faixas de IP, para saber se existem *hosts* online. Caso o atacante ache um servidor, por exemplo, ele pode continuar usando o próprio NMAP, combinando varias *flags*, para saber que serviços estão rodando, quais portas estão abertas neste *host*, dentre outras características para conhecer o alvo. A partir destas informações levantadas, o atacante precisará verificar a existência de falhas, que são possíveis de atacar, para iniciar o processo de ataque.

Já o Wireshark é um programa farejador de rede, ou seja, uma ferramenta que fica “escutando” tudo o que se passa, capturando pacotes. Estes podem ser analisados e podem mostrar onde os atacantes podem agir. O Wireshark é considerado como um programa de ataque passivo, pois ele só escuta os dados que estão passando pela rede, ele não consegue modificar os dados que estão sendo trafegados na rede.

Há ainda distribuições Linux que contém muitas ferramentas que fazem testes de invasão e auditoria de segurança em redes de computadores. Dentre essas distribuições estão o Kali e o Backtrack (descontinuado). “Kali é uma reconstrução completa do Back Track Linux, que adere totalmente aos padrões de desenvolvimento do Debian. [...]” (kali linux [s.d.]).

Outra ferramenta que pode ser usada é o Nessus, que pode ser usado tanto para segurança como também para ataques, pois ele mostra falhas e vulnerabilidades num ambiente de rede. Para isto, é necessário configurar políticas que já vêm pré-configuradas ou criá-las do zero. O resultado do Nessus pode ser visto por tipos de falhas e vulnerabilidades detectadas ou por *host*.

2.8 FERRAMENTAS QUE AUXILIAM A SI

Para minimizar a chance de ocorrência de ataques é necessário que os usuários tenham ferramentas que dêem um pouco de segurança no ambiente de rede.

Essas ferramentas são necessárias, pois detectam esse tipo de problema, através de testes que simulem ataques na rede, prevenindo incidentes de SI, falhas e vulnerabilidades. Essas ferramentas são denominadas como *scanners* de rede.

Para o presente trabalho, o estudo será abordado sobre ferramentas de segurança de rede. As ferramentas escolhidas para serem usadas serão o Nessus e o NMAP.

2.8.1 Nessus

O Nessus é uma ferramenta que auxilia na SI.

> [...] é um scanner de segurança de rede poderoso e fácil de usar, com um banco de dados de plugins abrangente e atualizado diariamente. [...] O Nessus permite realizar auditorias remotas e determinar se a rede foi comprometida ou usada de maneira indevida. O Nessus também permite verificar a presença de vulnerabilidades, especificações de conformidade, violações de políticas de conteúdo e outras anomalias em um computador local. (TENABLE 2014, p. 6).

Pode-se então observar que o Nessus examina ambientes de rede, sendo possível, até mesmo, examinar serviços, por exemplo, um servidor na porta TCP 7000.

Para Morimoto (2008) o Nessus nas suas versões iniciais (até a versão 2.2.8) era um software *open-source* (o código dele era liberado para qualquer pessoa) e as versões podiam ser personalizadas de acordo com o cliente. A Tenable Network Security (empresa responsável pelo Nessus) fazia *plugins* específicos para cada cliente, porém muitas empresas concorrentes aproveitavam desta característica da Tenable para lançar novos produtos no mercado que competiam com o seu produto. Após a versão 2.2.8, o Nessus passou a disponibilizar suas versões de forma paga, embora estejam disponíveis também versões gratuitas, porém com menos funcionalidades.

Atualmente o Nessus é disponibilizado nas versões Home, Professional, Manager e Cloud.

A versão Home, a qual será dada foco neste trabalho, tem como objetivo o uso doméstico e é uma versão bem mais básica. Já o Nessus Professional é uma versão voltada para empresas e é paga. O Nessus Manager é usado para gerenciamento de empresas e o Cloud é voltado para o uso de computação nas nuvens.

Este software, após efetuar os escaneamentos (testes), gera relatórios com níveis de criticidade baseados no CVE (*Common Vulnerabilities and Exposures* – Vulnerabilidades e Exposição Comuns) e Bugtraq, que é uma lista de endereços eletrônicos (grupo de *e-mail*) que discute sobre SI, vulnerabilidades e como corrigir as tais vulnerabilidades.

Uma das características importantes para o Nessus é a Varredura Inteligente que tem como característica.

> [...] Ao contrário de outros scanners de segurança, o Nessus não gera alarmes falsos. O programa não pressupõe que um determinado serviço está sendo executado em uma em uma porta fixa. Isso significa que, se o servidor Web for executado na porta 1234, o Nessus o detectará e testará sua segurança da forma apropriada. O programa verificará uma vulnerabilidade por meio de exploração sempre que possível. [...]. (TENABLE 2014, p.6).

Outra característica é sua arquitetura modular que pode ser classificada como:

> Arquitetura cliente/servidor oferece a flexibilidade de instalar o scanner (servidor) e conectar-se à interface gráfica do usuário (cliente) por intermédio de qualquer computador com um navegador, reduzindo, assim, os custos de gerenciamento (um servidor pode ser acessado por vários clientes). (TENABLE 2014, p.6).

Outra característica que se destaca é a arquitetura de plugins, que tem como objetivo.

> Arquitetura de plugin – Os testes de segurança são gerados por meio de um plugin externo e agrupados em uma das 42 famílias. Dessa forma, é possível adicionar facilmente seus próprios testes, selecionar plugins específicos ou escolher uma família inteira sem a necessidade de leitura do código do mecanismo do servidor Nessus, nessusd. [...]. (TENABLE 2014, p.6).

Os *plugins* são escritos na Linguagem NASL: “[...] – O *scanner* Nessus utiliza NASL (Nessus *Attack Scripting Language*), uma linguagem criada especificamente para a criação de testes de segurança de maneira fácil e rápida.” (TENABLE 2014, p.6).

O Nessus possui um banco de dados de vulnerabilidades atualizado, faz testes simultâneos em vários hosts e possui relatórios completos que tem como função: “[...] Além de detectar as vulnerabilidades de segurança existentes na rede e o nível de risco de cada uma delas (baixo, médio alto e grave), o Nessus oferece soluções para atenuá-las.” (Tenable 2014, p.6).

Os relatórios gerados após os escaneamentos podem ser vistos na tela do computador que está acessando o Nessus, sendo que, uma cópia, será guardada no próprio servidor para facilitar a futura análise dos dados. O Nessus possui o recurso de exportação de relatórios dos escaneamentos para a máquina que está acessando o servidor. A exportação pode ser obtida através de *download* do relatório em vários formatos como.PDF[4],HTML[5], .Nessus, dentre outros. Os modelos de relatórios adotados durante o estudo de campo foram HTML e PDF.

Observou-se no momento da exportação do relatório, tanto no PDF quanto no HTML, a existência de dois modelos de relatório sendo eles o *executive summary* (sumário executivo) e o customizado, que pode ser organizado por *host* e por vulnerabilidade. Como em ambos os testes realizados havia apenas um host sendo analisado, foi optado pela ordenação por *plugins*.

No relatório, do tipo sumário executivo, é possível perceber que existem 2 tabelas principais. A primeira com o nome do *host* analisado, podendo ser verificado nela informações de quantidade de vulnerabilidades totais achadas e por níveis. A segunda tabela possui informações do nível de cada criticidade, o número que detecta cada vulnerabilidade e o nome da vulnerabilidade. Caso o usuário precise de mais informações de uma determinada vulnerabilidade, torna-se necessário entrar no site do Nessus e procurar pelo número identificador de cada vulnerabilidade. O relatório sumário executivo está representado nas figuras

4 PDF: “Portable Documente Format (PDF) é um formato de arquivo usado para exibir e compartilhar documentos de maneira compatível, independente de software, hardware ou sistema operacional.” (ADOBE [s.d.]).

5 HTML: ”Hyper Text Markup Language. Uma linguagem de formatação de texto desenvolvida nos primórdios da Internet, mas padrão até hoje.” (MORIMOTO 2007).

que possuem o estudo de campo com os testes do Nessus. Sendo as figuras 11,12,15,16, 19 e 20.

No relatório customizado, existe uma separação por vulnerabilidades que são detectadas e, em cada vulnerabilidade apresentada, já vem toda sua descrição.

2.8.2 NMAP

O NMAP é uma ferramenta de *scanner* de rede que, através de comandos e *flags*, é possível obter dados dos alvos (*hosts*). Dentre estes dados, é possível encontrar *hosts* que estão *online* no momento, nome de aplicações rodando, versão do SO, tipos de *firewall*, dentre outras características.

> O Nmap (“Network Mapper”) é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. [...]. Embora o Nmap seja normalmente utilizado para auditorias de segurança, muitos administradores de sistemas e rede consideram-no útil para tarefas rotineiras tais como inventário de rede, gerenciamento de serviços de atualização agendados, e monitoramento de host ou disponibilidade de serviço. (NMAP [s.d.]).

3 METODOLOGIA

O trabalho caracteriza-se como um estudo de campo experimental, e propõe-se o desenvolvimento de um plano de teste, com relação à segurança dos dados da rede, utilizando Nessus e NMAP. Para isso, o cliente sofrerá uma série de ataques, para observar como a segurança desse *host* está e qual é a chance de perda, ou roubo, de dados do mesmo.

3.1 AMBIENTE

O ambiente a ser utilizado no estudo de caso terá o uso de duas máquinas virtuais, sendo uma utilizada como servidor e outra como cliente, onde serão montados cenários para a realização dos testes.

O *software* escolhido, e a ser usado, para gerenciar as máquinas virtuais, será o VirtualBox versão 4.3.18, da empresa Oracle. Esse *software* foi escolhido por ser *open-source* e atender os requisitos do problema proposto.

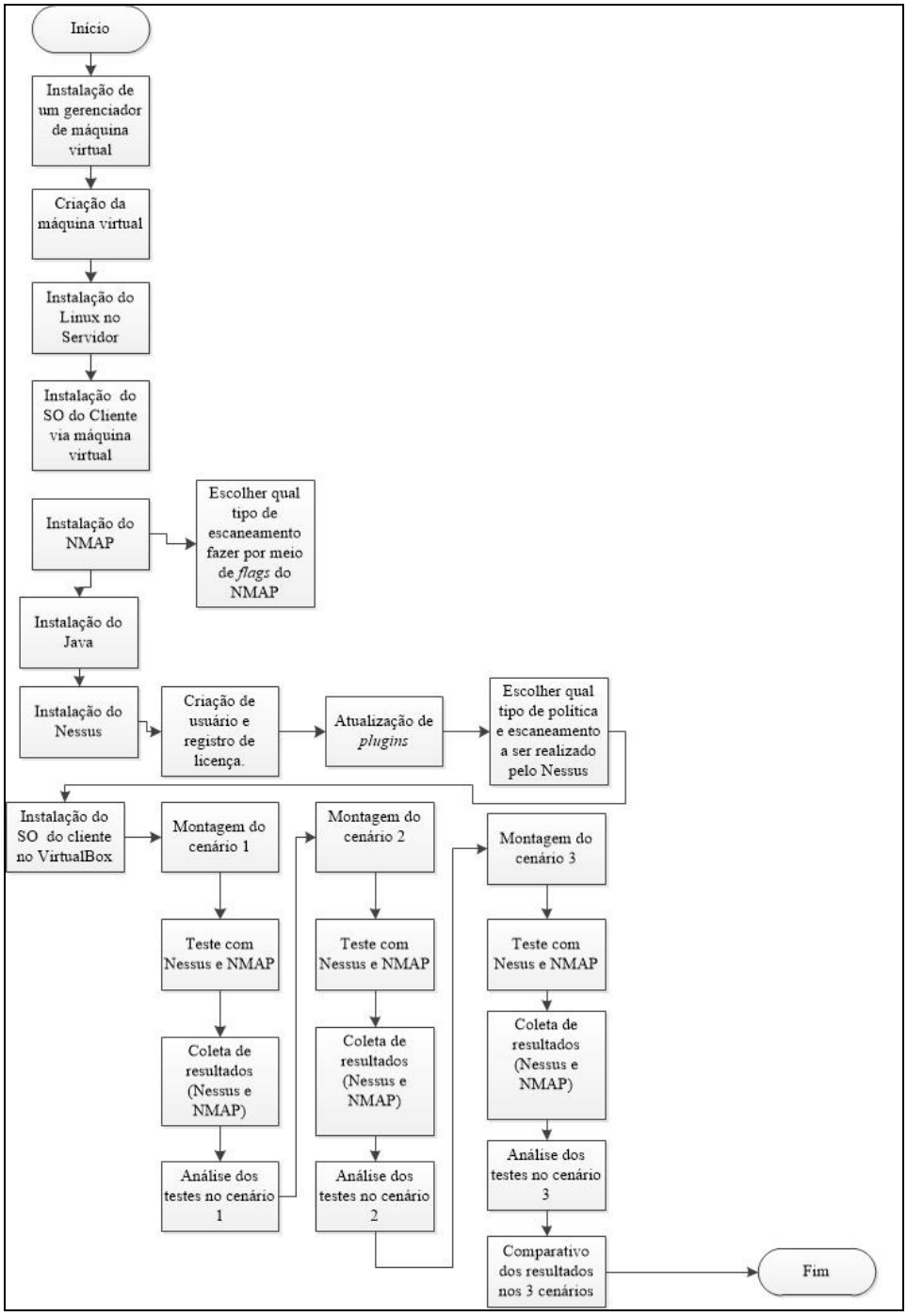
A configuração do Servidor fará uso do SO Debian versão 7.8.0 32 bits, com 1024 MB *(megabyte*) de memória Ram, Processador Intel core i3 1.50.GHz (*gigahertz*) e HD (disco rígido) de 30 GB (*gigabyte*). Já a máquina cliente terá o SO Windows 7 Professional 32 bits, com 1024 MB de memória Ram, Processador Intel I5 2.49 GHz e HD de 30 GB. Para as máquinas efetuarem comunicação via rede, foram configuradas, em ambas as máquinas virtuais, o tipo de conexão *bridge*[6].

3.2 ETAPA DOS TESTES

As etapas que foram adotadas para o estudo de campo podem ser observadas no fluxograma da Figura 5.

6 Placa de rede em modo bridge:"(...) onde a máquina virtual passa a ser ligada diretamente à rede principal, como se fosse um PC real ligado no hub. (...)".(MORIMOTO 2010).

Figura 5 - Fluxograma da metodologia do estudo de campo



Fonte: Próprio Autor (2015)

O processo do estudo de campo inicia-se com a instalação dos *softwares* que serão utilizados para gerenciar as máquinas virtuais no estudo de campo (Servidor e Cliente). Depois, é criado o ambiente do Servidor e é instalado o Debian juntamente com os *softwares* necessários para o estudo de campo, que serão: o NMAP, o Java e o Nessus.

Para saber como foi instalado e configurado o Java no servidor, consulte o apêndice B.

A instalação do cliente, é realizada com a instalação do VirtualBox e com a configuração da máquina virtual a ser utilizada como Cliente. Depois, passa-se a instalação do SO e a preparação dos cenários, onde serão aplicados testes com NMAP e Nessus.

Tanto no Nessus, como no NMAP é fundamental indicar o alvo, aonde o teste deve ser realizado, pode-ser feito via endereço IP ou nome do *host*.

Com todas as etapas de preparação prontas, monta-se o primeiro cenário no cliente, iniciando-se com o teste pelo NMAP. O No primeiro teste, será usado o comando nmap sem nenhuma *flag*. Outro teste realizado com o NMAP é a combinação com a *flag* "–A". Para maiores detalhes dos resultados dos testes consulte o apêndice A.

Após finalizar os testes com o NMAP, é iniciada a fase de testes utilizando o Nessus. Foram realizados dois testes no atual cenário utilizando o Nessus. O primeiro teste, a ser realizado no cenário, é o *Basic Network* (Básico de Rede) e o segundo é o *Host Discovery* (Descoberta de *host).* Para maiores detalhes de como foi configurado as políticas e os escaneamentos, além de como foi feita a instalação pode ser visto no apêndice C.

Com a conclusão do primeiro cenário, monta - se o segundo cenário no cliente e realiza-se os mesmos testes que já foram feitos no primeiro cenário. Com a conclusão desse cenário, passa-se ao próximo ao terceiro e repetem-se todas as etapas de testes.

Com a conclusão de todos os cenários, é feito uma comparação entre todos os cenários montados e submetidos aos mesmos testes, comparando qual é mais seguro e o menos seguro, segundo o que foi coletado com o Nessus e o NMAP.

]

3.3 CENÁRIOS

Todos os cenários a serem utilizados no atual estudo de campo, serão feitos no cliente que possui como SO, o Windows 7. Foram propostos 3 cenários diferentes, cada qual com diferentes tipos de configuração e softwares.

3.3.1 Cenário 1

O *host* terá o *firewall* do Windows desabilitado, juntamente com o Windows *Update*. O *firewall* é considerado como uma "porta", barrando ou liberando o acesso de programas e pacotes que querem comunicar-se com a máquina em questão. Para este cenário, esta "porta" estará liberando o acesso para todos os softwares e pacotes, independentemente de algo ruim acontecer ao ambiente. Já o Windows Update, realiza as atualizações de segurança e aprimoramento que a Microsoft lança para auxiliar em sua segurança do ambiente.

3.3.2 Cenário 2

O cliente terá o *firewall* ativado, porém o Windows Update continuará desativado. Então, esta "porta", bloqueará alguns pacotes e aplicações que tentarem trafegar no *host*.

3.3.3 Cenário 3

O *host* vai estar com a mesma configuração anterior, porém terá como antivírus instalado, o Avast Home, na versão 2015.10.2.2218. O Avast não será registrado e nem atualizado. Serão feitos os testes com a configuração padrão do Avast.

Na adoção do antivírus Avast (utilizado no estudo de campo), não se escolheu a opção de utilização do *firewall*, pois não é gratuito. Para utilizá-lo (*firewall* do Avast), uma das opções é a instalação do Internet Security. Para Avast [s.d.] “(...) Possibilita transações online seguras e emprega um firewall sofisticado para bloquear hackers.”.

4 ESTUDO DE CAMPO

Para mostrar os resultados dos testes executados nos cenários criados, adotou-se a técnica de *print screen* (foto da tela) para o nmap, com o objetivo de comprovar o que foi feito e, para o Nessus, adotou-se a importação dos relatórios, localizados no *host* servidor, nos formatos de arquivo PDF e HTML.

Para os relatórios do Nessus, adotou-se o tipo de relatório *executive summary* (sumário executivo), mais simples e breve, já que possuí as informações principais em apenas uma folha, trazendo apenas os números dos *plugin* encontrados, porém faz-se necessário procurar no site da Tenable[7] (responsável pelo Nessus) pelo número ou nome do *plugin* para entender o que o *plugin* representa.

Cada cenário adotado possui diferentes configurações. Em cada cenário realizou-se quatro testes, sendo dois com o NMAP e dois com o Nessus. Para a exibição dos resultados, separou-se os testes por cenário e, também, por ferramenta utilizada (NMAP e Nessus). Na ferramenta NMAP, utilizou-se como primeiro teste o comando NMAP junto ao seu complemento simples e no segundo com um *flag* junto a este comando.

No Nessus, utilizou-se no primeiro teste, a política de escaneamento *Basic Network Scan* (Escaneamento Básico de Rede) e no segundo a política *Host Discovery* (Descoberta de *host*).

4.1 CENÁRIO 1

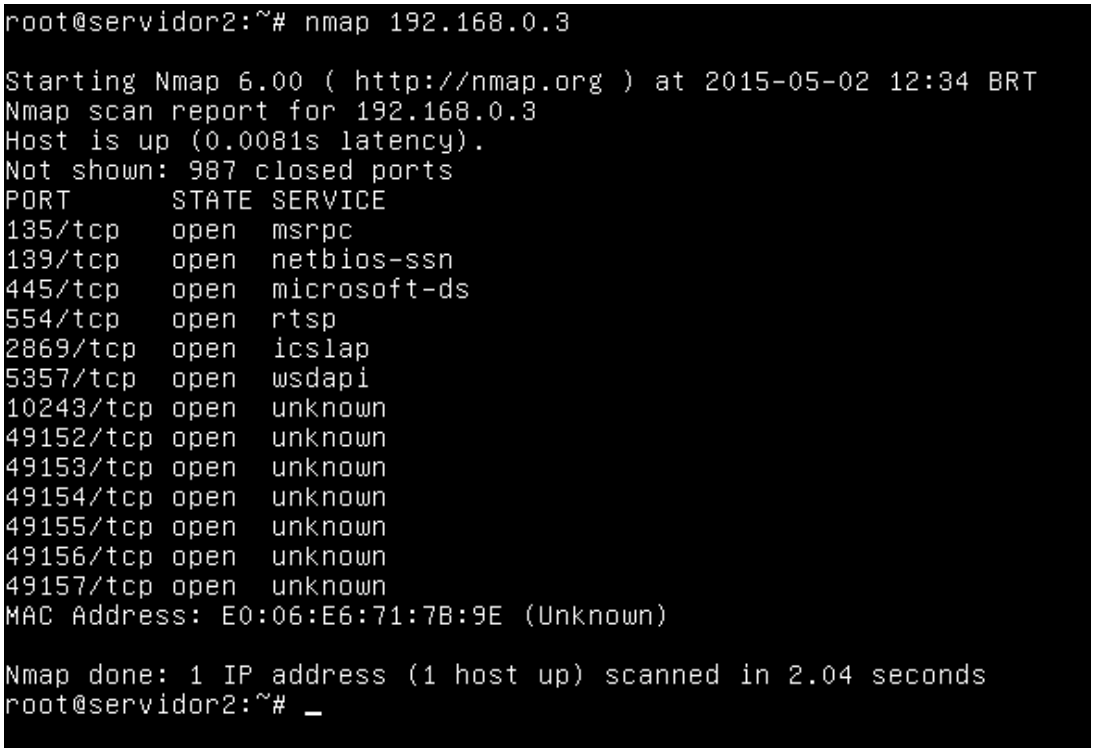
O cenário 1 é o mais simples e vulnerável para ataques, falhas e vulnerabilidades dentre os 3 cenários para o presente trabalho. Pois o *host* não possui nenhuma proteção para estes tipos de problemas, podendo ser alvo de atacantes. E mostra que se um determinado *host* estiver configurado sem nenhum tipo de proteção numa rede, além dele mesmo estar sujeito a atacantes, a rede fica mais vulnerável a problemas relacionados a SI.

7 Pesquisa para maiores detalhes dos plugins: http://www.tenable.com/plugins/index.php?view=search

4.1.1 Testes usando a ferramenta NMAP aplicada ao cenário 1

A Figura 6 mostra os resultados obtidos através dos testes com o NMAP. Através desse cenário pode-se detectar que várias portas, do protocolo TCP, estavam abertas, algumas rodando alguns serviços conhecidos e outras que não pode-se detectar o serviço que estava rodando. Dentre os serviços descobertos, pode-se elencar: o netbios-ssn[8], que está rodando na porta TCP 139; e o rtsp[9], que está trabalhando na porta TCP 554.

Figura 6 - Teste 1 com NMAP no cenário 1



Fonte: Próprio Autor (2015)

No resultado exibido, na Figura 7 também é possível observar o mac-address[10] (endereço mac da placa de rede), porém detectou sua origem, não

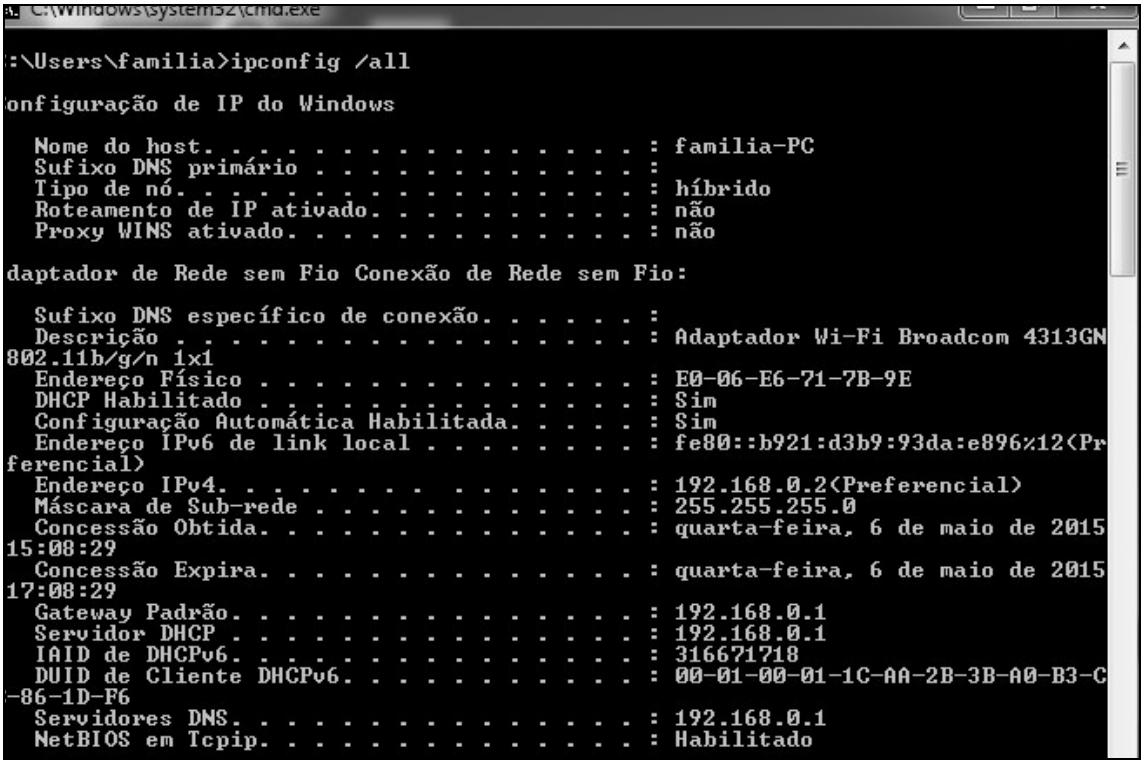
8netbios-ssn: "Permite que os aplicativos em computadores separados comuniquem-se através de uma rede local.[...] O NetBios não suporta um mecanismo de roteamento.[...]." SYMANTEC [s.d.]).

9 rtsp: "[...] Esse é um protocolo de nível de aplicativo, que foi criado especificamente para controlar a entrega de dados em tempo real, como, por exemplo, conteúdo de áudio e vídeo." (MICRSOFT 2007).

10 mac-adress: é um endereço escrito na base hexadecimal que todos os dispositivos conectados a uma rede possuem.

sendo o mesmo da máquina virtual. Esse endereço representa onde está instalado o cliente, que é usado nos testes.

Figura 7 - Resultado do comando "ipconfig /all" no host cliente



Fonte: Próprio Autor (2015)

Na Figura 8, são apresentados os resultados obtidos através do segundo teste realizado utilizando o comando NMAP no cenário 1. Pode-se observar através deste teste, utilizando o comando NMAP, as mesmas portas abertas, no protocolo TCP, do primeiro teste.

Além deste fator, observou-se a detecção do *mac-address* da máquina virtual (cliente Windows, onde foram realizados os testes), nome de *host* da máquina e o seu grupo como mostra a Figura 9.

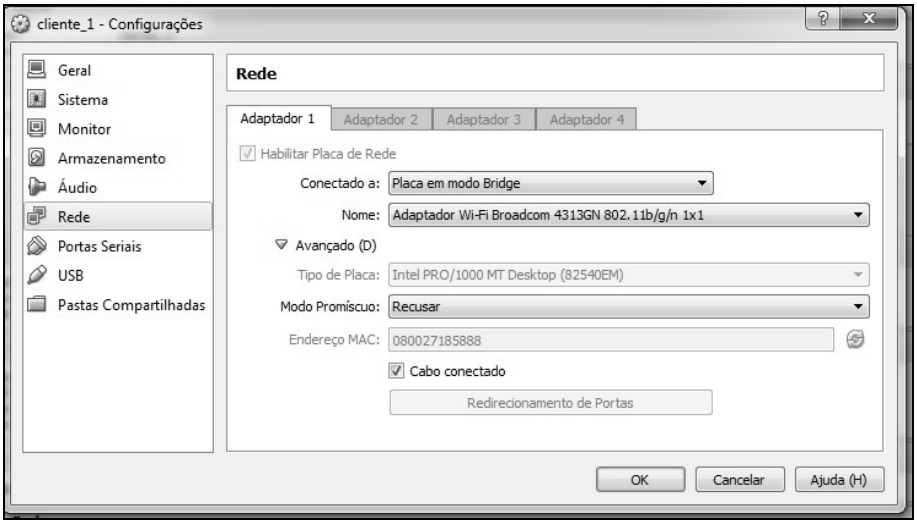
Na Figura 10, é possível visualizar, o nome do *host* é cliente_tcc, foi detectado como o SO **"Windows 7 Profissional"** e o tipo de configuração de rede "workgroup" como mostra a Figura10.

Figura 8 - Teste 2 com NMAP no cenário 1

```
Starting Nmap 6.00 ( http://nmap.org ) at 2015-05-02 12:40 BRT
Nmap scan report for 192.168.0.3
Host is up (0.011s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: E0:06:E6:71:7B:9E (Unknown)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 or Windows Server 2008 SP1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENTE_TCC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00
:27:18:58:88 (Cadmus Computer Systems)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: <blank>
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   NetBIOS computer name: CLIENTE_TCC
|   Workgroup: WORKGROUP
|_  System time: 2015-05-02 12:59:51 UTC-3

TRACEROUTE
HOP RTT       ADDRESS
1   11.12 ms 192.168.0.3

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 246.00 seconds
```

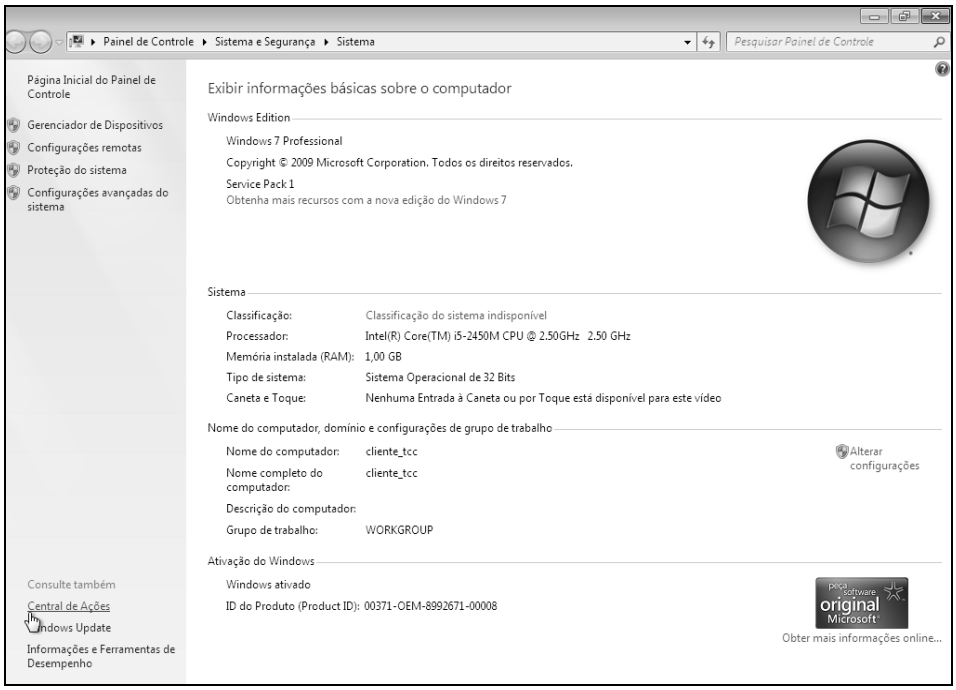
Fonte: Próprio Autor (2015)

Figura 9 - Detalhes da configuração da placa de rede do cliente



Fonte: Próprio Autor (2015)

Figura 10 - Configurações do *host*



Fonte: Próprio Autor (2015)

Com todas as informações obtidas, utilizando o NMAP, um atacante já possui informações suficientes para iniciar seus ataques, faltando apenas descobrir vulnerabilidades sobre as portas abertas.

4.1.2 Testes usando a ferramenta Nessus aplicados ao cenário 1

Com o primeiro teste realizado utilizando o Nessus no cenário 1, que esta representado na Figura 11. Pode-se observar algumas coisas importantes. Esta figura mostra o relatório que foi possível obter após a finalização do primeiro teste usando este *software* aplicado no cenário1.

No primeiro teste, realizado com o Nessus, detectou-se um total de 21 vulnerabilidades, sendo uma considerada critica, uma média e dezenove informativas. A vulnerabilidade critica detectada está na resolução do serviço de DNS no *host* alvo, que pode permitir a execução remota de código.

Já a vulnerabilidade média é sobre a Assinatura SMB Obrigatória O Serviço SMB esta relacionado ao Servidor Samba que é um serviço criado especificamente para compartilhamento de arquivos.

Figura 11 - Resultado do primeiro teste usando Nessus

192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
1	0	1	0	19	21

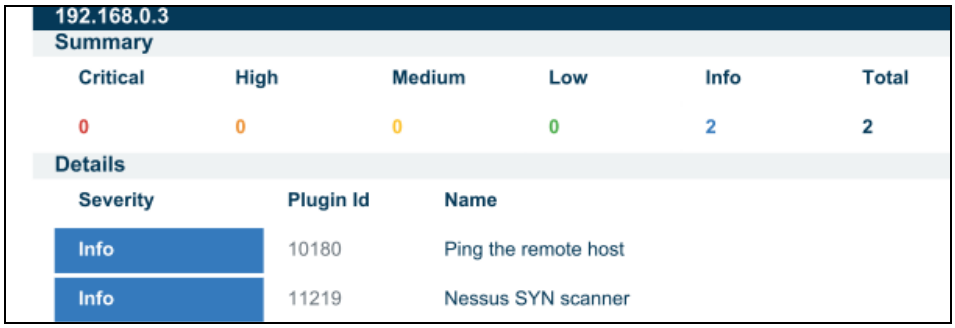
Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (5.0)	57608	SMB Signing Required
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	22964	Service Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Fonte: Próprio Autor (2015)

Com o segundo teste realizado, pode-se detectar algumas outras informações como mostra a Figura 12.

Figura 12- Resultado do segundo teste usando Nessus no cenário 1



192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	10180	Ping the remote host
Info	11219	Nessus SYN scanner

Fonte: Próprio Autor (2015)

Neste cenário percebe-se somente 2 vulnerabilidades, que são consideradas informativas. A primeira vulnerabilidade é a “ping *host* remoto”, ela mostra que o *host* está online na rede durante a execução do teste, ou seja, não é considerada uma falha, apenas uma demonstração de que o *host* está respondendo aos testes de comando *ping*. A segunda vulnerabilidade é “*Scanner* Nessus SYN”, que indica as portas abertas no protocolo TCP e que podem acarretar falhas, invasões e vulnerabilidades. Para corrigir esta falha, torna-se necessário acrescentar um filtro IP, como, por exemplo, um f*irewall*.

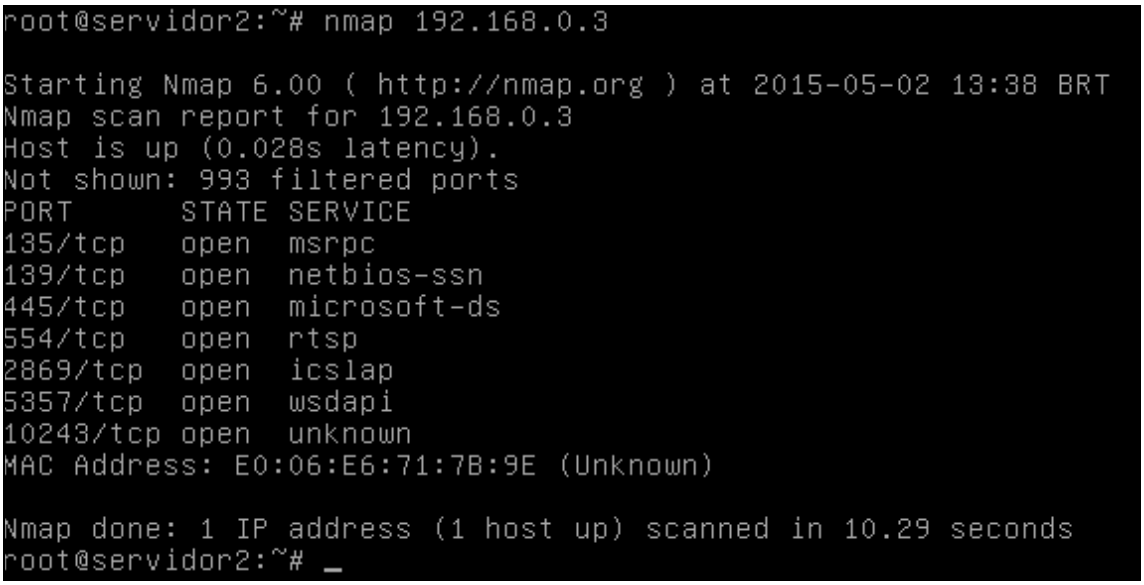
4.2 CENÁRIO 2

O Cenário 2 possui algumas melhorias no quesito de SI, mais ainda está bem longe de estar seguro. O uso do *firewall* ajuda a melhorar a segurança, mas, sozinho ele não consegue resolver muitas falhas. Para melhorar a Segurança neste *host* é necessário ter um antivírus bem configurado e atualizado, juntamente com o SO do *host* estando com as atualizações automáticas ativas.

4.2.1 Testes usando a ferramenta NMAP aplicada ao cenário 2

Com o primeiro teste do NMAP, podem-se observar algumas informações importantes como pode ser observado na Figura 13.

Figura 13 - Teste 1 com NMAP no cenário 2



Fonte: Próprio Autor (2015)

Percebe-se que nesse teste, permaneceram-se as mesmas 5 portas abertas que no cenário 1, porém agora se tem somente uma porta desconhecida. Outro fator que permanece inalterado é o endereço mac-address, já que para este teste esta sendo utilizada a mesma máquina.

Na Figura 14 representa os resultados obtidos no segundo teste usando NMAP. Como se pôde observar, as portas detectadas neste teste da Figura 14 foram às mesmas que apareceram no teste anterior, exceto a porta 10243.

Figura 14 - Teste 2 com NMAP no cenário 2

```
root@servidor2:~# nmap -A 192.168.0.3

Starting Nmap 6.00 ( http://nmap.org ) at 2015-05-02 13:46 BRT
Nmap scan report for 192.168.0.3
Host is up (0.010s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
MAC Address: E0:06:E6:71:7B:9E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cp
e:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Wind
ows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENTE_TCC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00
:27:18:58:88 (Cadmus Computer Systems)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: <blank>
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   NetBIOS computer name: CLIENTE_TCC
|   Workgroup: WORKGROUP
|_  System time: 2015-05-02 13:46:10 UTC-3
```

Fonte: Próprio Autor (2015)

4.2.2 Testes usando a ferramenta Nessus aplicados ao cenário 2

Em relação ao teste realizado com o Nessus, detectou-se algumas informações, em sua maioria coincidentes com o teste anterior como mostra a Figura15. Neste teste, detectou-se 20 vulnerabilidades, sendo consideradas uma de nível de critica, uma de nível médio e dezoito informativas.

Figura 15 - Resultado do primeiro teste usando Nessus

192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
1	0	1	0	18	20

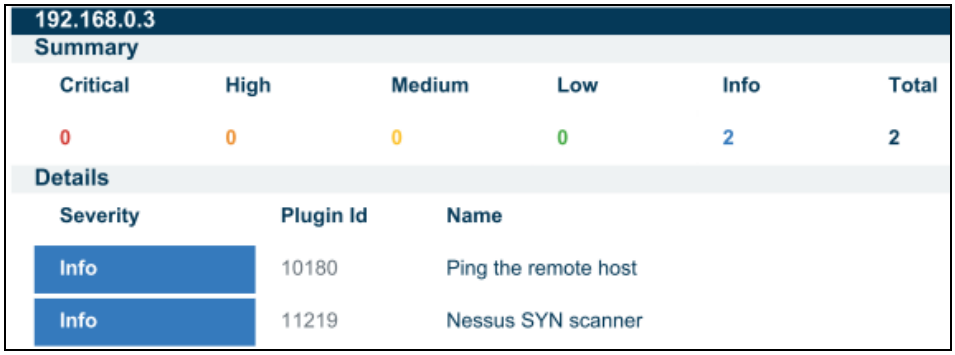
Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (5.0)	57608	SMB Signing Required
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	22964	Service Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Fonte: Próprio Autor (2015)

O resultado do teste 2 com o Nessus pode ser observado na Figura 16, apresenta de maneira igual ao cenário 1.

Figura 16 - Resultado do segundo teste usando Nessus



192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	10180	Ping the remote host
Info	11219	Nessus SYN scanner

Fonte: Próprio Autor (2015)

4.3 CENÁRIO 3

O cenário 3 é aparentemente o mais seguro, dentre todos, que foram abordados no presente trabalho. Ainda não é seguro total, pois o antivírus (Avast) vai funcionar suas atualizações por 30 dias, e após esse período, ele não vai se atualizar mais. Mais o SO não esta totalmente seguro, durante o período que o Avast vai estar se atualizando, porque, o Windows Update (ferramenta do Windows que mantém atualizado o SO) está desativado.

4.3.1 Testes usando a ferramenta NMAP aplicada ao cenário 3

Com os testes do NMAP sobre esse cenário, observou-se alguns resultados importantes como pode ser observado na Figura17, que refere-se ao teste ,1 usando o *software* NMAP Nesta figura é possível observar que, foram detectadas 7 portas abertas, sendo 6 portas com serviços identificados, e 1 porta que o serviço não foi detectado.

Já a Figura 18, mostra os resultados que foram possíveis coletar após o segundo teste, outras informações puderam ser detectadas, a Figura 18. Como se pôde observar, os resultados são os mesmos do cenário 1. O SO do cliente é um Windows 7 *Professional*. O primeiro endereço mac representa o *host* em que está instalado a máquina virtual cliente. Já o segundo é do computador cliente.

Figura 17 - Teste 1 com NMAP no cenário 3

```
root@servidor2:~# nmap 192.168.0.3

Starting Nmap 6.00 ( http://nmap.org ) at 2015-05-02 15:10 BRT
Nmap scan report for 192.168.0.3
Host is up (0.012s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: E0:06:E6:71:7B:9E (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
root@servidor2:~# _
```

Fonte: Próprio Autor (2015)

Figura 18 - Teste 2 com NMAP no cenário 3

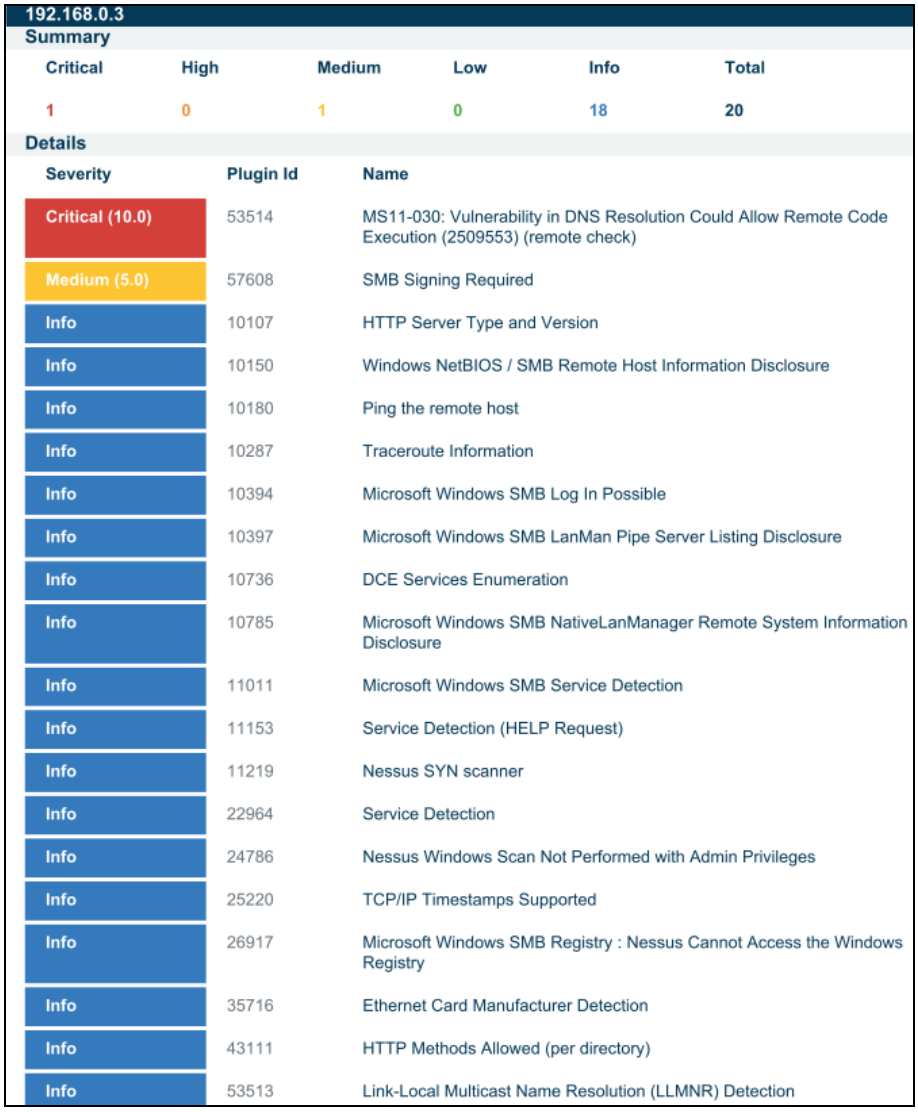
```
root@servidor2:~# nmap -A 192.168.0.3

Starting Nmap 6.00 ( http://nmap.org ) at 2015-05-02 15:17 BRT
Nmap scan report for 192.168.0.3
Host is up (0.0098s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
MAC Address: E0:06:E6:71:7B:9E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server 2
008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENTE_TCC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:18:58:88 (Cadmus Computer Systems)
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   NetBIOS computer name: CLIENTE_TCC
|   Workgroup: WORKGROUP
|_  System time: 2015-05-02 15:16:47 UTC-3
```

Fonte: Próprio Autor (2015)

4.3.2 Testes usando a ferramenta Nessus aplicados ao cenário 3

Nos testes com o Nessus no cenário 3 detectou-se algumas informações. A Figura 19 mostra o que foi possível coletar através do primeiro teste usando o Nessus.

Figura 19 - Resultado do primeiro teste usando Nessus



192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
1	0	1	0	18	20

Details

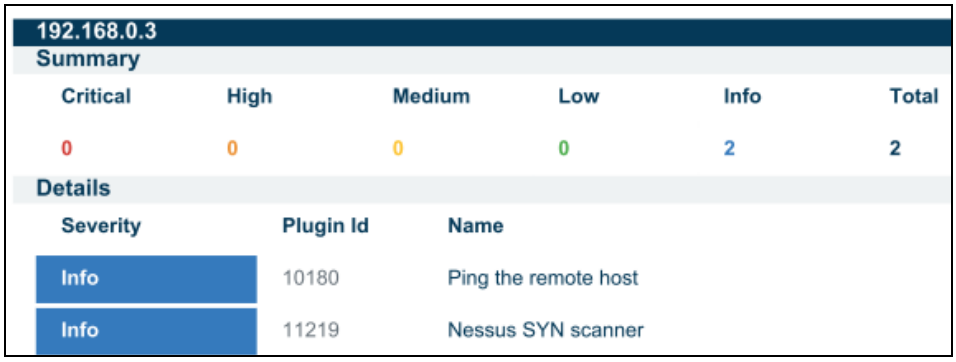
Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Medium (5.0)	57608	SMB Signing Required
Info	10107	HTTP Server Type and Version
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	22964	Service Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Fonte: Próprio Autor (2015)

Neste teste observou-se 20 falhas, sendo uma considerada critica uma média, e dezoito informativas.

O segundo teste retornou informações similares aos testes anteriores realizados nos cenários 1 e 2, como revela a Figura20.

Figura 20 - resultado do segundo teste usando o Nessus



192.168.0.3

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	10180	Ping the remote host
Info	11219	Nessus SYN scanner

Fonte: Próprio Autor (2015)

4.4 COMPARAÇÃO DOS 3 CENÁRIOS APRESENTADOS

Como pode ser observado ao longo do estudo de campo apresentado ao longo deste capitulo. Dentre os 3 cenários apresentados o cenário 1 é o mais critico, o cenário 2 é considerado médio para falhas, e o mais seguro dentre os 3 é o cenário 3 é o que tem menos riscos nos requisitos de SI. Como pode ser observado no primeiro cenário observando os testes com o NMAP foi detectado mais portas abertas, porém muitas destas portas que estão abertas não foram reconhecidas os serviços que nela estão rodando.

Em relação ao Nessus, nos testes em que foram baseados na política Host Discovery (descoberta de *host*) foram encontradas 2 vulnerabilidades consideradas como informações, sendo uma delas resposta ao comando ping, e escaneamento usando a flag SYN que com ele o Nessus revela as portas TCP que estão abertas. Já em relação a política *Basic Network Scan* (política de escaneamento básico na rede) os resultados são mais densos, pois está é uma política que realiza testes mais profundos. No cenário 1 foi detectado foi detectado mais vulnerabilidades sendo no total de 21, 1 crítica ,1 média e 19 de informativas. No cenário 2 e 3 foi detectado no total de 18 vulnerabilidades, sendo consideradas 1 média, 1 critica e 18 informativas.

5 CONSIDERAÇÕES FINAIS

Com o atual aumento de informações dispostas em formatos digitais, tornou-se necessário buscar meios de protegê-los, criando-se assim uma área especifica, com a função de proteger a informação de pessoas e sistemas maliciosos. Nomeou-se essa área com Segurança da Informação, comumente conhecida como SI.

Porém, mesmo com a criação dessa área, torna-se necessário seguir algumas salvaguardas, sendo estas baseadas nos pilares que sustentam a própria área, baseando-se, principalmente na Integridade, Confidencialidade, Disponibilidade e Auditabilidade. Todos esses pilares, caso assegurados na proteção das informações, possuem altas chances de mantê-las em segurança, já que não se consegue garantir a plena segurança.

Em relação ao objetivo principal deste trabalho, foram abordados os 2 *softwares* (Nessus e NMAP), aplicando no estudo de campo, onde foram feito 2 testes com ambos programas em 3 cenários. Conclui-se que com o uso dessas ferramentas, que em ambientes de redes ou um *host* possui vulnerabilidades, onde as mesmas poderão torná-lo um alvo fácil para atacantes que conheçam as vulnerabilidades do mesmo. Isso acontece porque mesmo as pequenas vulnerabilidades podem se tornar uma grande falha, que, caso não tratada a tempo, poderá se transformar em um incidente, que pode ser inofensivo ou, no pior cenário, gerar danos irreversíveis e irreparáveis.

Caso essas vulnerabilidades não venham a ser tratadas a tempo, os problemas gerados por ela serão muito grandes, principalmente se o atacante as souber explorar. Podendo deixar sistemas parcialmente ou até totalmente fora do ar. Por este motivo torna-se necessário sempre efetuar o uso de ferramentas que ajudem a proteger a informação, sendo o Nessus e o NMAP fortemente indicados para essa tarefa.

Como sugestões para trabalhos futuros estão uma análise detalhada dos relatórios gerados em cima destes cenários, configurar o serviço de auditoria e de relatório via *e-mail,* sms*,* no Nessus. Também com sugestão pra trabalhos futuros está a exploração das famílias de *plugins* do Nessus, fazer outros testes tanto no NMAP, quanto no Nessus, efetuar um aumento no número de cenários, dentre outros tipos de mudanças

REFERÊNCIAS BIBLIOGRÁFICAS

ADOBE. Acrobat. **Sobre o Adobe PDF: O que é PDF?.** Disponível em: <https://acrobat.adobe.com/br/pt/products/about-adobe-pdf.html> . Acesso em: 25 abr. 2015.

AVAST. **Avast Internet Security.** Disponível em: <https://www.avast.com/pt-br/internet-security>.Acesso em: 28 jun. 2015.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 2.ed. Brasília, 2007.

CERT.BR. Comitê Gestor de Internet no Brasil: **Cartilha de segurança da Informação para Internet**. 2 ed. São Paulo, 2012.

_____.Centro de Estudos e tratamento de Incidentes de Segurança no Brasil. **Incidentes Reportados ao CERT.br – janeiro a dezembro de 2013**: Análise de alguns fatos de interesse observados nesse período. 2014. Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-dec/analise.html>. Acesso em: 29 mar. 2015.

FONTES, Edison **Segurança da Informação**: O usuário faz a diferença. 1.ed. São Paulo:Saraiva,2006.

._____ **Gestão de Risco em Segurança da Informação**. Disponível em: <http://imasters.com.br/artigo/16323/seguranca/gestao-de-riscos-em-seguranca-da-informacao/>. Acesso em: 16 mar. 2015

FOROUZAN, Bhrouz A. **Comunicação de dados e rede de computadores.** 4.ed. São Paulo: McGraw-Hill,2008.

GENNARI, Maria Cristina. **Minidicionário Saraiva Informática.** 5. Ed. São Paulo,2003

GONÇALVES, Sérgio Ricardo M. **Hackers, crackers, spammers**: quem são e o que fazem? Mundo jurídico, 2005. Disponível em: <http://www.mundojuridico .adv.br/sis_artigos/artigos.asp?codigo=659>. Acesso em: 18 set. 2001.

INFORMABR. **Segurança da Informação:** Processo de Conexão e ACK. Disponível em: <http://www.informabr.com.br/tcpconexao.htm>. Acesso em: 28 mar. 2015.

IPV6.BR.A nova geração do Protocolo Internet.**Endereçamento IPv6.** Disponível em: <http://ipv6.br/enderecamento-ipv6/>. Acesso em: 13 abr. 15
IPV6.BR.A nova geração do Protocolo Internet.**Endereçamento.** Disponível em: <http://ipv6.br/entenda/ enderecamento/>. Acesso em: 22 mar. 2015.

Java. Onde posso obter mais informações técnicas sobre o Java?: **Qual a diferença entre o JRE e o JDK?** Disponível em: <https://www.java.com/pt_BR /download/faq/techinfo.xml> . Acesso em: 22.abr. 2015.

Kali Linux. Official Documentation. **O que é o Kali Linux**. Disponível em: <http://br.docs.kali.org/introduction-pt-br/o-que-e-o-kali-linux >. Acesso em: 10 abr. 15

MARTINS, Elaine. **O que é SSL?** Disponível em: <http://www.tecmundo.com .br/seguranca/1896-o-que-e-ssl-.htm>. Acesso em: 13 mai. 2015

_____. **O que é cracker?** Disponível em: <http://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acesso em: 17 mar. 2015.

MICROSOFT. **Protocolo ARP (Address Resolution Protocol).** Disponível em: <https://technet.microsoft.com/ptbr/library/cc758357%28v=ws.10%29 . aspx?f=255&MSPPError=-2147217396>. Acesso em: 18 mai. 2015.

_____. **Protocolo de mensagens de controle da Internet (ICMP).** Disponível em: <https://technet.microsoft.com/pt-br/library/cc758065%28v=ws.10%29 . aspx>. Acesso em: 18 mai. 2015

_____ **Roteamento IP**. Disponível em: <https://technet.microsoft.com/pt-br/library/cc785246% 28v=ws.10%29.aspx>. Acesso em: 8 abr. 15.

_____.**Usando o Protocolo RTSP.** Disponível em: <https://technet.microsoft . com/pt-br/library/cc770781(v=ws.10).aspx>. Acesso em: 3. mai. 2015

MORIMOTO, Carlos E.**IPV4.** Disponível em: http://www.hardware.com.br /termos/ipv4 Acesso em: 22 mar. 2015.

_____. **Significado de siglas.** Disponível em: <http://www.hardware.com. br/artigos/significado-siglas/> Acesso em: 25 abr.2015

MORIMOTO. **Usando o Nessus.** Disponível em: <http://www.hardware.com.br / livros/redes/usando-nessus.html>. Acesso em: 5 abr. 2015.

_____. **Configurando a rede no VirtualBox.** Disponível em: <http://www.hardware.com.br/dicas/rede-virtualbox.html > Acesso em: 17 abr. 2015.

MULLER.Leornado. **O que é Phishing?** Disponível em: < http://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm> Acesso em: 17 fev. 2015

NMAP.BR. Guia de Referência do NMAP (Página do Manual). Disponível em: <http://nmap.org/man/pt_BR/index.html#man-description>. Acesso em: 6 abr. 2015.

PEIXOTO, Mario César Pintaudi.**Engenharia Social e Segurança da Informação na Gestão Corporativa**. 1. ed. Rio de Janeiro: Brasport, 2006.

RASMUSSEN,Bruna.**O que é o protocolo TCP/IP?** Disponível em: <http://canaltech.com.br/o-que-e/o-que-e/O-que-e-o-protocolo-TCPIP/>. Acesso em: 22 mar. 2015.

STTALLINGS, William. **Criptografia e Segurança de Redes**. 4. ed. São Paulo: Pearson, 2008.

SYMANTEC. Norton by Symantec: **Glossário.** Disponível em: <http://br.norton.com/security_response/glossary/define.jsp?letter=n&word=netbios-network-basic-input-output-system>. Acesso em: 3 mai. 2015.

TANEBAUM, Andrew S. **Rede de Computadores.**4.ed. Rio de Janeiro:Campus,2003.

TENABLE. Network security. **Guia de instalação e configuração do Nessus 5.2.** 2014. Disponível em: <http://www.tenable.com/products/nessus/documentation#portuguese>. Acesso em: 5 abr. 2015.

TORRES, Gabriel.**O modelo de Referência OSI para Protocolos de Rede.** Disponível em: <http://www.clubedohardware.com.br/artigos/O-Modelo-de-Referencia-OSI-para-Protocolos-de-Rede/1349/1>. Acesso em: 22 mar. 2015.

Vlaswinkel, Koen. Digital Ocean. **How To install Java on Ubuntu with Apt-Get.** Disponível em: <https://www.digitalocean.com/community/tutorials/how-to-install-java-on-ubuntu-with-apt-get>. Acesso em: 22.abr. 2015.

Apêndice A – NMAP

Instalação do NMAP

Para instalar o NMAP é necessário que algumas coisas sejam previamente observadas. Em primeiro lugar é preciso verificar se servidor possui acesso a Internet, para de este modo ser possível fazer o *download* dos pacotes que serão necessários para sua instalação. Uma das maneiras para verificar se há Internet no servidor, é digitar o comando *ping* junto com algum site, aguardar um tempo e pressionar "**Ctrl+c"**, e observar se perdeu todos os pacotes; caso perdeu muito ou todos os pacotes o *host* não está com Internet. Para digitar os comandos de instalação, e os comandos para executar os escaneamentos é preciso estar usando o usuário *root* no Debian. Após a confirmação, é necessário digitar alguns comandos para conseguir efetuar as operações desejadas. O primeiro comando a ser digitado é o **"apt-get install nmap"** como pode ser observado na Figura 21.

Figura 21 – Comando de instalação do NMAP

Fonte: Próprio Autor (2015)

Após este comando será apresentado um resumo das modificações que serão executadas com a instalação do NMAP, como se pode observado na Figura 22. Se o usuário estiver de acordo com as modificações descritas, é necessário que o próprio confirme com a letra **"S**", e as modificações descritas na Figura 22 vai ocorrer. Caso queira-se abortar a instalação, pressione a letra **"N"** para cancelar o processo de instalação. Se a tecla **"S"** for usada, serão feitas as modificações que já foram descritas anteriormente.

Após a instalação, o terminal de comando vai esperar a próxima ação do usuário, que poderá ser o uso do NMAP ou alguma outra operação com o SO.

Figura 22 - Confirmação da Instalação do NMAP

Fonte: Próprio Autor (2015)

Como já dito, o NMAP é uma ferramenta de linha de comando responsável por realizar escaneamentos na rede. Para cada tipo de escaneamento é usado uma combinação de *flags*. Para NMAP.org[s.d.] o comando do nmap tem a seguinte estrutura: **"nmap [*<Tipo de Scan>* ...] [*<Opções>*] { *<especificação do alvo>* }"**. A especificação do alvo pode ser um endereço IP ou um nome do host. Um exemplo típico do NMAP é o uso do comando nmap seguido por um endereço IP: "nmap 192.168.20.20". Neste exemplo, geralmente virá como resultado a quantidade de portas abertas e o número do m*ac-adrress* (endereço físico) da placa de rede. Outro exemplo é usando a *flag* **"–A".** O uso desta flag "[...] habilita a detecção de SO e a versão, [...]"(.NMAP.org [s.d.])

Apêndice B – Java

Instalação do Java

Para a instalação do Java, tornam-se necessárias algumas garantias, dentre elas a verificação da existência de Internet no *host* em que será instalado, para poder efetuar o *download* e a atualização dos pacotes do Debian. Outro requisito necessário é estar utilizando o usuário administrador (*root*).

O primeiro passo a ser efetuado depois das garantias tomadas é a verificação da existência do Java na máquina. “para verificar se o Java está instalado digite no terminal o comando **“java –version”**”. (DIGITAL OCEAN 2014). Caso o resultado retorne não encontrado, como mostra a Figura 23, o Java não está instalado.

Figura 23 - Verificação se o Java está instalado

Fonte: Próprio Autor (2015)

O uso do Java, no atual estudo de campo, não é obrigatório, mas para mais segurança e confiabilidade nos relatórios do Nessus seu uso foi adotado.

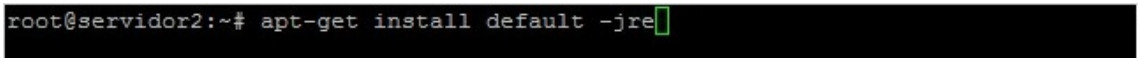
A instalação do Java é feita por módulos. Para o Nessus gerar os relatórios, em PDF, são necessário dois módulos, o JRE (Java *Runtime Environment*)[11] e o JDK (Java *Development Kit*)[12]. Para a instalação do JRE é usado o comando **“apt-get install default -jre”**, como mostra a Figura 24.

Com a conclusão da instalação pode-se verificar a atualização de pacotes, juntamente com os novos pacotes instalados por meio de *downloads* para a instalação do JRE, como mostra a Figura 25.

11 JRE(Java Runtime Environment): “É uma implementação do Java Virtual Machine* que na verdade executa programas Java.”. (JAVA.COM[s.d.])

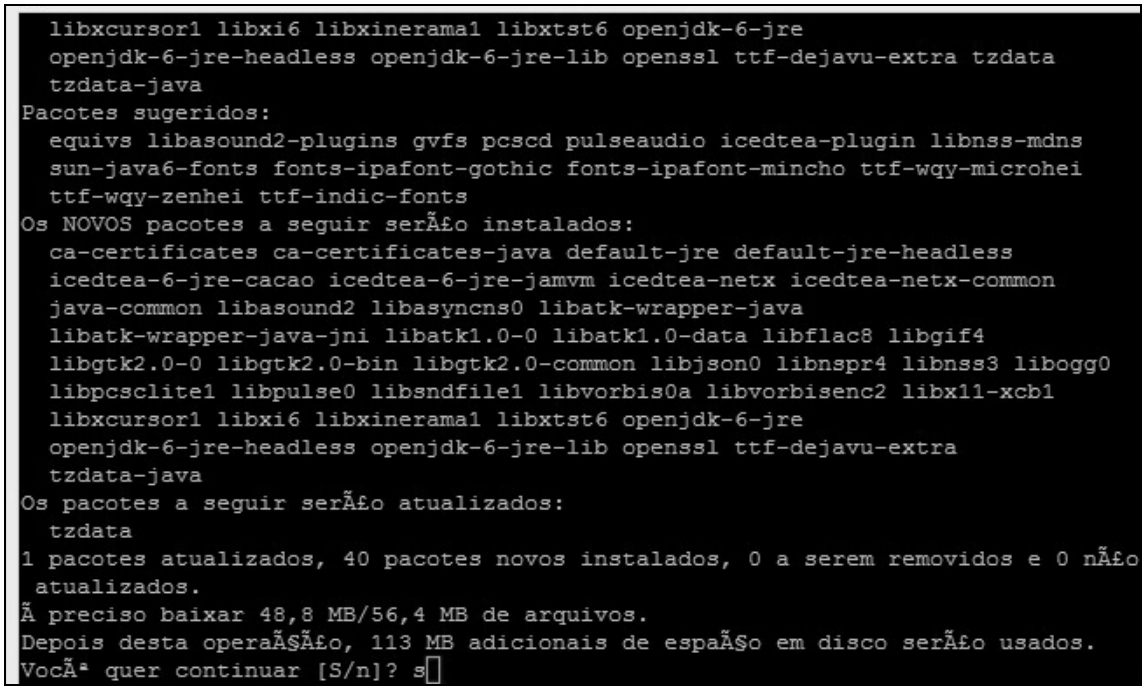
12 JDK (Java Development Kit): “É um pacote de software que você pode usar para desenvolver aplicativos baseados em Java”. (JAVA.COM [S.D]).

Figura 24 - Instalação do Módulo JRE



Fonte: Próprio Autor (2015)

Figura 25 – Confirmação da instalação do módulo JRE



Fonte: Próprio Autor (2015)

Após a confirmação da atualização dos pacotes a serem obtidos e do processo de instalação deste módulo ter sido concluído, é feita a instalação do segundo módulo, por meio do comando **"apt-get install default –jdk"**, como mostra a Figura 26.

Figura 26 – Instalação do Módulo JDK

Fonte: Próprio Autor (2015)

Após a confirmação da instalação dos pacotes a serem instalados, o processo de instalação é concluído, como mostra a Figura 27 representa.

Figura 27 – Confirmação da instalação do módulo JDK

Fonte: Próprio Autor (2015)

Para verificar se o Java está instalado pode-se usar o comando **"Java –version"**, se o resultado retornar a versão do Java, semelhante a Figura 28, o Java irá funcionar corretamente no Nessus.

Figura 28 – Confirmação da Instalação do Java

Fonte: Próprio Autor (2015)

Apêndice C – Nessus

Instalação, Criação de políticas, escaneamentos, e exportação dos relatórios no Nessus

Para a instalação do Nessus, é necessário atentar-se a alguns cuidados, sendo: o primeiro a verificação da existência de acesso a Internet no *host;* o segundo o uso do usuário administrador (*root*); e o terceiro o uso de um navegador web para a utilização e configuração do serviço. Para este cenário de estudo, fez-se o uso do navegador Firefox, da empresa Mozilla.

Para a instalação, faz-se, primeiramente, o *download*[13] do Nessus no site da fabricante, do Nessus (Tenable), localizando a versão que coincida com a arquitetura do computador ao qual ela será instalada (32 ou 64 bits) e com o sistema operacional utilizado por ela, principalmente quando o sistema é baseado em Linux, devido a existência de diferentes versões. Para este cenário foi feito o uso do "Nessus Home" versão 6.3.4, compatível com arquitetura 32 bits e sistema operacional, baseado em Linux, "Debian 6 ou 7".

Concluindo-se o *download* dos arquivos é feita a instalação. Para este cenário de estudo, optou-se por utilizar o diretório "/nessus".

Instalação

Para a instalação, torna-se necessário, em primeiro lugar, localizar os arquivos de instalação. Para localizá-los, utiliza-se o comando **"ls-l"**, como mostra a Figura 29.

13 Página de download: http://www.tenable.com/products/nessus/select-your-operating-system

Figura 29 - Resultado do comando ls-l

Fonte: Próprio Autor (2015)

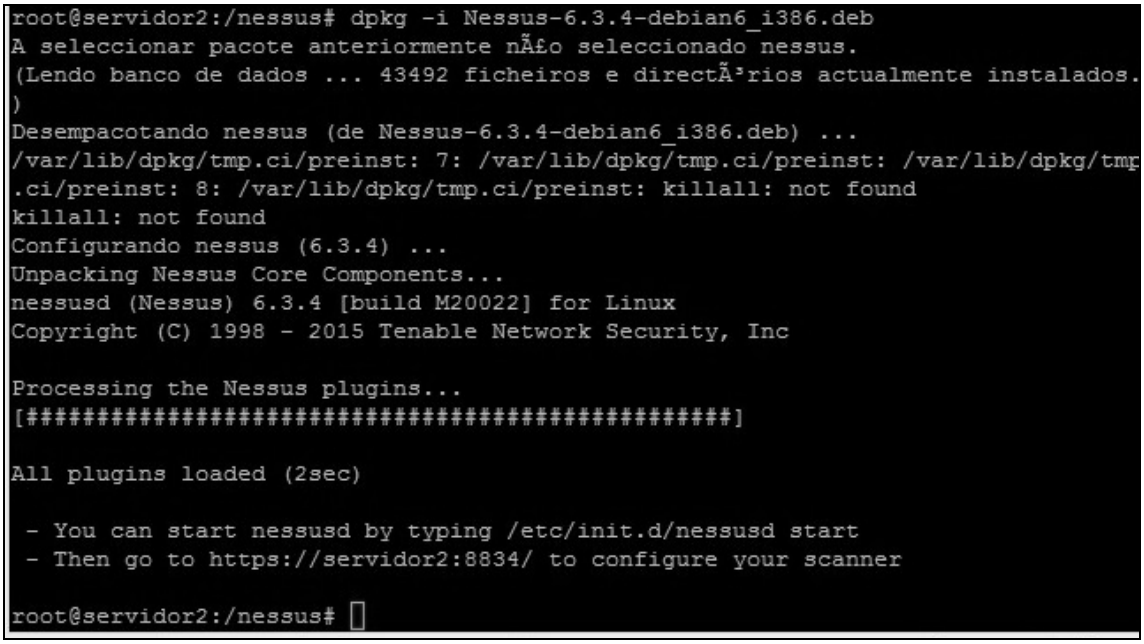
Após a verificação da localidade dos arquivos, efetua-se a instalação, utilizando o comando "**dpkg –i +** ***nome do arquivo***", como demonstra a Figura 30.

Figura 30 - Comando para instalar o Nessus

Fonte: Próprio Autor (2015)

Após o processo de instalação ter sido concluído, alguns detalhes irão aparecer na tela como a Figura 31 mostra.

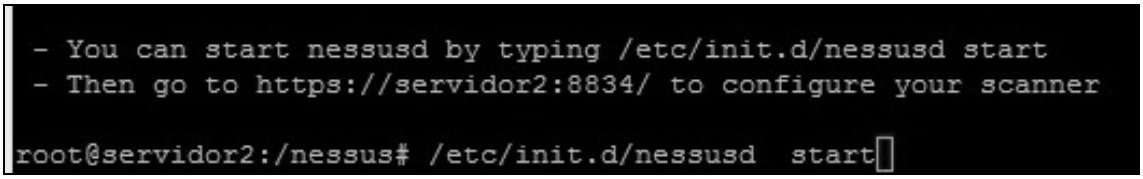
Figura 31 - Resultado do comando de instalação do Nessus



Fonte: Próprio Autor (2015)

Para a inicialização do Nessus, torna-se necessário utilizar o comando **“/etc/init.d/nessusd start”** como mostra a Figura 32.

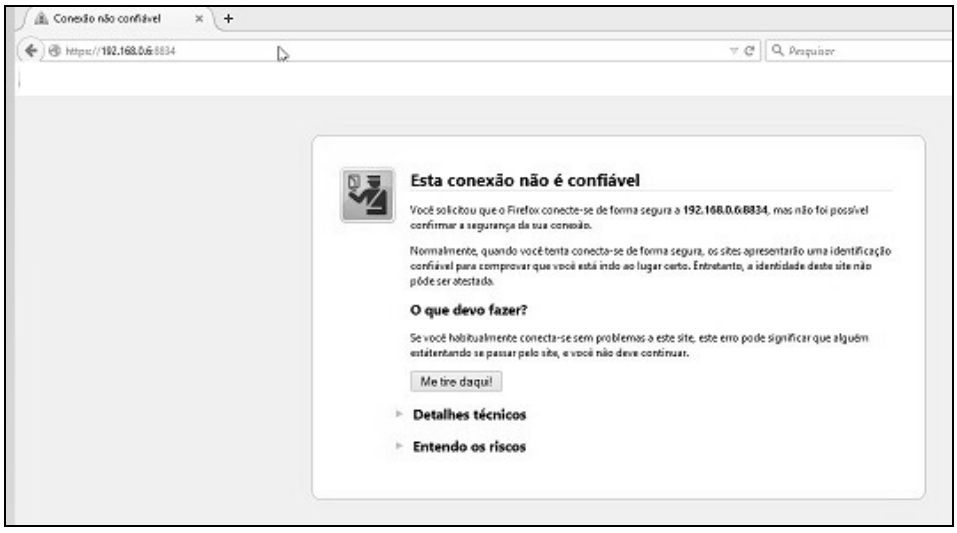
Figura 32 - Uso do comando para inicializar o serviço do Nessus



Fonte: Próprio Autor (2015)

O próximo passo da instalação necessita de um navegador para acessar o Nessus. Em sua barra de endereço, digita-se **“https://nome do servidor:8834”** ou **“https://endereço IP do servidor:8834”** para, deste modo, o servidor ser acessado o serviço do Nessus. Para o estudo de campo as opções são: **“https://servidor2:8834”** ou **“https://192.168.0.6:8834”** , como mostra a Figura 33.

Figura 33 - Primeira tela para acesso do Nessus pelo navegador

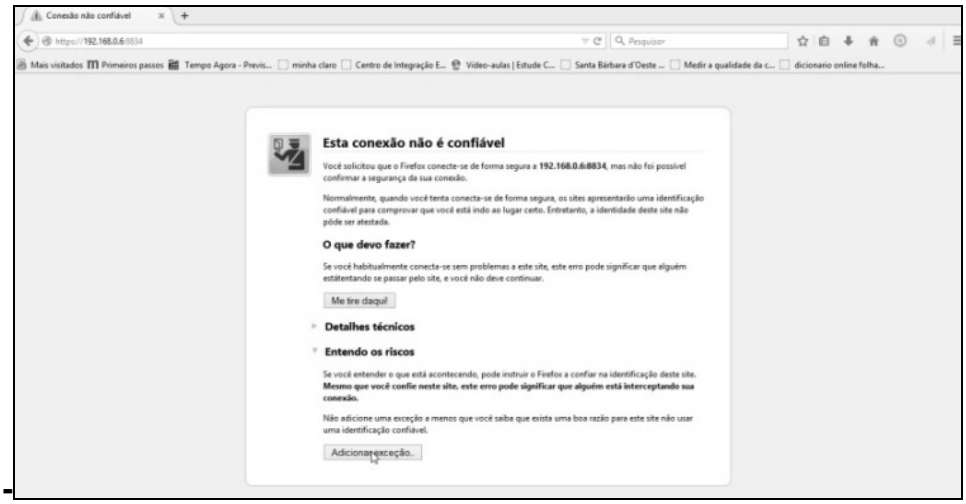


Fonte: Próprio Autor (2015)

Com o processo de acesso concluído, torna-se necessário seguir algumas outras etapas. O sistema exibirá uma mensagem de falta de certificado

SSL[14] (HTTPS[15]), já que o servidor trabalha com esse tipo de certificado. Para a resolução desse problema, torna-se necessários alguns passos como mostra as Figuras 34 e 35.

Figura 34 - Resolvendo erro de certificado SSL no Nessus



Fonte: Próprio Autor (2015)

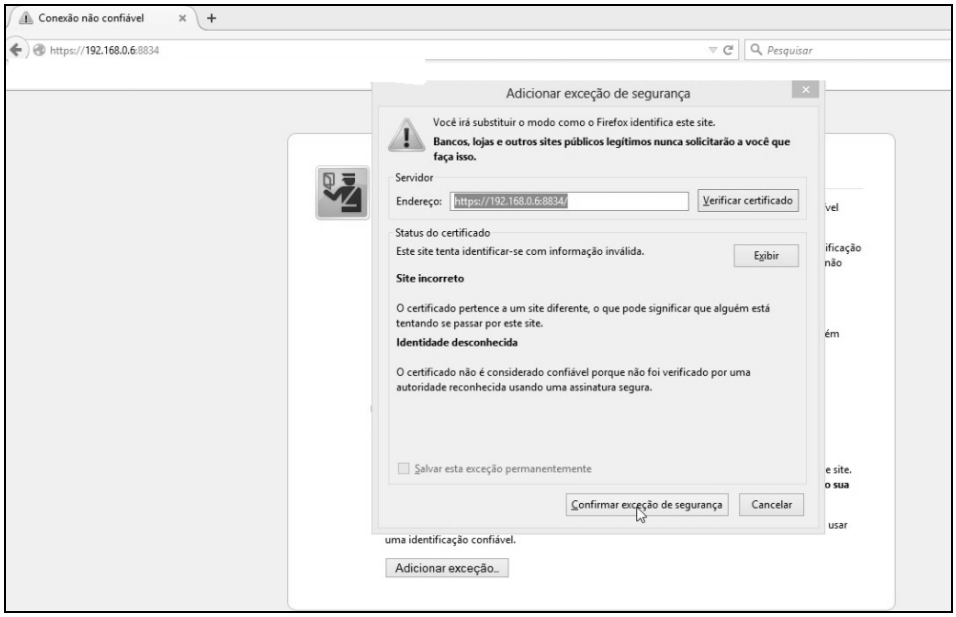
No primeiro passo escolhe-se a opção "Entendo os riscos" e consequentemente **"Adicionar exceção..."**, como pode ser observado na Figura 34. Em seguida será exibida uma nova janela como mostra a Figura 35, onde torna-se necessário confirmas a exceção, clicando no botão **"Confirmar exceção de segurança"** como pode ser visto na Figura 35. Com o processo concluído, a tela de inicialização do Nessus será exibida semelhante à Figura 36 e a mensagem não voltará a aparecer nos próximos acessos ao Nessus, a menos que a exceção seja retirada do navegador ou o nome do *host* servidor, ou endereço IP, mudem.

Na tela de apresentação (boas vindas) do Nessus que está representada na Figura 36, torna-se necessário ler as informações passadas pelo sistema, versão 6 do Nessus, e continuar o processo, selecionando a opção "***Continue***", para, deste modo, iniciar a configuração do Nessus.

14 SSL: "[...] (Secure Socket Layer). Ele permite que aplicativos cliente/ servidor possam trocar informações em total segurança, protegendo a integridade e a veracidade do conteúdo que trafega na Internet." (MARTINS 2009).

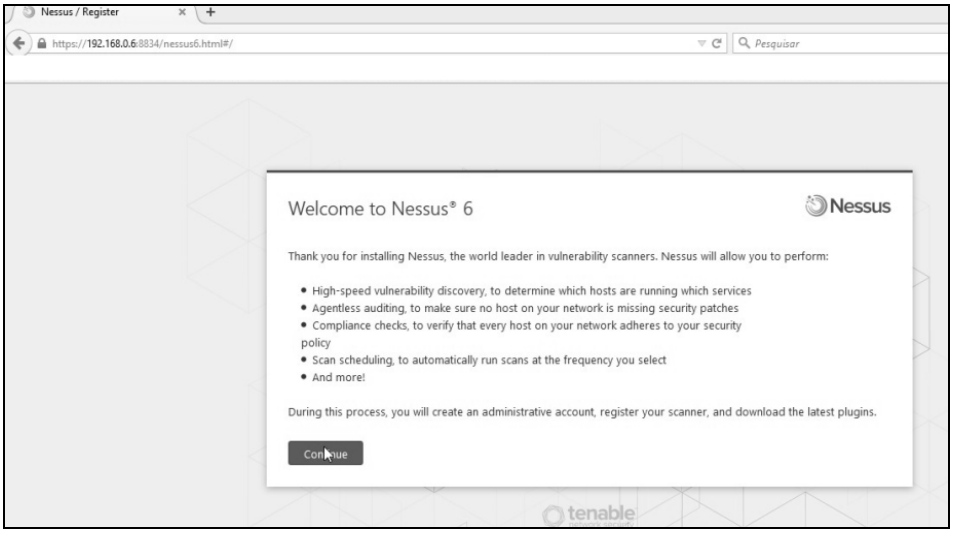
15 HTTPS: é um protocolo da camada de aplicação do modelo ISO/OSI, ou seja, camada 7. Onde este protocolo tem a função de requisitar páginas web utilizando juntamente SSL.

Figura 35 - Solução da mensagem do certificado digital para o Nessus



Fonte: Próprio Autor (2015)

Figura 36 - Tela de boas vindas ao Nessus Versão 6

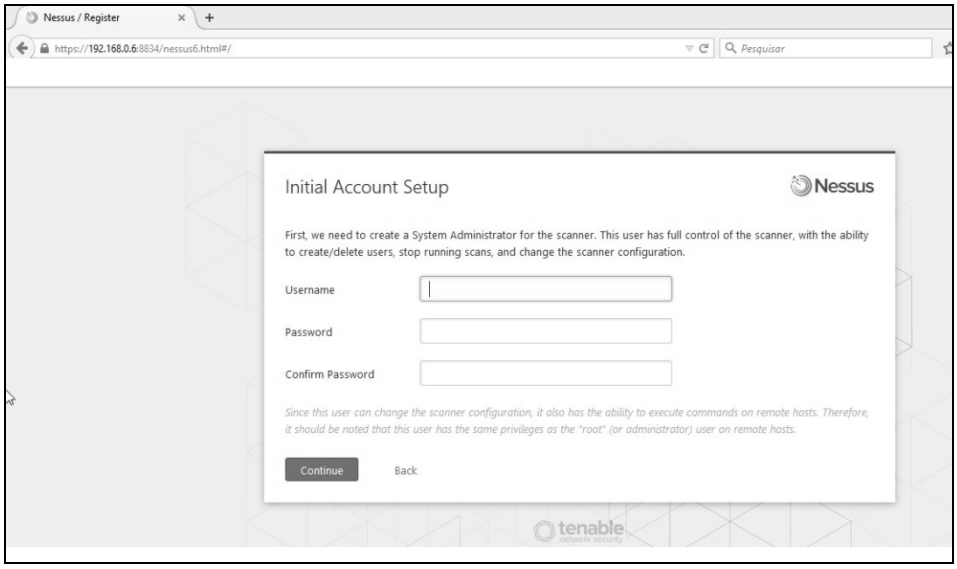


Fonte: Próprio Autor (2015)

Para a continuação do processo de configuração, torna-se necessário a criação de um usuário administrador, que terá todos os direitos, e senha para o uso do Nessus. Na tela de configuração da Figura 37, podem-se observar três caixas de texto para serem preenchidas. A primeira representa o nome de usuário para acessar o serviço, a segunda a senha e a terceira a confirmação da senha,

que deve ser idêntica a anterior. Com o preenchimento desses campos, deve-se clicar no botão **"*Continue*"**.

Figura 37 - Configuração do nome e senha para o primeiro usuário



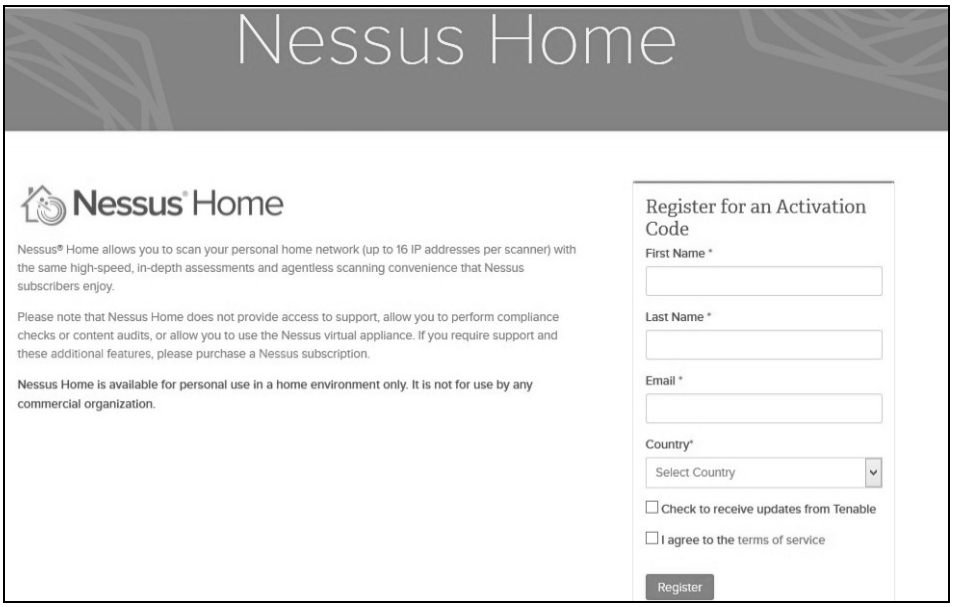
Fonte: Próprio Autor (2015)

Em seguida, o processo de configuração, pedirá o código de registro do software. Este código estará no *e-mail* colocado no ato do pedido. Para efetuar o pedido, torna-se necessário entrar no site do fabricante[16] e efetuar o preenchimento do formulário que está representado na Figura 38. No formulário será necessário informar, no primeiro campo, o primeiro nome do usuário; no segundo campo, o último sobrenome do usuário; no terceiro, o *e-mail* para qual o código será enviado; e no quarto, deve-se selecionar o país em que se está. Com os campos preenchidos, torna-se necessário, em seguida, marcar a opção **"*I agree to the terms of service*"**, que concordará com o contrato que possui as regras estipuladas pela Tenable, para o registro do produto e, por fim, clicar no botão "***Register***" para finalizar o processo de envio.

Para prosseguir com o processo de configuração, torna-se necessário buscar o código de registro no *e-mail* cadastrado. O código de ativação é formado por números na base hexadecimal.

16 http://www.tenable.com/products/nessus-home

Figura 38 - Página do Nessus para obter código de ativação



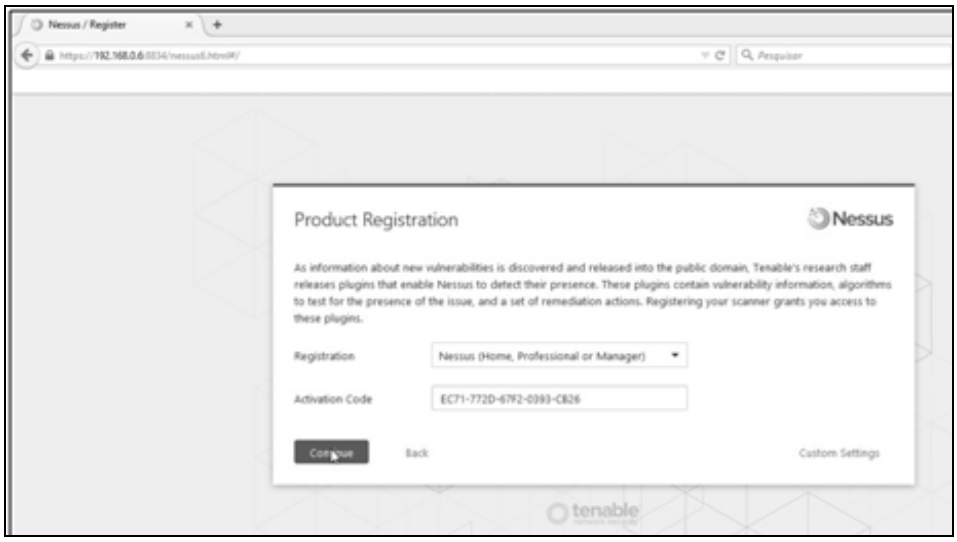
Fonte: Próprio Autor (2015)

Com o código em mãos, o processo de configuração pode ser concluído como mostra a Figura 39, para isso, torna-se necessário escolher a opção de registro no primeiro campo "***Registration***" escolha a versão Nessus, pois na lista terá vários produtos da Tenable. No segundo campo, "***Activation Code***", informa-se o código de ativação, previamente enviado no *e-mail* cadastrado. Com os campos preenchidos, torna-se necessário clicar no botão "***Continue***" da Figura 39.

Com o processo de configuração concluído, a etapa seguinte consiste-se no *download* e atualização dos *plugins* a ser utilizado pelo Nessus e, em seguida, com o processo concluído, o Nessus é inicializado como a Figura 40 mostra.

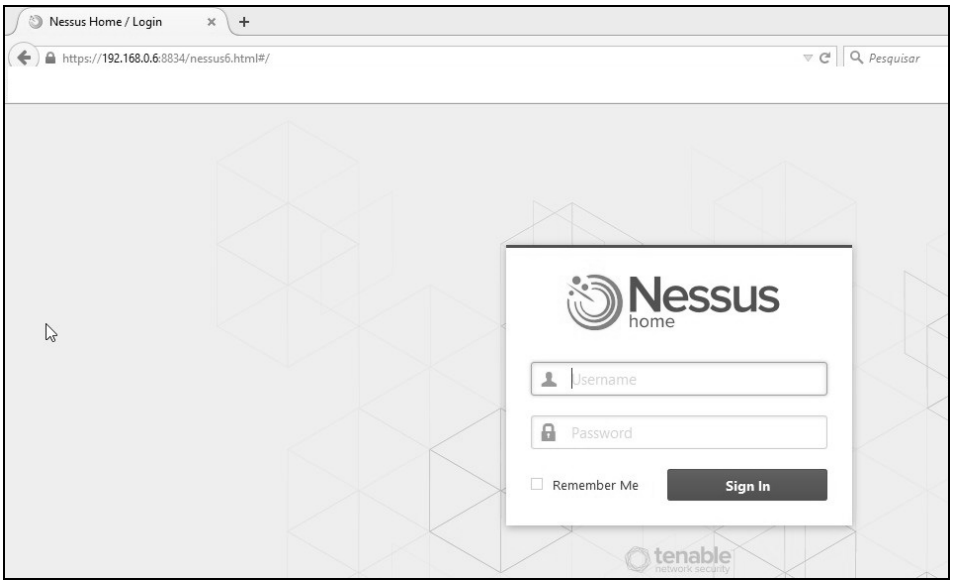
Na Figura 40 é possível perceber que após a inicialização completa do serviço do Nessus, o serviço aguarda o usuário entrar com o *login* que foi cadastrado ao longo do processo da instalação deste serviço.

Figura 39 - Representação da etapa do registro do Nessus



Fonte: Próprio Autor (2015)

Figura 40 - Tela de *login* do Nessus



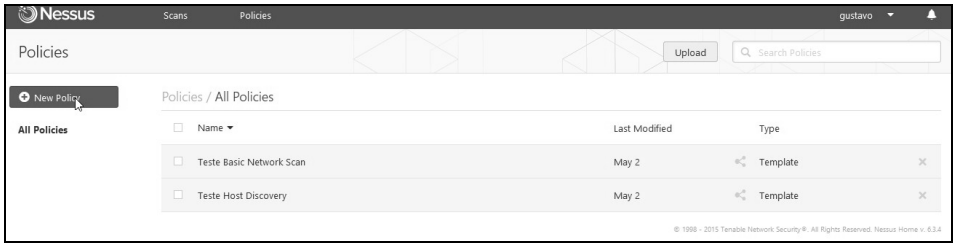
Fonte: Próprio Autor (2015)

Criação das políticas

Os escaneamentos realizados pelo Nessus podem ser feitos a partir de uma política previamente criada, ou de uma política criada no momento da execução do teste. Para este estudo, efetuou-se a escolha de políticas criadas para cada tipo de teste, sendo estas criadas de forma prévia. Para a criação das

políticas necessita-se seguir algumas etapas estipuladas pelo Nessus, a primeira é seguir a Figura 41

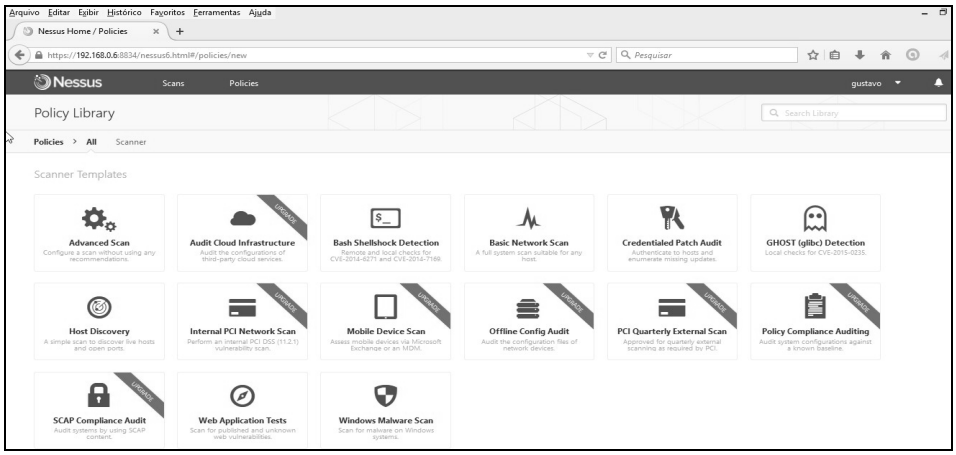
Figura 41 - Início da criação das políticas



Fonte: Próprio Autor (2015)

Inicialmente torna-se necessário escolher a opção "***Polices***" e dentro dela escolher a opção **"*New Police"*** como mostra a Figura 41. Com esta escolha algumas opções de políticas estarão disponíveis para ser configurada, a Figura 42, mostra o tipo de políticas que o Nessus permite criar.

Figura 42 - Tipos de políticas a serem criadas

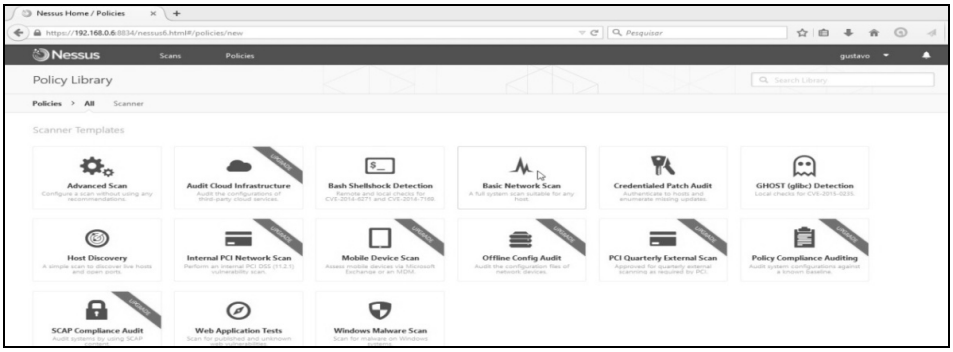


Fonte: Próprio Autor (2015)

Criação da política de escaneamento básico de rede

Para este estudo de campo, utilizou-se políticas específicas, sendo a primeira delas, o escaneamento básico na rede. Para escolher a política torna-se necessário selecionar a opção *Basic Network Scan* como mostra a Figura 43.

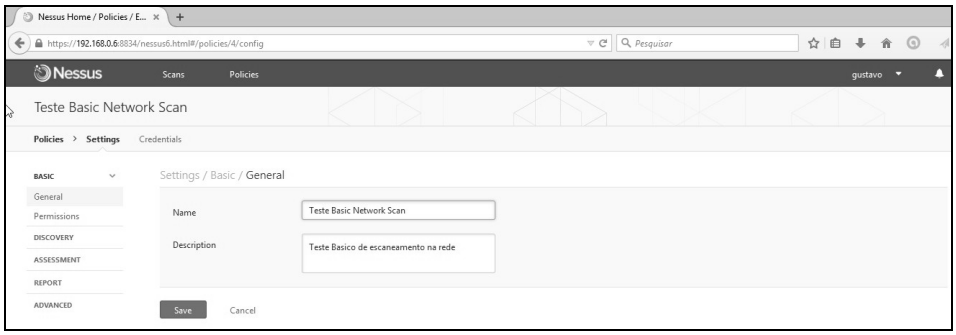
Figura 43 - Escolha da política de escaneamento básico de rede



Fonte: Próprio Autor (2015)

No processo de criação das políticas, torna-se necessário seguir várias etapas de configuração. A primeira etapa é a escolha do nome da política, juntamente com sua descrição, que pode ser vista pós configura na Figura 44.

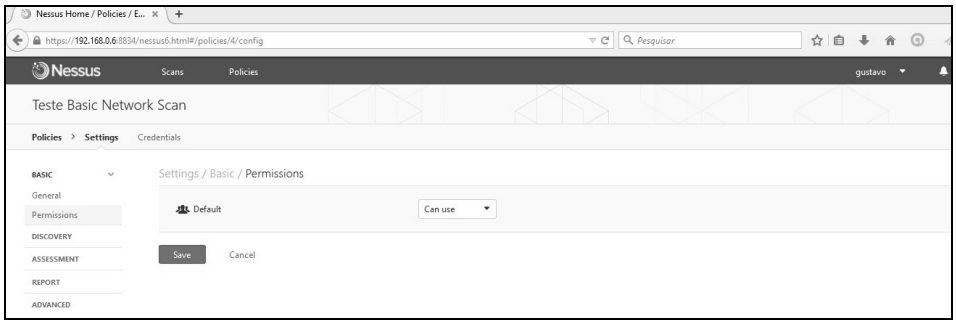
Figura 44 - Etapa 1 da criação da política 1



Fonte: Próprio Autor (2015)

A segunda etapa é o compartilhamento das políticas com outros usuários do sistema, permitindo que os mesmo tenham acesso a essa política. A Figura 45 está com a opção "***Can use"*** indica que a política esta compartilhada.

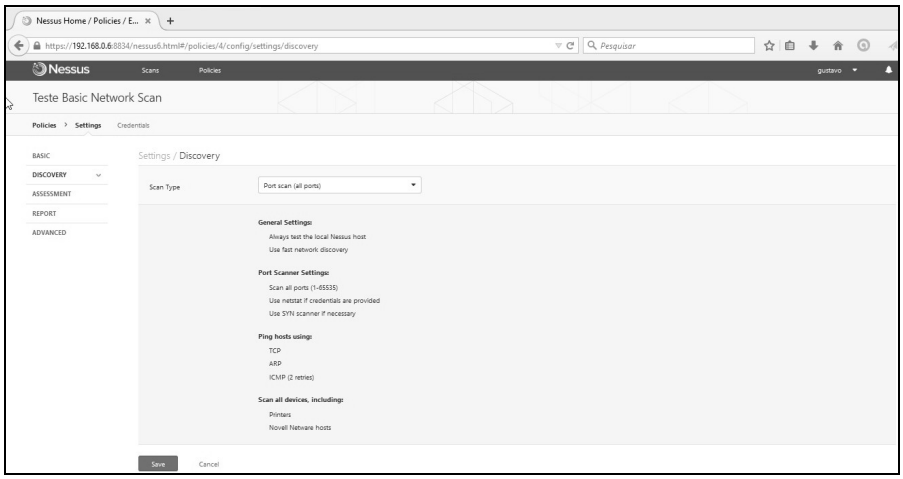
Figura 45 - Etapa 2 da criação da política 1



Fonte: Próprio Autor (2015)

A próxima etapa é a escolha do tipo de escaneamento a ser realizado pela política. O tipo de *Port Scan* (*all ports*) realiza testes e verifica vulnerabilidades em todas as portas, usando os protocolos TCP, ARP[17], ICMP[18], dentre outros, como a Figura 46.

Figura 46 - Etapa 3 da criação da política 1



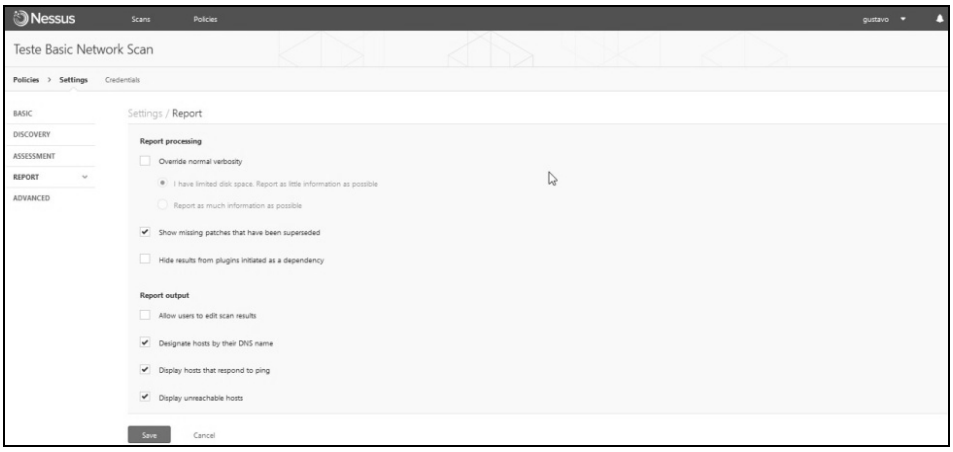
Fonte: Próprio Autor (2015)

17 ARP:Este protocolo é um padrão necessário para o protocolo TCP/IP. "[...] Ele resolve os endereços IP utilizados por programas de software que usam TCP/IP para endereços de controle de acesso à mídia usados por hardware de rede local (LAN). [...]."Technet [s.d.].

18 ICMP: Este também é um protocolo usado no padrão TCP/IP, que significa Protocolo de mensagens de controle da Internet, ou Internet Control Message Protocol. "[...] Com o ICMP, os hosts e roteadores que usam a comunicação IP podem relatar erros e trocar informações de status e controle limitado." Technet [s.d].

Após a escolha do tipo de escaneamento, necessita-se configurar as opções para o relatório, que contém os resultados da coleta. A Figura 47 mostra como foi configurada o relatório dos resultados para esta política.

Figura 47 - Etapa 4 da criação da política 1



Fonte: Próprio Autor (2015)

As configurações principais efetuadas neste estudo baseiam-se no tipo de relatório escolhido, dentre elas algumas podem ser destacadas. A opção "***Show missing patches that have been suspended***", permite mostrar falhas ausentes, que outras políticas não mostrariam, como: portas desconhecidas, portas executando serviços, dentre outras coisas que podem ser detectadas.

O relatório emitirá sua saída agrupando os *hosts,* que terão seus nomes através do DNS[19]. Ele informará se existe resposta do *host* ao comando *ping,* já que, se o *host* não estiver online, não há como realizar os testes, processo este pelo qual o *ping* é responsável. Além disso, o relatório detectará também *host* que estiverem desconhecidos, porém que não foi possível realizar o teste.

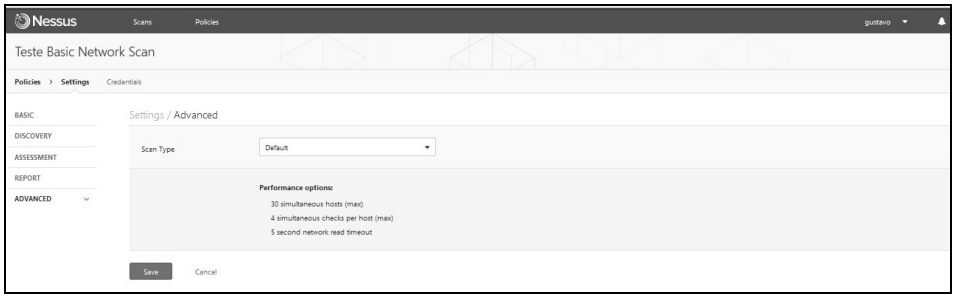
A última etapa da configuração do tipo de escaneamento, que para este estudo foi mantida como padrão, já que a mesma conta com escaneamento em até 30 *hosts* simultaneamente, detectados como acessíveis em até 5 segundos pelo Nessus, *hosts* estes que sofrerão os testes de escaneamentos. A

19 DNS: Domain Name System (Sistema de Nomes de Domínios). È um protocolo, cujo qual seu serviço é converter um endereço IP no nome do seu host e vice versa.

Figura 48 mostra os detalhes do modelo padrão das configurações avançadas da criação desta política.

Após esta etapa, torna-se necessário apenas efetuar o salvamento das configurações na opção “***Save”***.

Figura 48 - Etapa 5 da criação da política 1

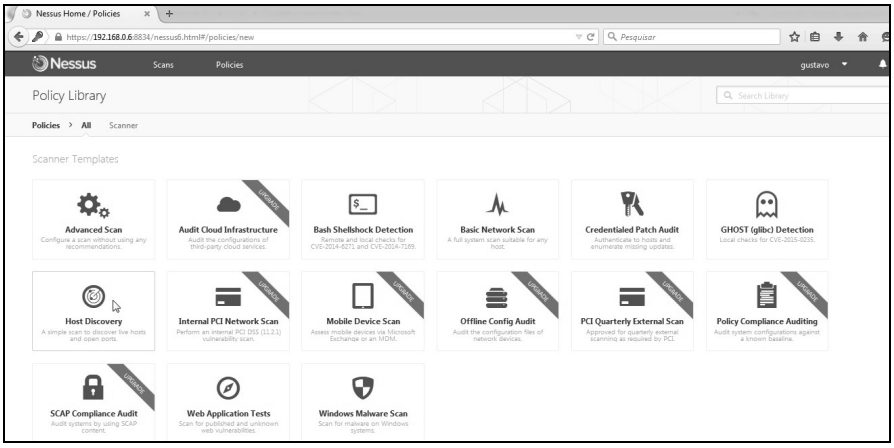


Fonte: Próprio Autor (2015)

Criação da política de descoberta de host

Para a criação de uma nova política, o processo inicial é o mesmo da Figura 42, em que será exibida uma listagem dos tipos de políticas para serem configuradas. Para está política, torna-se necessária a escolha *Host Discovery*, como a Figura 49 mostra.

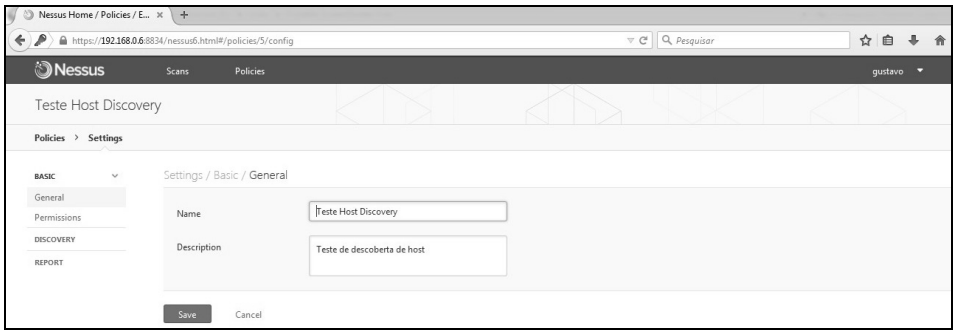
Figura 49 - Etapa 1 da criação da política 2



Fonte: Próprio Autor (2015)

Com a escolha efetuada, a configuração inicia-se com a escolha de um nome e uma descrição para a política, a Figura 50, mostra como foi configurada para o presente trabalho.

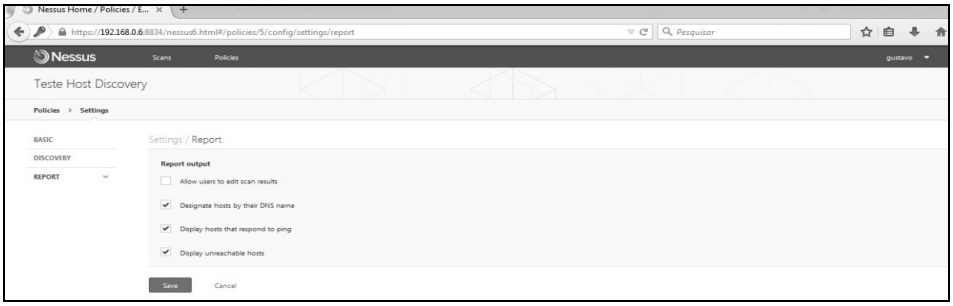
Figura 50 - Etapa 2 da criação da política 2



Fonte: Próprio Autor (2015)

O próximo passo é a definição do compartilhamento com outros usuários desta política para os mesmos terem acesso a ela, como mostra a Figura 45. A etapa seguinte é a escolha do tipo do escaneamento, para este teste será o *default* como mostra a Figura 46. Para finalizar, novamente, torna-se necessário configurar os detalhes para a geração do relatório com os resultados obtidos nessa política, como mostra a Figura 51. Para este estudo foram escolhidas as opções: separar os *hosts*; mostrar os *hosts* que responderam ao comando "***ping***"; e mostrar os *hosts* que estão indisponíveis. Após todas as configurações feitas, torna-se necessário salvar as alterações na criação, clicando em "***Save***".

Figura 51 - Última etapa da criação da política 2

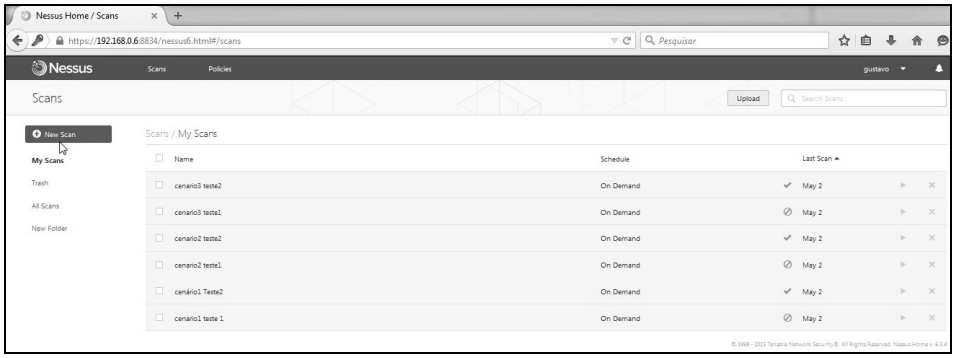


Fonte: Próprio Autor (2015)

Fazendo escaneamentos

Com as políticas criadas, o passo seguinte baseia-se na realização dos escaneamentos. Para realizar os escaneamentos alguns passos são necessários alguns passos. Para o primeiro passo necessita-se estar na guia "***Scan***" e em seguida escolher a opção *"**New Scan**"*, como mostra a Figura 52.

Figura 52 - Primeira etapa para realizar os escaneamento



Fonte: Próprio Autor (2015)

Após a escolha da opção de criação de um novo escaneamento, todas as políticas padrões e as criadas pelo usuário estarão disponíveis, tendo o usuário que escolher uma delas para iniciar o escaneamento, como mostra a Figura 53. Após a escolha, alguns campos precisam ser preenchidos, como: o nome para o escaneamento, a descrição do escaneamento, o local em que será salvo o resultado do escaneamento, o tipo de escaneamento (rede local ou externa) e os alvos[20] (podendo ser especificados por endereço IP ou nome).

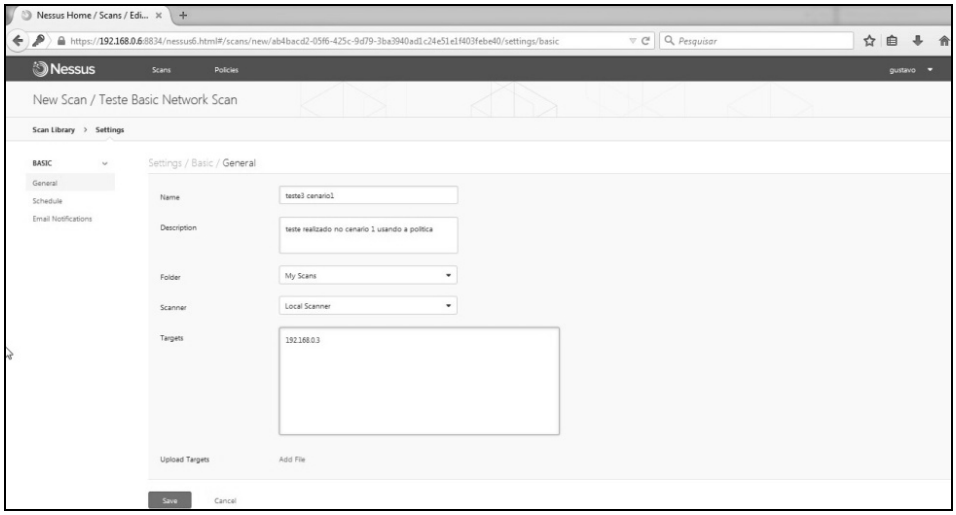
A próxima etapa consiste na configuração do agendamento deste escaneamento criado, podendo ser adiado ou feito de imediato, para este estudo a opção escolhida foi à imediata, como mostra a Figura 54.

A etapa final consiste no envio do resultado do escaneamento por *e-mail*, que para este estudo não foi configurado esta opção do Nessus, e deste modo exibe uma mensagem de erro, como a Figura 55 mostra. Com todas as

20 Alvo: são os hosts onde vai ser realizado um determinado teste

configurações feitas, torna-se necessário salvar as alterações, escolhendo a opção "***Save***". Depois da opção selecionada o escaneamento irá iniciar.

Figura 53 - Primeira parte para configurar um escaneamento

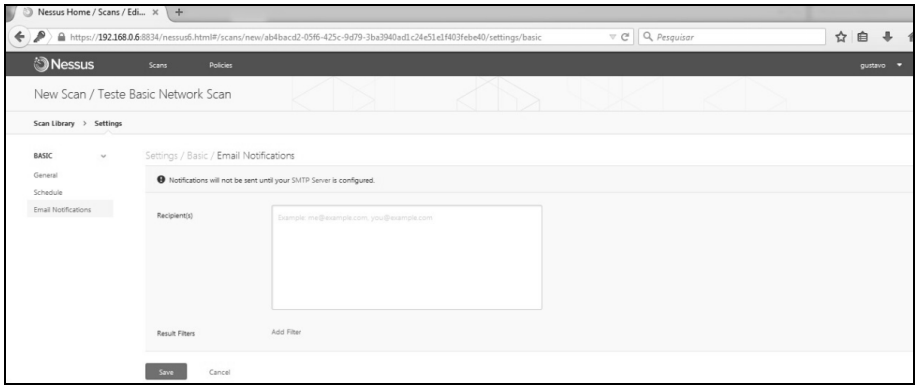


Fonte: Próprio Autor (2015)

Figura 54 - Configuração para agendamento do escaneamento

Fonte: Próprio Autor (2015)

Figura 55 - Etapa para configurar relatórios de escaneamento via e-*mail*

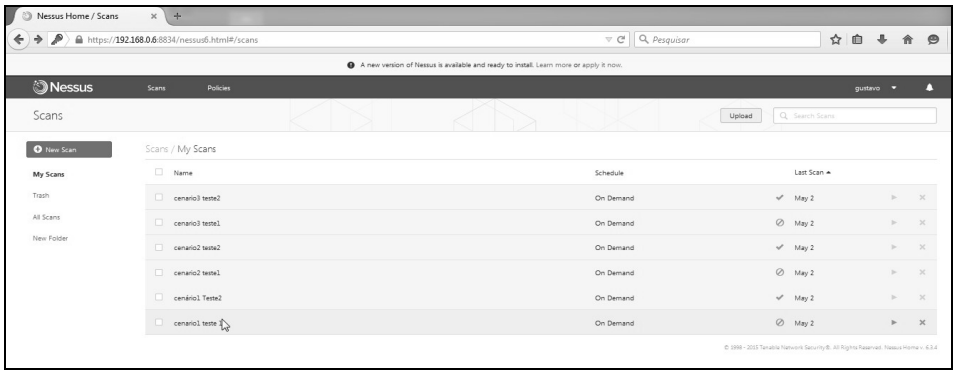


Fonte: Próprio Autor (2015)

Exportação dos relatórios gerados após os escaneamentos

Com as políticas criadas e os escaneamentos realizados, torna-se necessário exportar os relatórios com os resultados. Após o fim do escaneamento, na guia "***Scans***", estarão disponíveis todos os testes realizados. Para se obter os relatórios, torna-se necessário clicar sobre o nome do teste realizado, como mostra a Figura 56.

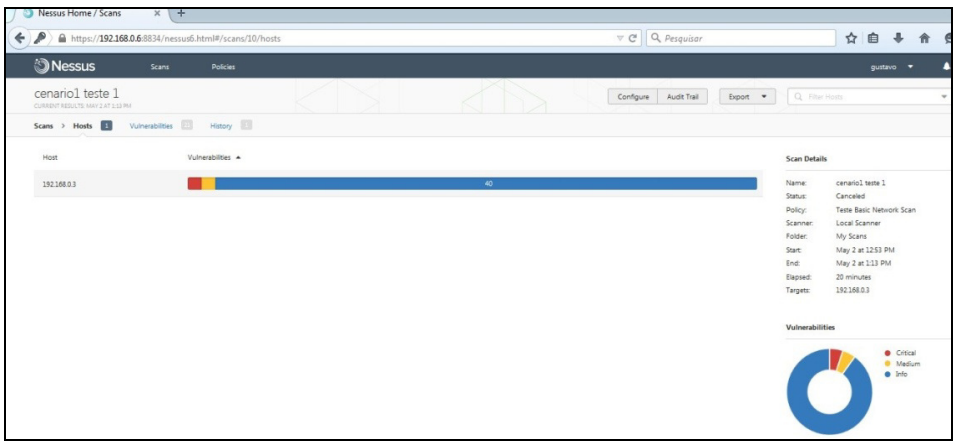
Figura 56- Escolha do teste para obter maiores detalhes do resultado



Fonte: Próprio Autor (2015)

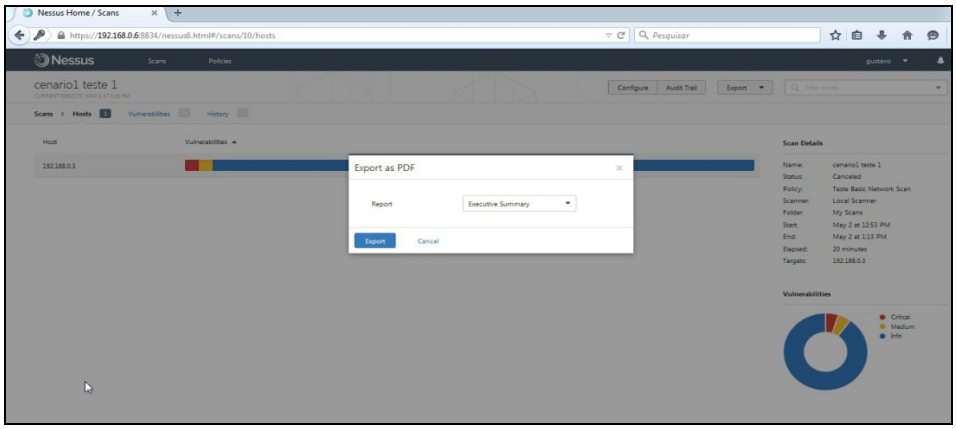
Após clicar no nome, será aberto um resumo do que o Nessus conseguiu detectar ao longo do teste, juntamente com gráfico, e mais alguns detalhes, como mostra Figura 57.

Figura 57 - Resumo dos resultados de um determinado escaneamento



Fonte: Próprio Autor (2015)

Figura 58 Escolha do tipo do relatório e seu formato, para exportar



Fonte: Próprio Autor (2015)

Esse resultado irá mostrar um resumo por *hosts*, mostrando o que foi detectado. Para observarem-se os detalhes, torna-se necessário clicar sobre o gráfico de um *host*, para saber as vulnerabilidades detectadas. Esse relatório pode ser exportado para vários formatos, como, por exemplo, PDF, HTML, entre outros. Para exportá-lo é preciso escolher a opção "***Export***", a extensão do arquivo e o tipo do relatório, como pode ser observado na Figura 58. Para este estudo o tipo de relatório escolhido foi o sumário executivo e o formato PDF. Após esta escolha será necessário informar o nome e o local em que será salvo o arquivo, caso estas informações não sejam informadas, o relatório será exportado para o diretório *download* do usuário da máquina.