UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

UNIDADE ACADÊMICA DE SERRA TALHADA

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

THIAGO FRANCISCO DE ANDRADE SILVA

Teste de Invasão: um relato de experiência em uma instituição pública de ensino no Brasil

Serra Talhada,
Fevereiro/2019

Thiago Francisco de Andrade Silva

Teste de Invasão: um relato de experiência em uma instituição pública de ensino no Brasil

Projeto de Conclusão de Curso apresentado ao Curso de Bacharelado em Sistemas de Informação da Unidade Acadêmica de Serra Talhada da Universidade Federal Rural de Pernambuco como requisito parcial à obtenção do grau de Bacharel.

Orientador: Prof. Dr. Richarlyson Alves D'Emery
Coorientador: Yago Dyogennes Bezerra Vieira

Serra Talhada,
Fevereiro/2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca da UAST, Serra Talhada - PE, Brasil.

S586t Silva, Thiago Francisco de Andrade
Teste de Invasão: um relato de experiência em uma instituição pública de ensino no Brasil / Thiago Francisco de Andrade Silva. – Serra Talhada, 2019.
66 f.: il.

Orientador: Richarlyson Alves D'Emery
Coorientador: Yago Dyogennes Bezerra Vieira

Trabalho de Conclusão de Curso (Graduação em Bacharelado em Sistemas de Informação) – Universidade Federal Rural de Pernambuco. Unidade Acadêmica de Serra Talhada, 2019.
Inclui referências e apêndices.

1. Teste de invasão (Medidas de segurança para computadores). 2. Entidades governamentais. 3. Vulnerabilidade. I. D'Emery, Richarlyson Alves, orient. II. Vieira, Yago Dyogennes Bezerra, coorient. III. Título.

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DE SERRA TALHADA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

THIAGO FRANCISCO DE ANDRADE SILVA

Teste de Invasão: um relato de experiência em uma instituição pública de ensino no Brasil

Trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Sistemas de Informação, defendida e aprovada por unanimidade em 18/02/2019 pela banca examinadora.

Banca Examinadora:

_____
Prof. Dr. Richarlyson Alves D'Emery
Orientador
Universidade Federal Rural de Pernambuco

_____
Prof. Me. Marcelo Iury de Sousa Oliveira
Universidade Federal Rural de Pernambuco

_____
Prof. Me. Hidelberg Oliveira Albuquerque
Universidade Federal Rural de Pernambuco

DEDICATÓRIA

A minha tia-avó Maria Suzana de Andrade (in memorian), que fez tanto por mim ao longo de sua vida.

AGRADECIMENTOS

Quero agradecer, em primeiro lugar, a Deus, pela força e coragem durante toda esta longa caminhada.

Aos meus pais Francisco Luís da Silva e Gildenice Maria de Andrade Silva que me deram apoio e incentivo nas horas difíceis, de desânimo e cansaço.

A minhas irmãs Thatianny Andrade, Thaciany Andrade e Thalyta Andrade por sempre me apoiarem nas minhas escolhas e sempre me incentivarem desde o início desta jornada.

Aos meus avós, tios e primos por acreditarem no meu potencial e nunca me negarem uma palavra de incentivo.

Ao Professor e Orientador Richarlyson Alves D'Emery pela paciência na orientação e incentivo que tornaram possível a conclusão deste trabalho.

Ao meu amigo e Coorientador Yago Dyogennes Bezerra Vieira por todo apoio ao longo da elaboração deste trabalho.

Ao curso de Bach. em Sistemas de Informação e às pessoas com quem convivi nesses espaços ao longo desses anos.

Aos meus amigos do SI L4P4D4 pelas conversas, conselhos e resenhas no qual estamos sempre compartilhando tanto no WhatsApp quanto na vida pessoal.

A minha namorada Maria Gabriela Silva Carvalho que foi compreensiva com os momentos em que permaneci distante

Aos meus professores que me ensinaram com carinho e dedicação em toda minha vida acadêmica.

Aos meus colegas de trabalho que sempre me ajudaram no que podiam.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“A jornada é o que nos traz felicidade e não o destino. ”

Filme Poder Além da Vida

RESUMO

Atualmente, o uso de tecnologias cresce nas instituições tornando-as passíveis de ataques que põem em risco seus ativos, consequentemente, demandam-se manter a segurança da informação no ambiente. Informações confidenciais vazadas e indisponibilidade de acesso podem causar prejuízos financeiros e a reputação de uma organização. Nesse sentido, testes de intrusão são ferramentas que permitem validar a segurança da informação nesses ambientes, através do levantamento informações sobre a rede, mapeamento e exploração de vulnerabilidades analisando ativos da organização, classificando em níveis as ameaças e seu possível impacto na instituição, classificar e sugerir soluções dentro do ambiente. Diante desse cenário, nesta Monografia discute-se e apresenta a utilização de teste de intrusão por *Pentest* na prevenção de ataques cibernéticos às organizações, em especial, a uma instituição pública de ensino. Realizou-se um levantamento sobre informações da rede, ou seja, um mapeamento de vulnerabilidades no ambiente realizado. Foram utilizadas as ferramentas no Kali Linux: Nmap, Nbtscan, Nessus, Metasploit e Aircrack-ng. Apesar de o mapeamento apontar diversas vulnerabilidades, destacam-se as *NFS Exported Share Information Disclosure* e *Microsoft Windows SMB Shares Unprivileged Access*, tidas como severidade de risco crítica e alta, respectivamente. Por fim, apresentam-se sugestões para as soluções necessárias.

Palavras-chave: Segurança da Informação, Ataque, Teste de Intrusão, Pentest, Instituição Pública, Vulnerabilidades, Ferramentas, Soluções, Rede.

ABSTRACT

Currently, the use of technologies grows in institutions making them susceptible to attacks that put their assets at risk, consequently, information security in the environment is demanded. Confidential information leaked and unavailability of access can cause financial damage and the reputation of an organization. In this sense, intrusion tests are tools that allow validating information security in these environments, through the collection information on the network, mapping and exploiting vulnerabilities by analyzing assets of the organization, ranking the threats and their possible impact on the institution, classify and suggest solutions within the environment. Given this scenario, this monograph discusses and presents the use of Pentest intrusion test in the prevention of cyber attacks to organizations, especially to a public educational institution. A survey was carried out on network information, that is, a mapping of vulnerabilities in the environment. The tools in Kali Linux were used: Nmap, Nbtscan, Nessus, Metasploit e Aircrack-ng. Although the mapping points to several vulnerabilities, stand out the NFS Exported Share Information Disclosure and Microsoft Windows SMB Shares Unprivileged Access, which are considered as critical and high risk severity, respectively. Finally, suggestions are presented for the necessary solutions.

Keywords: Information security, Attack, Intrusion Testing, Pentest, Public Institution, , Vulnerabilities, Tools, Solutions, Network.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryptation Standard*
CCMP	*CCM Mode Protocol*
CID	Confidencialidade, Integridade e Disponibilidade
CSRF	*Cross-site Request Forgery*
CVE	*Common Vulnerabilities and Exposures*
CVSS	*Common Vulnerability Scoring System*
DDOS	*Distributed Denial of Service*
DOS	*Denial of Service*
EAP	*Extensible Authentication Protocol*
IFES	Instituições Federais de Ensino Superior
IP	*Internet Protocol*
ISSAF	*Information Systems Security Assessment Framework*
MAC	*Media Access Control*
MSB	*Microsoft Security Bulletin*
NFS	*Network File System*
NIST	*National Institute of Standards and Technology*
NVD	*National Vulnerability Database*
OSSTMM	*Open Source Security Testing Methodology Manual*
OSWAP	*Open Web Application Security Project*
PSK	*Pre-Shared Key*
SMB	*Server Message Block*
TKIP	*Temporal Key Integrity Protocol*
WEP	*Wired Equivalent Privacy*
WPA	*Wi-Fi Protected Access*

SUMÁRIO

1 Introdução

1.1 Contextualização

Com a ascensão tecnológica, cada vez é maior o número de pessoas que utilizam de meios digitais para comunicar, trabalhar, divertir, informar-se de notícias, entre outros. Essa tecnologia engloba, principalmente, o uso de *smartphones*, *tablets* e computadores, quase sempre conectados a Internet. É através de falhas dessas tecnologias que pessoas se aproveitam para tirar algum proveito, seja financeiro, intelectual ou moral, por exemplo.

Se imaginar o simples fato de ter um invasor espiando um familiar pela *webcam* de seu *smartphone* conectado a Internet da praça comunitária; roubando dados do cartão de crédito de uma pessoa durante uma transação de compra *online* a partir do computador conectado no *wifi* de sua casa; ou até mesmo se aproveitando de uma falha de segurança da antena utilizada na conexão com o serviço de banda larga de um provedor para minerar *criptomoedas*, é no mínimo angustiante.

Esses são apenas exemplos de uma imensidão de possibilidade que pessoas mal-intencionadas podem realizar.

Quando direcionado a contexto de organizações, investir em segurança da informação se tornou algo essencial e indispensável na administração de dados, pois envolve a proteção de recursos tecnológicos dentro da organização. Restringindo acesso a pessoas, dispositivos não autorizados e ataques de *crackers*[1] ou *black hats*[2], assim evitando que informações confidenciais sejam divulgadas ou adulteradas.

Para Stallings e Brown (2008), a segurança de computadores é a proteção oferecida a um sistema automatizado para se garantir integridade, disponibilidade e confidencialidade dos

---

[1] Termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança de forma ilegal ou sem ética

[2] Inspirados nos filmes clássicos de faroeste, em que o vilão sempre vestia chapéu preto, no contexto da tecnologia, é um termo usado para designar um extremo de práticas digitais mal intencionadas e, em alguns casos, até ilegais.

ativos de sistemas de informação. Essa tríade incorpora os objetivos principais de segurança para dados e informações, bem como para serviços de Computação.

A implantação da prática de segurança da informação no ambiente organizacional compreende em uma sequência de ações importantes e indispensáveis para identificar e analisar as atividades de negócios da organização e a influência exercida por informação dentro dessas atividades. Visa o dimensionamento do nível de segurança necessário, identificar mecanismos e ferramentas utilizadas, realizar testes de vulnerabilidades, dimensionar os riscos ao qual está exposta a organização. Deve-se ainda considerar os níveis de segurança constatados e seus respectivos envolvidos, como, por exemplo, ambientes, *hardware*, *software*, dados, pessoas, documentação e materiais.

Estudos da Norton Cyber Security Insights Report (2017) indicam que a falta de investimentos nos ativos da informação tem dados alarmantes, em 2017 empresas e pessoas somaram um prejuízo de US$ 22 bilhões em ataques cibernéticos somente no Brasil, enquanto o prejuízo de 20 países chegou a US$ 172 bilhões.

Dados do relatório da segurança digital no Brasil do dfndr lab[3] (laboratório especializado em cibersegurança da Empresa PSafe[4]) detectaram 120,7 milhões de ataques cibernéticos no primeiro semestre de 2018. Esse número praticamente dobrou em relação ao mesmo período de 2017 (PSAFE, 2018).

Segundo Zani (2014), gerente de Engenharia de Sistemas da McAffe[5] no Brasil, nas instituições educacionais não poderia ser diferente. Essas também vêm sendo alvo de ataques que causam danos à rede e credibilidade, por possuírem ambientes com funções diferentes, logo precisam estar seguros e disponíveis, divididos em níveis de criticidade. Áreas em que docentes e discentes tem acesso e outras restritas apenas a docentes, podem trazer diversos riscos à segurança já que existe um enorme fluxo de usuários. Para o autor, ambientes laboratoriais são os mais propensos a qualquer tipo de ataque, o uso de diversos dispositivos aumenta o dano às ferramentas, assim como alteração ou roubo de dados confidencias das instituições, como histórico de alunos, resultados de pesquisas, dados administrativos e outras informações acadêmicas.

---

[3]Laboratório especializado em segurança digital. Site oficial: https://www.psafe.com/dfndr-lab/pt-br/

[4]Empresa de desenvolvimento de aplicativos de segurança, performance e privacidade. Site oficial: https://www.psafe.com/

[5]Empresa de segurança cibernética. Site oficial: http://www.mcafee.com

Santos (2017), líder da Cisco Systems[6] no Mercado de Educação para o Brasil e América do Sul, reforça que diferente de outras áreas da economia como os bancos, cujo foco é em segurança, as instituições de ensino têm a cultura organizacional de incentivar e facilitar o acesso à informações e trocas de conhecimentos entre as pessoas. Alunos, professores e pesquisadores acessam as informações acadêmicas de diversos locais, dentro e fora do *campus* e de vários de dispositivos. E quanto maior o número de dispositivos e pessoas conectados, maior será a vulnerabilidade da instituição a ataques.

Segundo Narezzi (2017), especialista em cibersegurança da 4CyberSec[7], é necessário um processo de segurança mais eficiente que projeta as instituições de ataques. Mesmo como as melhores ferramentas de proteção, não há garantia que não exista riscos, nem sempre um sistema poderá defender a instituição, por isso a organização deve contar com um apoio de um especialista em segurança que trabalhará em conjunto em um plano de segurança, a fim de evitar ataques.

Nesse sentido, *Pentest* ou teste de invasão (do inglês, *penetration testing)* é um teste que objetiva mapear, descobrir e expor todas as possíveis vulnerabilidades, que possam após exploração obter acesso não autorizado a determinado sistema. Normalmente aplicados em redes, sistemas operacionais, *Web*, *Wireless*, banco de dados, aplicativos e programas, nos quais podem-se descobrir falhas nos ambientes testados e assim criar mecanismos de defesa adequados para uma organização (MORENO, 2015).

Ainda segundo Moreno (2015), o Pentest não visa apenas conseguir acesso não autorizado a determinado sistema, mas sim aplicar os devidos mecanismos de segurança quando encontrada alguma falha. Vale reforçar que invasão de dispositivo sem autorização é crime previsto em Lei Nº 12.737:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. "

[6]Empresa de segurança e soluções tecnológicas. Site oficial: http://www.cisco.com

[7]Empresa especializada em cybersegurança. Site oficial: http://www.4cybersev.com

As correções podem ser aplicadas da melhor forma possível, seja com reparações de *hardware*, atualização de *patchs* de segurança e políticas de senha. No final de cada teste realizado, um relatório com as vulnerabilidades encontradas e soluções de correções é entregue a organização.

Nas próximas seções apresenta-se: Problema, Motivação e Justificativa; Objetivos Geral e Específicos; Descrição do Trabalho e Organização do Trabalho.

1.2 Problema, Motivação e Justificativa

Diante do cenário que aponta as organizações de ensino como alvos de ataques, ameaçando a segurança dos seus ativos, causando prejuízos econômicos e à credibilidade dessas, surge o questionamento: como garantir segurança dentro desse tipo de organização? É preciso garantir a confidencialidade, integridade e disponibilidade de informações, restringindo o acesso de pessoas não autorizadas, analisar e identificar possíveis vulnerabilidades no ambiente.

Os crimes cibernéticos, segurança em transações, infraestrutura de TI são os principais responsáveis por motivar o aumento do investimento em segurança; e os investimentos nesse setor propiciam um ambiente digital seguro e que sejam menos propensos a ataques virtuais (ALERTA SECURITY, 2017).

Diante da problemática de soluções que permitam garantir a segurança de uma organização, em especial na detecção de eventuais vulnerabilidades, impulsiona-se o desenvolvimento deste projeto. Assim ele será direcionado aos estudos de Pentest.

É através de *Pentest* que se efetuam diversos testes necessários nessas organizações, de acordo com o ambiente, escopo e objetivos necessários para que possam ser realizados os testes de exploração de possíveis vulnerabilidades encontradas e efetuar a devidas correções reduzindo os riscos de ataques que ameaçam a organização.

O *Pentest* pode ser realizado por um colaborador da área de TI da instituição com uma especialização em teste de invasão, por exemplo. Utilizando-se ferramentas *software* livre, a exemplo de sistemas operacionais totalmente gratuitos como o Kali Linux. Este possui as ferramentas necessárias para realização de um *Pentest*, reduzindo, consequentemente, não só os custos com aquisição de *software* pagos, mas evitando os prejuízos que podem ser

causados se forem realizados ataques por pessoas mal-intencionadas dentro e fora da instituição.

1.3 Objetivos

Esta pesquisa tem por objetivo geral analisar e explorar vulnerabilidades e sugerir correções das que colocam em risco à segurança da informação numa Instituição de Ensino Pública.

Para alcançar esse objetivo, têm-se os seguintes objetivos específicos:

- Levantar as informações sobre o ambiente a ser explorado;
- Mapear os tipos de vulnerabilidades e o alvo da exploração;
- Definir os tipos de testes a serem realizados;
- Levantar as vulnerabilidades presentes;
- Explorar as vulnerabilidades encontradas; e
- Apresentar os resultados com as vulnerabilidades exploradas e possíveis correções para prevenção de riscos.

1.4 Descrição do Trabalho

Foi realizado um teste de invasão em um ambiente de uma instituição pública de ensino, utilizando-se de ferramentas para coleta de informações de rede Nmap e Nbtscan, para análise de vulnerabilidades a ferramenta Nessus, o Metasploit na execução de módulos *exploit* e o conjunto de ferramentas Aircrack-ng no teste em rede *Wireless*.

1.5 Organização do Trabalho

Este trabalho está estruturado da seguinte forma:

- Capítulo 1 - apresenta-se a contextualização do cenário que envolve este trabalho, o problema e motivação que inspiram a realização desta pesquisa, os objetivos gerais e específicos, descrição do trabalho e como o trabalho está organizado;
- Capítulo 2 - abordam-se conceitos de segurança de informação, vulnerabilidades, ameaças, ataques externos e internos, alguns tipos de ataques, sobre teste de invasão e algumas ferramentas que auxiliarão nos testes;
- Capítulo 3 - apresentam-se trabalhos relacionados;
- Capítulo 4 - apresentam-se os resultados obtidos a partir da metodologia empregada;
- Capítulo 5 - Apresentam-se as considerações finais, apontando as contribuições e limitações da pesquisa; e
- Ao final são apresentadas as referências e apêndices que complementam o trabalho.

2 Referencial Teórico

2.1 Segurança da Informação

Falar em segurança da informação tem como objetivo mostrar as formas que garantam proteção ao principal ativo das organizações: a informação, na qual está ligada em todos os processos que envolvem a organização. Ao se falar de segurança não se pode deixar de falar dos princípios que formam a tríade confidencialidade, integridade e disponibilidade. Esses três conceitos envolvem os objetivos fundamentais da segurança da informação tanto para dados quanto para serviços da computação.

A confidencialidade, integridade e disponibilidade são os princípios de segurança providos de diferentes mecanismos a falta deles pode afetar a segurança do ambiente, com eles é possível identificar melhor os problemas e fornecer melhores soluções (HINTZBERGEN et al., 2018).

Ainda segundo Hintzbergen et al. (2018) a **confidencialidade** assegura que o sigilo seja aplicado nos elementos do processamento de dados e impeça a divulgação não autorizada de dados, essa confidencialidade deve ser garantida quando os dados em transmissão até chegar ao destino e enquanto residirem em sistemas e dispositivos na rede.

A **integridade** refere-se à corretude e consistência com o estado ou informação; modificações não autorizadas, seja intencional ou acidental, viola o princípio de integridade.

A **disponibilidade** consiste nas características de oportunidade que garante que a informação esteja disponível quando necessário, a continuidade que garante que a informação esteja disponível mesmo em caso de falha e a robustez que garante que a informação esteja disponível quando todos estejam acessando a mesma.

A segurança de informação nas organizações tem sofrido mudanças nas últimas décadas, consideradas importantes dentro da organização antes era feita por meios físicos e administrativos (STALLINGS, 2005). E com a propagação da Internet surgiu um novo desafio para os Engenheiros de *Software*: projetar e implementar sistemas seguros (SOMMERVILLE, 2007). Medidas de segurança de rede durante as transmissões de dados são necessárias para garantir autencidade e proteção dos dados (STALLINGS, 2005).

2.2 Vulnerabilidades

Na segurança da informação a vulnerabilidade é tida como a fraqueza que permite que o atacante viole a segurança da rede ou sistema. Moreno (2015) reforça que com o mapeamento das vulnerabilidades pode-se analisar e identificar as possíveis vulnerabilidades que através da coleta de informação, descobrimento e enumerações de alvos, serviços e portas, podem-se analisar quais destas compromete a segurança.

Moreno (2015) ainda classifica as vulnerabilidades em local e remota. A local é geralmente usada para aumentar o acesso do atacante, já a remota busca acesso remoto a estação atacada. Para McClure, Scambray e Kurtz (2014), local é definido um *shell* de comando ou *login* real; enquanto o remoto é definido como obter acesso por meio da rede ou outro canal de comunicação.

Para identificação dessas vulnerabilidades são usados *Scanners* de vulnerabilidades. O mapeamento é o processo que relaciona os atributos de segurança específicos de um sistema a uma vulnerabilidade associada ou em potencial (MCCLURE; SCAMBRAY; KURTZ, 2014). O *Pentester*[8], responsável pela realização do teste de invasão, utiliza-se dos *scanners* para descobrir e mapear as vulnerabilidades que podem ser exploradas (WEIDMAN, 2014). Os *scanners* automatizados contêm banco de dados atualizados (MCCLURE; SCAMBRAY; KURTZ, 2014) como *Common Vulnerabilities and Exposures* (CVE), *National Vulnerability Database* (NVD) e *Microsoft Security Bulletin* (MSB).

Uma vez coletadas e mapeadas as informações sobre as vulnerabilidades, de acordo com Giavaroto e Santos (2013), estas podem se exploradas através de *exploit* e *payload*, sendo o primeiro um código escrito para explorar determinada falha e provar que a vulnerabilidade existe, ganhando o acesso antes não permitido; enquanto o segundo é relacionado a carga do código escrito aplicada ao alvo para abrir a comunicação entre o atacante e o alvo, como, por exemplo, o acesso ao *prompt* de comando do alvo.

É importante ressaltar que muitas destas vulnerabilidades não existem *exploits* sem custo ou, quando existente, são pagos (MORENO, 2015).

---

[8] Termo para o profissional de segurança responsável por encontrar vulnerabilidades em sistemas, redes e empresas

2.3 Ameaça

Qualquer coisa que possa afetar ou atingir o funcionamento, operação ou disponibilidade, integridade da rede ou sistema. Na terminologia de Sommerville (2007), ameaças são circunstâncias que pode causar perda ou dano, uma vulnerabilidade que está sujeita a um ataque.

Hintzbergen et al. (2018) reforçam que uma ameaça em potencial pode causar um incidente não desejado, resultando prejuízos ao sistema ou à organização e que um agente ameaçador é uma entidade que tira vantagem de uma vulnerabilidade. Um agente ameaçador pode ser um invasor acessando a rede através de uma porta no *firewall*, um processo que viole a política de segurança ao acessar dados, um funcionário que comete um erro de forma não intencional, mas que exponha informações confidenciais ou destruindo a integridade do arquivo e um tornado destruindo uma instalação. As ameaças em cada país diferem do uso de Internet e do nível de desenvolvimento, a segurança da informação é importante para governos, universidades, militares, saúde, etc.

2.4 Ataques, Características e Tipos

O ataque pode ser definido como a ação que compromete a segurança da informação dentro de uma organização. Na terminologia de Sommerville (2007), o ataque é a exploração de uma vulnerabilidade na tentativa de causar algum dano, geralmente partindo de fora do sistema.

Stallings e Brown (2014) definem como uma ação que comprometa a segurança que a organização possui. Os ataques podem ser classificados como **externo** quando originado de fora da rede protegida ou **interno** quando originado de dentro da rede protegida da organização. Um ataque não autorizado, mas bem-sucedido é denominado de invasão.

São diversos os tipos de ataques. Os **ataques de senhas** se aproveitam do fato que senhas representarem um ponto fraco, no que diz respeito a testes de invasão, riscos relacionados à autenticação baseada sem senha, os ataques de força bruta e palpite embasado representam riscos sérios a senhas fracas. O uso de senhas fortes é obrigatório para garantir a

segurança, porque tudo que estiver entre o invasor e os dados poderá ser afetado (WEIDMAN, 2014).

Em geral os **ataques *Wireless*** são feitos utilizando-se de criptografia e de duas técnicas em geral, cujo objetivo dessas técnicas é o de atacar sistemas de encriptação e recuperar uma chave em uso, em vez de simplesmente recuperar o texto claro a partir de um único texto cifrado. As duas técnicas, descritas por Stallings (2015), são **criptoanálise** em que os ataques utilizam a natureza do algoritmo e talvez o conhecimento das características comuns ao texto claro ou ainda algumas amostras de pares de texto claro-cifra, o ataque explora as características do algoritmo para tentar deduzir um texto claro ou especifico ou a chave utilizada. Já no **ataque força bruta**, o atacante testa todas a chaves possíveis no texto cifrado, até obter um tradução inteligível para o texto claro, geralmente metade de todas as chaves possíveis precisam ser experimentadas para então se obter sucesso.

Ainda em relação à criptografia, redes com criptografia OPN, ou seja, sem criptografia, não existe nenhum processo de autenticação, assim as máquinas conseguem se conectar à rede sem nenhuma requisição de senha. Só conectá-la e o acesso é permitido e o dispositivo já estará na rede (MORENO, 2016).

A criptografia *Wired Equivalent Privacy* (WEP) acrescenta criptografia aos pacotes que circulam na rede *Wireless*, objetivando proteger os dados. Caso ocorra um ataque de captura a rede, os pacotes serão criptografados, deixando os dados inelegíveis. É um tipo de criptografia ultrapassado, mas ainda muito utilizada. O algoritmo de criptografia usado é o RC4 que pode ser quebrado em questão de minutos usando criptoanálise (MORENO, 2016).

Pelo fato do sistema de criptografia WEP ser considerado frágil, criou-se o *Wi-Fi Protected Access* (WPA) em que se é utilizado outro tipo de autenticação. O *Extensible Authentication Protocol* (EAP) ou *Pre-Shared Key* (PSK) usa o protocolo *Temporal Key Integrity Protocol* (TKIP), fundamento no RC4, mas é baseado em troca de chaves dinâmicas, adicionando mais segurança na criptografia, mas ainda assim apresenta falhas. Assim lançou-se o WPA2, que utiliza o protocolo *CCM Mode Protocol* (CCMP) e algoritmo de criptografia *Advanced Encryptation Standard* (AES), considerado um algoritmo bem superior (MORENO, 2016).

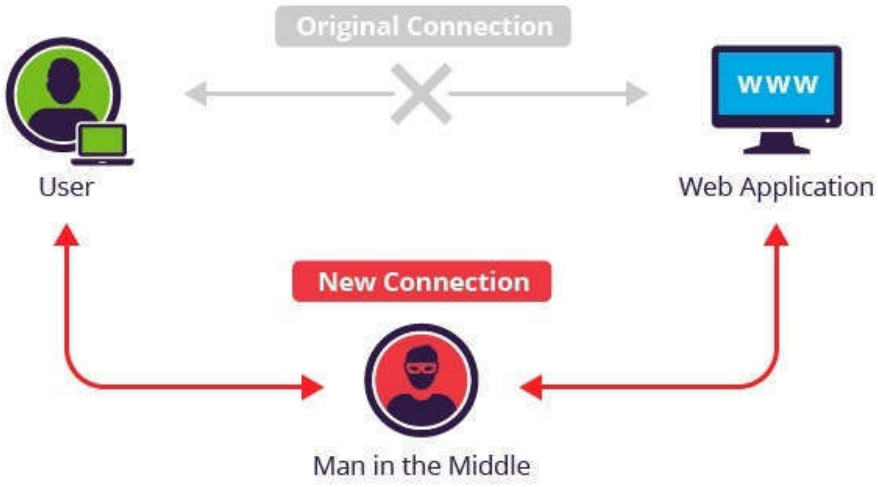
Sempre que um cliente se conecta a uma rede *Wireless* acontece o *Handshake* (aperto de mão), pode-se esperar impacientemente um cliente se conectar ou forçar a desautenticação de um cliente para que quando o cliente se conecte novamente aconteça o *Handshake* (MCCLURE; SCAMBRAY; KURTZ, 2014).

Os **ataques de negação de serviço** é um ataque que impede o uso ou gerenciamento normal dos recursos de comunicação. Podem ter alvos específicos, como, por exemplo, uma entidade pode suprimir todas as mensagens direcionadas a determinado destino (como o serviço da auditoria de segurança). Outra forma de negação de serviço é o distúrbio de toda rede ou servidor, desativando o servidor de rede ou sobrecarregando-o com mensagens do modo que comprometa o seu desempenho (STALLINGS, 2005).

Esses ataques podem ser do tipo ataque de negação de serviço distribuído (DDoS, do inglês *Distributed Denial of Service*), que consiste em várias máquinas atacando o alvo, todas realizando um ataque de negação de serviço (DoS, do inglês *Denial of Service*) ao mesmo tempo para aumentar o desempenho (MORENO, 2015). Esse ataque é dos maiores problemas da rede *Wireless*, porque depois de conectado à rede o objetivo é atacar os que estão dentro da rede interna (MORENO, 2016).

O **ataque Man in the Middle** (MitM) é provavelmente o ataque mais eficiente dentro de uma rede, interceptando a conexão entre dois *hosts*, ficando entre a conexão. O MitM efetua ataques de captura, leitura e redirecionamento de trafego (MORENO, 2015). A Figura 2.1 ilustra o ataque.

Figura 2.1 – Ataque MitM



Fonte: Nunes (2017)

Vale ressaltar ainda, a existência do **ataque de engenharia social**, que consiste na obtenção de informação através de pessoas. São técnicas de manipulação ou persuasão para obter algum tipo de informação não autorizada como informações confidenciais ou ter acesso a áreas restritas (MORENO, 2015).

2.5 Teste de Invasão ou Pentest

Testes de invasão ou *Pentesting* são simulações de ataques reais que avaliam os riscos associados a possíveis brechas de segurança, em que *Pentesters* realizam o mapeamento de vulnerabilidades que poderiam ser usadas pelos invasores, mas também exploram essas vulnerabilidades, sempre que possíveis, para avaliar o que pode acontecer após uma exploração bem-sucedida (WEIDMAN, 2014).

Weidman (2014) ainda reforça que o escopo dos testes de invasão varia de acordo com cada necessidade, a avaliação poderá ser de uma ou mais aplicações *Web*, ataques de engenharia social, teste de invasão de rede quando dentro da rede através do teste de invasão interno ou quando fora da rede como um ataque a rede *Wireless*, quando o teste de invasão externo.

2.5.1 Etapas

As etapas do teste de invasão descritas por Weidman (2014) têm início com a **preparação** (*pre-engagement*), quando é decidido sobre o escopo do teste e os objetivos do teste. Seguida da fase de **coleta de informações** (*information-gathering*), em que um Pentester verifica as informações disponíveis publicamente e que podem ser usadas para se conectar aos sistemas. A fase de **modelagem de ameaças** (*threat-modeling*) usa essas informações para determinar o valor e impacto de que cada descoberta possa causar a organização caso seja invadida, é a fase em que pode ser realizado o desenvolvimento de um plano de ação e métodos de ataque. A fase de **análise de vulnerabilidades** (*vulnerabity analysis*) é realizada antes de qualquer tentativa de ataque, um Pentester realiza uma análise das vulnerabilidades que podem ser exploradas na fase de **exploração de falhas** (*explotation*). Um *exploit* pode ser útil na fase de **pós-exploração de falhas** (*post-explotation*), tirando mais vantagens dos resultados da exploração, a fim de descobrir mais informações, obter dados importantes para organização ou acessar outros sistemas. Por fim, o Pentester apresenta relatórios técnicos e executivos na fase de **geração de relatórios** (*reporting*).

2.5.2 Tipos

Os tipos de Pentest podem ser classificados, segundo Moreno (2015), como:

- ***Black-Box*** **-** o *Pentester* não tem nenhum conhecimento prévio sobre a infraestrutura (rede, máquina, mapeamento, servidos ou processos). É o tipo que mais se assemelha ao ataque externo, pode ser feito de fora da rede e o atacante não tem nenhum conhecimento sobre a infraestrutura atacada. Pode ser subcategorizada em:
  - *Blind* **-** o Pentester não tem nenhuma informação sobre a rede e o alvo sabe que será atacado e quais testes serão realizados; e
  - *Double Blind* **-** o Pentester não tem nenhuma informação sobre a rede e o alvo não sabe que será atacado e não quais testes serão realizados.
- ***White-Box*** **-** o *Pentester* tem total conhecimento sobre a infraestrutura, seja a infraestrutura de rede, diagrama, mapeamento, endereços de *Internet Protocol* (IP), *firewall*, códigos fontes, etc. Pode ser subcategorizada em:
  - *Tandem* **-** o Pentester tem informação total sobre a rede e o alvo sabe que será atacado e quais testes serão realizados; e
  - *Reversal* **-** o Pentester tem informação total sobre a rede e o alvo não sabe que será atacado e não quais testes serão realizados.
- ***Gray-Box*** **-** o *Pentester* tem conhecimento parcial sobre a rede testada, é uma mistura dos tipos *Black-Box* e *White-Box*. Pode ser subcategorizada em:
  - *Gray-Box* **-** o Pentester tem informação parcial sobre a rede e o alvo sabe que será atacado e quais testes serão realizados; e
  - *Double gray-box* **–** o Pentester tem informação parcial sobre a rede e o alvo não sabe que será atacado e não quais testes serão realizados.

2.5.3 Metodologias

A metodologia Pentest a ser usada em testes de invasão varia de acordo com a necessidade, cenário e escopo de cada projeto, podem ser escolhidos para testes de segurança

de forma geral ou de forma específica, a partir disso Moreno (2015) destaca as principais metodologias:

- ISSAF - metodologia para auditoria rápida. Abrange de forma geral e está dividida nas fases de planejamento, avaliação, tratamento e acreditação;
- OSWAP - metodologia voltada para aplicações *Web* e servidores. Dentre os testes realizados no ambiente *Web* estão injeção, quebra do sistema de autenticação, referência direta a objetos, *directy traversal*, *file upload*, configurações falhas, exposição de dados sensíveis, *Cross-site request forgery* (CSRF), controle de acesso quanto a função, utilização de componentes vulneráveis, manutenção de acesso e negação de serviço;
- OSSTMM - não é uma metodologia específica. É baseada em métodos científicos que geram o processo de segurança da informação, de forma geral essa metodologia se passa por três fases: pré-teste, teste e pós-teste;
- FEOIS (BSI, 2003) – descreve e estrutura o teste de penetração comissionado, deve-se estar de acordo com os objetivos do cliente, delineando as etapas necessárias para alcançar os objetivos do teste, está dividido em: preparação, reconhecimento, análise de informações, execução e análise final; e
- NIST (WACK; TRACY; SOUPPAYA, 2008) – metodologia do *National Institute of Standards and Technology* (NIST) que está dividida em 4 fases: planejamento, reconhecimento, ataque e documentação.

2.5.4 Relatórios

Ao final do Pentest apresentam-se relatórios dos testes divididos em duas visões: a executiva e a técnica.

Na executiva utiliza-se de uma maneira de transmitir informações na qual todos possam compreender, enquanto na técnica se faz a inclusão de todos os termos técnicos e que só uma pessoa habilitada possa compreender.

2.6 Ferramentas para Realização de Pentest

São diversas as ferramentas que podem ser utilizadas por um *Pentester*. Nessa seção apresentam-se algumas.

Kali Linux[9] é uma distribuição GNU/Linux baseada no Debian, considerada a sucessora do BackTrack. O projeto apresenta várias melhorias, além de mais aplicativos. É voltada principalmente para auditoria e segurança de computadores em geral. É desenvolvida e mantida pela Offensive Security Ltd.

Nmap[10] é um *software* livre que realiza *port scan*. É desenvolvido pelo Gordon Lyon, autoproclamado *hacker* "Fyodor". É muito utilizado para avaliar a segurança dos computadores e para descobrir serviços ou servidores em uma rede de computadores. Nmap é conhecido pela sua rapidez e pelas opções que dispõe. Com o Nmap temos muitas informações úteis, mas para aqueles que preferem interfaces gráficas podemos usar o ZenMap que é apenas um *frontend* para o Nmap. A vantagem de uso do ZenMap[11] está no pequeno mapa da rede e a possibilidade de ver dados das máquinas individualmente com um clique.

Nbtscan[12] é um programa para verificação de redes IP para informações de nomes NetBIOS (semelhante ao que a ferramenta nbtstat do *Windows* fornece em relação a *hosts* únicos). Ele envia uma consulta de status do NetBIOS para cada endereço em um intervalo fornecido e lista as informações recebidas em formato legível. Para cada *host* respondido, ele lista o endereço IP, o nome do computador NetBIOS, o nome de usuário registrado e o endereço *Media Access Control* (MAC).

Nessus[13] é um programa de verificação de falhas/vulnerabilidades de segurança, composto por um cliente e servidor, sendo que o *scan* propriamente dito é feito pelo servidor.

Aircrack-ng[14] é um detector de redes, *sniffer* de pacote, aplicativo de quebra de WEP e ferramenta de análise para redes locais sem fios 802.11. Funciona com qualquer placa

---

[9] Disponivel em https://www.kali.org/downloads/

[10] Disponível em https://nmap.org/

[11] Disponível em https://nmap.org/zenmap/

[12] Disponível em https://sectools.org/tool/nbtscan/

[13] Disponível em https://www.tenable.com/downloads/nessus

[14] Disponível em https://www.aircrack-ng.org/

Wireless cujo driver suporta modo de monitoramento bruto e pode capturar e analisar tráfego 802.11a, 802.11b e 802.11g.

Metasploit[15] é um projeto de segurança de informação com o objetivo de análise de vulnerabilidades de segurança e facilitar testes de penetração e no desenvolvimento de assinaturas para sistemas de detecção de intrusos.

2.7 Considerações Finais

Diante do que foi abordado, se vê a importância de garantir a segurança de informação, em que um ambiente nem sempre estará seguro e à medida que testes e técnicas são aplicados e falhas são corrigidas, outras novas aparecerão e o processo de aplicação deverá ser sempre repetido.

Verifica-se, diante da necessidade de garantir a segurança, que a aplicação de um *Pentest* com a realização de suas etapas pode ser aplicada por um profissional para minimizar os riscos. A aplicação de técnicas de testes de invasão podem ser tornar também atividades no núcleo de tecnologia da organização.

Através do uso de técnicas e ferramentas, que podem ser aplicadas em diversas situações, é possível realizar um levantamento e mapear vulnerabilidades que poderiam comprometer o ambiente e que devem ser corrigidos previamente, mantendo sempre os princípios de segurança.

[15] Disponível em https://www.metasploit.com/

3 Trabalhos Relacionados

No trabalho intitulado “Análise de vulnerabilidades através de *scanners* detectores”, Buzzatte (2014) propõe uma análise de vulnerabilidades na rede corporativa da UFSM e CIFSM apresentando *scanners* capazes de detectar vulnerabilidades presentes na rede, destacando pontos em nível baixo, médio e alto e que podem ser possíveis alvos de ataques como portas abertas, serviços que não deveriam estar ativos e atualização de tipos de vulnerabilidades não efetivas. Entretanto, não realiza exploração ou solução para as vulnerabilidades encontradas.

No trabalho “Auditoria de segurança da informação em sistema de aplicações” de Cruz (2017) propõe-se a análise de vulnerabilidades, teste de segurança em sistemas em três estudos de casos em determinados ambientes internos e externos avaliando os riscos e sugerindo as correções necessárias para garantir a segurança e evitar possíveis ataques. Foi realizado o reconhecimento do ambiente e coletada de informações como IP, linguagem de programação, servidor *Web*, serviços, portas, arquiteturas, por exemplo. Visando obter o máximo de detalhes possíveis, após esse procedimento foi feito uma varredura de portas e serviços com Nmap, objetivando-se identificar portas abertas e serviços que poderiam ser explorados. Utilizando a ferramenta Veja, analisaram-se vulnerabilidades e as classificando em alta, média e baixa. Nas vulnerabilidades classificadas como alta é dada uma atenção especial, já que essas podem ser exploradas de forma mais fácil e causas maiores danos. No primeiro caso um ataque *SQL Injection* foi executado de forma controlada e cuidadosa, a fim de evitar causar indisponibilidade ou danos ao sistema, explorando as vulnerabilidades encontradas neste caso. No segundo caso, não foi realizado a exploração do ambiente já que o teste foi feito de forma parcial sendo este finalizado na etapa de análise de vulnerabilidades. No terceiro caso, a análise ainda classificou as vulnerabilidades em mais um nível acima, o crítico, e a exploração foi mais além, foram vulnerabilidades em que se executou a *SQL Injection*. Nas vulnerabilidades em que o serviço remoto do *Windows* estava ativo, foi feito o ganho de acesso remoto ao sistema.

Lepesqueur e Oliveira (2012), em seu trabalho “*Pentest*, análise e mitigação de vulnerabilidades”, propuseram a realização de um *Pentest* e análise em dois tipos de cenários distintos, um primeiro centrado na realização de um ataque externo em um ambiente comum

(*smartphones*, *tablets* e *notebooks*), que utilizam rede sem fio para obterem acesso à rede. Objetivando em um ataque a se infiltrar nessa rede, executou-se ataque de força bruta para realização da quebra de senha WEP, WPA e WPA2 com auxílio da ferramenta Aircrack-ng. O segundo cenário é focado no ataque interno, já que o invasor já se encontrava conectado na rede e o enfoque do ataque era o de explorar possíveis falhas de segurança, podendo causar danos a serviços, destruir informações confidenciais e afetar os demais usuários conectados à rede. Através da ferramenta Nmap obtiveram-se informações sobre a rede e atacou-se, consequentemente, *Firewall* e roteadores. Vulnerabilidades presentes no *firewall* baseadas em protocolo SSH podem ser submetidos a ataques DoS. Foram apresentadas soluções de correções para vulnerabilidades da rede sem fio, recomendando-se a utilização de um servidor Radius, assim as senhas passam ser criptografadas entre o servidor e cliente *Radius*, solicitando uma nova autenticação para acesso. Para o ataque interno a solução apresentada é a definição de uma política a ser seguida pelo *Firewall* como bloqueio de todas as conexões e liberar aos poucos.

Vieira (2018) propôs em "Utilização de *Pentest* na Prevenção de Ataques Cibernéticos às Organizações" a realização de testes de segurança em ambientes computacionais de uma empresa privada, as quais poderiam causar danos aos ativos e credibilidade da organização caso fossem praticados por *Black hats*. Nas informações não protegidas foram exploradas falhas reais. Teve como objetivo principal demonstrar métodos das análises de falhas de segurança, que quando implementadas auxiliam da prevenção de ataques cibernéticos. Apresentou documentos com as falhas e suas correções para que os responsáveis pudessem corrigi-las.

O trabalho "Teste de invasão em ambiente corporativo" de Domingues (2012), tem-se a realização de teste de invasão em rede interna através de um levantamento de vulnerabilidades com os *scanners* Nessus, OpenVas e Nmap. Realizado o escaneamento, foi encontrada uma vulnerabilidade Microsoft, que uma vez explorada com sucesso pode dar controle total ao sistema. Utilizou o Metasploit para encontrar um *exploit* para exploração das vulnerabilidades, Meterpreter executado para manter acesso ao sistema, executando comandos de usuário principal da máquina; e as ferramentas Aircrack e Hydra foram usadas para quebrar senhas. O trabalho não apresenta soluções para vulnerabilidades.

3.1 Trabalho Proposto

Este trabalho propõe a realização de um *Pentest*, análise de vulnerabilidades e possíveis soluções de correções dentro do ambiente de rede interno e externo de uma instituição pública, a fim de garantir segurança à informação dentro da organização. Utilizando-se de ferramentas específicas para cada etapa descrita nos objetivos do trabalho, inicialmente na fase de reconhecimento e levantamento de informações podem ser usadas diversas técnicas e ferramentas como Nmap e Nbtscan para mapear o ambiente da rede; fazer levantamento e mapeamento de vulnerabilidades por meios de *scanners* Nessus; explorar vulnerabilidades com uso de *exploits* encontradas e ferramentas de quebras de senhas Aircrack-ng.

Para realização do trabalho será utilizado o sistema operacional Kali Linux que é um sistema voltado para auditoria e segurança, possuindo diversas ferramentas que auxiliam na realização deste trabalho. Ao final, pretendem-se apresentar os resultados com um quadro dos testes realizados, ferramentas utilizadas, vulnerabilidades encontradas e seus níveis de criticidade, vulnerabilidades exploradas e soluções para as mesmas.

O Quadro 3.1, apresenta uma análise comparativa entre os trabalhos relacionados apresentados.

Quadro 3.1 – Trabalhos Relacionados *versus* Proposto

Trabalho	Ambiente	Ferramentas	Exploração de Vulnerabilidades	Promoção de Ataque	Apresentação de Solução
Buzzatte (2014)	Interno	LanGuard, Nessus e OpenVas	Sim	Não	Não
Cruz (2017)	Interno e Externo	Nmap, Nessus e OpenVas,	Sim	Sim	Sim
Lepesqueur e Oliveira (2012)	Interno e Externo	Nmap, OpenVas, Nessus e Metasploit	Sim	Sim	Sim
Vieira (2018)	Interno e Externo	Mestaploit, Maltego,Wireshark, Nmap, Aircrack, OpenVas	Sim	Sim	Sim
Domingues (2012)	Interno	Nessus, Nmap, Metasploit, OpenVas, Aircrack-ng e Meterpreter	Sim	Sim	Não
Esta Pesquisa	Interno e Externo	Nmap, Nbtscan, Nessus, Metasploit e Aircrack-ng	Sim	Sim	Sim

Fonte: Elaborado pelo autor

4 Materiais e Métodos

4.1 Descrição do Ambiente de Teste

Para realização dos testes, utilizou-se um computador com o sistema operacional Kali Linux 2018.3, contendo as ferramentas necessárias para a realização dos testes; processador Intel Core i7 2.5 GHZ, memória de 8 GB RAM e armazenamento de 100GB de HD.

O ambiente em questão para realização dos testes é distribuído no campus de uma IFES, a exemplo de laboratórios no ambiente interno da rede (rede local cabeada) e ambiente externo da rede (rede W*ireless*), roteadores e *hotspots* institucionais e de terceiros, em que dispositivos próximos e que haja tráfego de rede necessário para realização dos testes. Há também um grande fluxo de pessoas (professores, técnicos e alunos) que utilizam Internet através de *smartphones, tablets* e *notebooks*, podendo também ser explorados com o objetivo de ingressar na rede. Esta etapa tem como objetivo apresentar as ferramentas na prática e seus resultados. O tipo de *pentest* realizado foi o *Black-box* já que não tínhamos nenhuma informação prévia sobre a infraestrutura da rede teste, como número de computadores e como eles se comunicam.

A metodologia utilizada neste trabalho, foi a descrita por Delgado e Santtos (2011), em que, de forma geral, é dividida em 3 etapas (Figura 4.1), comumente utilizada em Empresas do Ramo de testes de penetração, a saber: Planejamento e Preparação; Avaliação e Documentação e Relatório.

Figura 4.1 – Metodologia utilizada em empresas do ramo de testes de penetração

Fonte: Delgado e Santtos (2011)

No **planejamento e preparação** são definidos os objetivos dos testes e como eles serão realizados; a **avaliação** é a fase em que os testes são efetivamente executados, podendo ser divididos em obtenção de informações, mapeamento da rede, identificação de

vulnerabilidades e possível exploração; **documentação e relatório** contêm informações sobre o teste, ferramentas utilizadas, vulnerabilidades encontradas e exploradas e como estas podem ser corrigidas.

Apesar da existência de outras etapas, como as propostas pelas metodologias FEOIS (BSI, 2003) e NIST (WACK; TRACY; SOUPPAYA, 2008) ilustradas na Figura 4.2; justifica-se que a sua não utilização está relacionada ao tempo necessário para sua execução e viabilidade de experiência técnica em áreas específicas da Computação para promoção de ataques as vulnerabilidades, por exemplo. Ressalta-se que nesta pesquisa realizou-se o ataque para quebra de senhas.

Figura 4.2 – Equivalência entre as Fases do Teste de Penetração

<table>
<tr><th>FEOIS</th><th>NIST</th><th>Empresas do Ramo</th></tr>
<tr><td>Preparação</td><td>Planejamento</td><td>Planejamento e Preparação</td></tr>
<tr><td>Reconhecimento</td><td>Reconhecimento</td><td>Avaliação</td></tr>
<tr><td>Análise de informações</td><td>Ataque</td><td rowspan="3">Documentação e Relatório</td></tr>
<tr><td>Execução</td><td rowspan="2">Documentação</td></tr>
<tr><td>Análise Final</td></tr>
</table>

Fonte: Delgado e Santtos (2011)

Na realização dos testes coletaram-se informações sobre o ambiente para entender mais sobre a instituição e a estrutura da organização. Criou-se um mapeamento da rede a fim de entender como estava interligada, verificando status de portas e serviços ativos, ou seja, as primeiras informações sobre a rede. Para este procedimento foi utilizado o *scanner* de porta (Nmap) e o Nbtscan que lista *hosts* ativos e fornece informações como, por exemplo, o nome da máquina e o seu endereço MAC.

Para o mapeamento de vulnerabilidades e investigação dessas que possam comprometer a rede em questão utilizou-se o *scanner* Nessus. Na fase de exploração utilizaram-se *exploits* contra as vulnerabilidades encontradas. Para este procedimento foi utilizada a ferramenta Metasploit. Também foi utilizado o conjunto ferramentas para quebras de senhas como do Aircrack-NG contra redes sem fio.

O Quadro 4.1 sintetiza as ferramentas utilizadas neste trabalho.

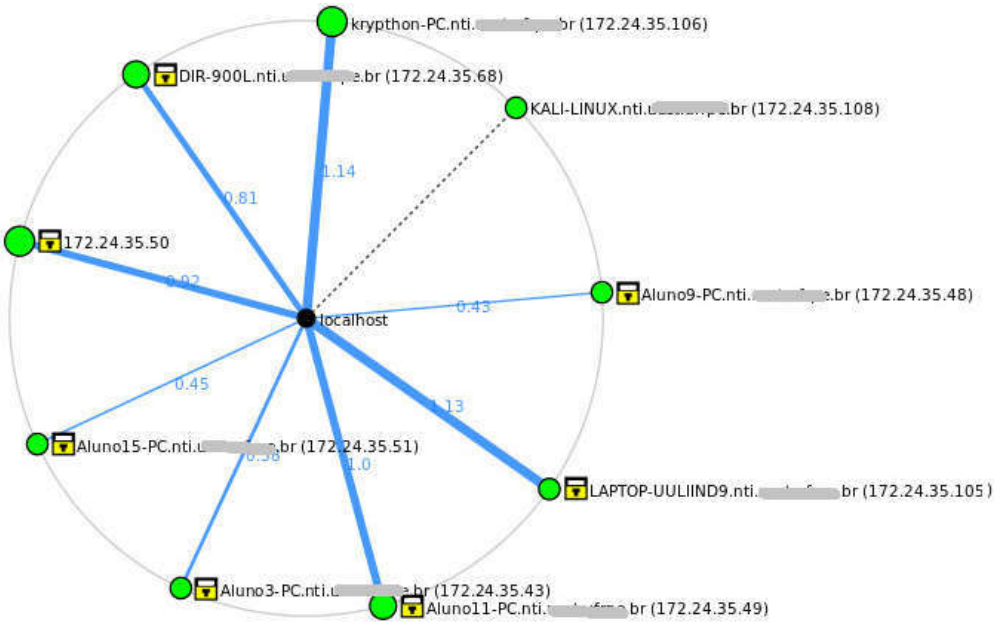
Quadro 4.1 – Quadro de Ferramentas

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

Fonte: Elaborado pelo autor

A Figura 4.3 ilustra um ambiente de teste, onde dispositivos (*smartphones, tablets* e *notebooks*) estão conectados em rede, e que as ferramentas descritas foram aplicadas.

Figura 4.3 – Topologia laboratório alvo de exploração



Fonte: Elaborada pelo autor a partir do Zenmap

5 Resultados

Inicialmente foi realizado teste na rede interna (cabeada) a fim de coletar informações sobre os possíveis alvos. Nesta etapa foram obtidas informações a respeito da rede usadas no processo de análise de vulnerabilidades e que auxiliam posteriormente em uma possível exploração, as ferramentas Nmap e Nbtscan foram utilizadas nesta etapa.

Na Figura 5.1 ilustra a execução do comando *ifconfig* para a descoberta do IP da máquina, o endereço encontrado foi o 172.24.68.162. Na Figura 5.2 executando a varredura simples do Nmap 172.24.68.0/24, em busca de *hosts* ativos, é possível verificar 256 IPs (0 a 255) daquela rede. Foi possível constatar 8 *hosts* ativos naquela rede que correspondiam aos computadores ligados no ambiente que o teste foi realizado, ou seja, em determinado laboratório. O 0/24 indica que foram escaneados todos os *hosts* da rede.

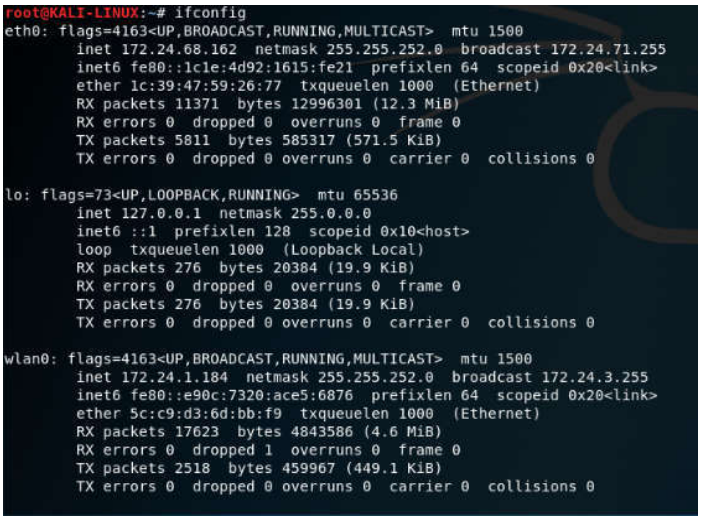
Conforme a Figura 5.3(a) foi utilizada a ferramenta Nbtscan a execução da ferramenta verificou os *hosts* ativos no laboratório onde o teste era realizado, a varredura obteve informações como, por exemplo, o nome da máquina e endereço MAC. A varredura com final 0/24 indica leitura de 256 *hosts*.

Já na Figura 5.3(b), foi preciso de uma leitura maior da rede, já que a instituição possui diversos ambientes como sala de estudos, professores e coordenadores, além dos laboratórios. Logo foi executada varredura com Nbtscan na classe B, o 0/16 indica uma leitura de 65.536 *hosts*, assim foi possível identificar outros IPs ativos na rede.

Através de diversas varreduras feitas pela ferramenta Nbtscan durante períodos do teste foi possível estruturar o quadro com o *range* de IPs e seus supostos ambientes, como é mostrado na Figura 5.4.

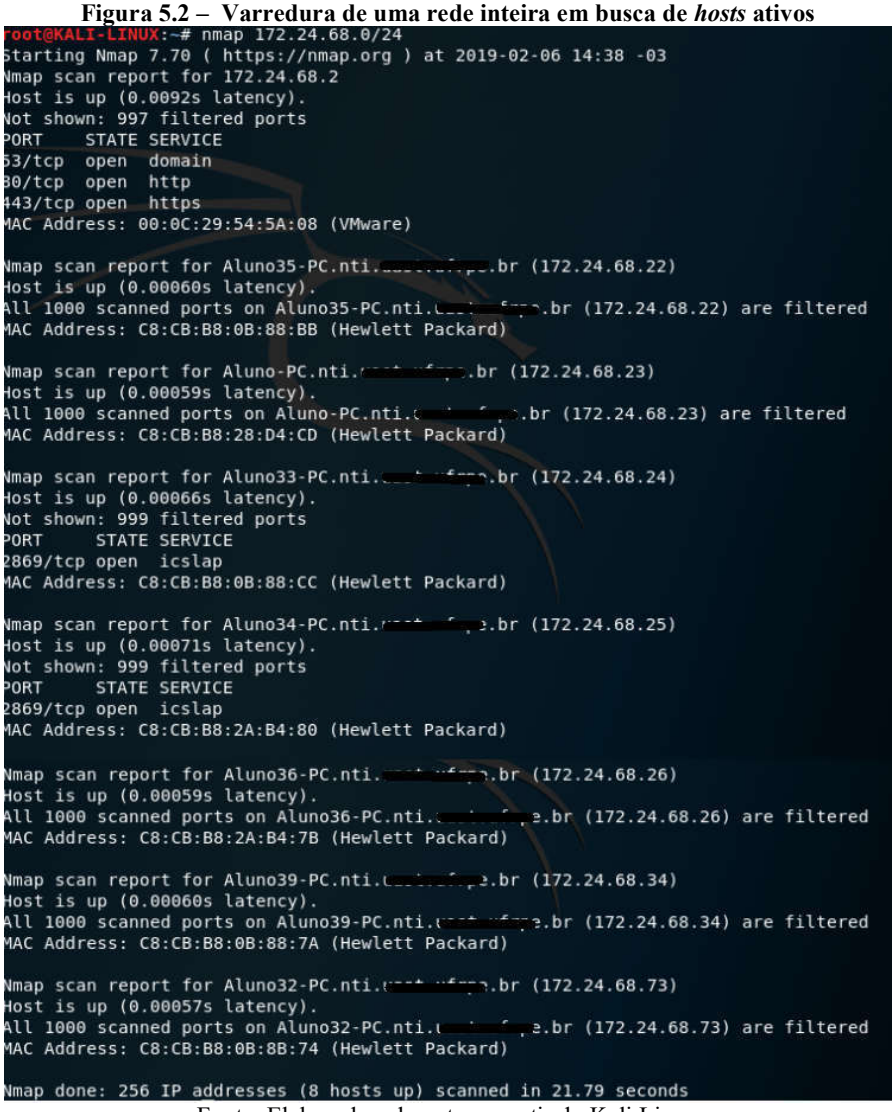
Após a coleta de informações importantes sobre a rede, realizou-se a análise das vulnerabilidades encontradas. As vulnerabilidades encontradas foram enumeradas bem como seus níveis de criticidade.

Figura 5.1 – Comando *ifconfig*



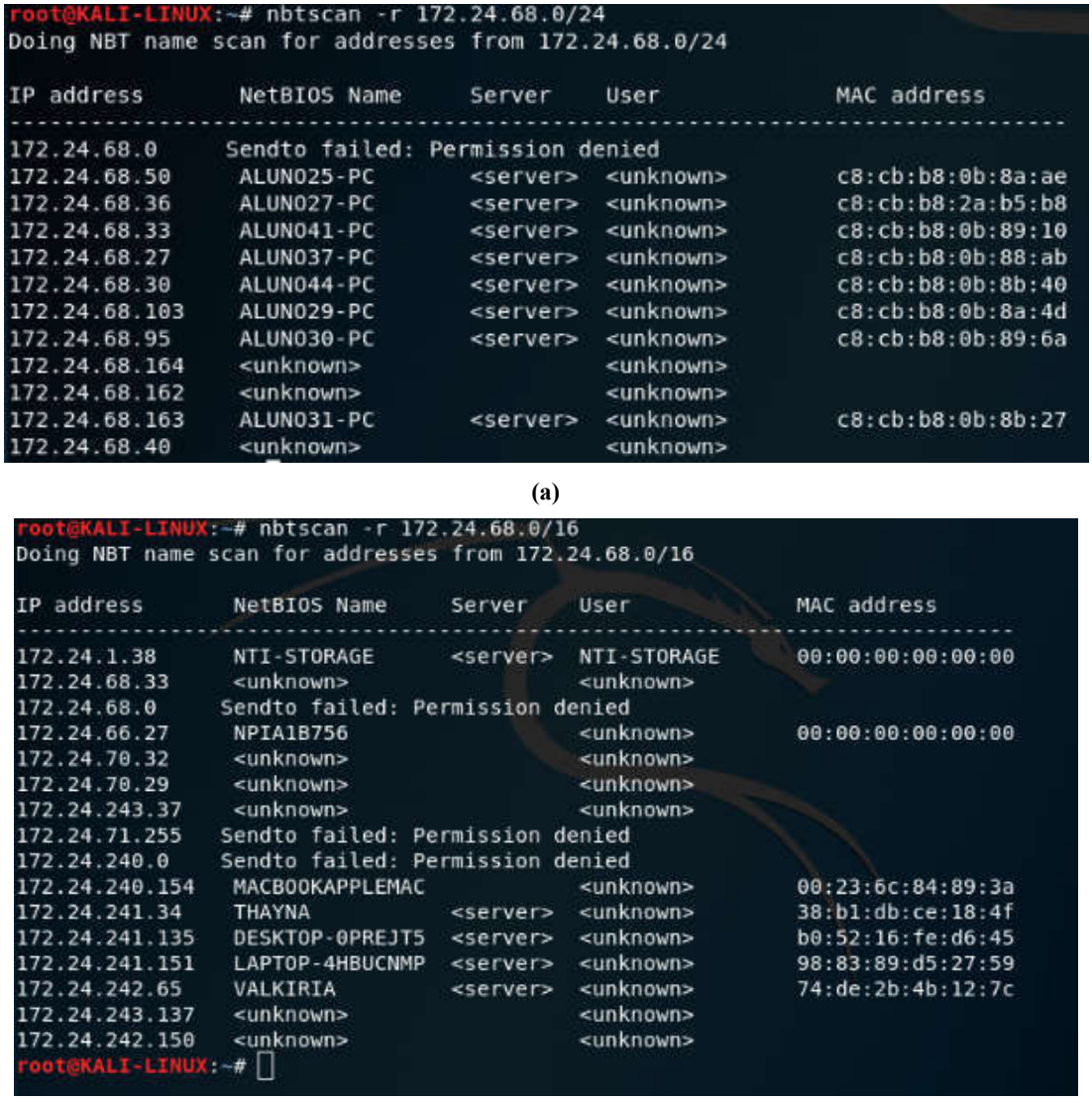
Fonte: Elaborada pelo autor a partir do Kali Linux

Figura 5.2 – Varredura de uma rede inteira em busca de *hosts* ativos



Fonte: Elaborada pelo autor a partir do Kali Linux

Figura 5.3 – Varredura *Nbtscan: (a) CLASSE C (256 hosts); (b) CLASSE B (65.536 hosts)*



```
root@KALI-LINUX:~# nbtscan -r 172.24.68.0/24
Doing NBT name scan for addresses from 172.24.68.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.24.68.0     Sendto failed: Permission denied
172.24.68.50     ALUNO25-PC       <server>  <unknown>        c8:cb:b8:0b:8a:ae
172.24.68.36     ALUNO27-PC       <server>  <unknown>        c8:cb:b8:2a:b5:b8
172.24.68.33     ALUNO41-PC       <server>  <unknown>        c8:cb:b8:0b:89:10
172.24.68.27     ALUNO37-PC       <server>  <unknown>        c8:cb:b8:0b:88:ab
172.24.68.30     ALUNO44-PC       <server>  <unknown>        c8:cb:b8:0b:8b:40
172.24.68.103    ALUNO29-PC       <server>  <unknown>        c8:cb:b8:0b:8a:4d
172.24.68.95     ALUNO30-PC       <server>  <unknown>        c8:cb:b8:0b:89:6a
172.24.68.164    <unknown>                  <unknown>
172.24.68.162    <unknown>                  <unknown>
172.24.68.163    ALUNO31-PC       <server>  <unknown>        c8:cb:b8:0b:8b:27
172.24.68.40     <unknown>                  <unknown>
```

(a)


```
root@KALI-LINUX:~# nbtscan -r 172.24.68.0/16
Doing NBT name scan for addresses from 172.24.68.0/16

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
172.24.1.38      NTI-STORAGE      <server>  NTI-STORAGE      00:00:00:00:00:00
172.24.68.33     <unknown>                  <unknown>
172.24.68.0     Sendto failed: Permission denied
172.24.66.27     NPIA1B756                  <unknown>        00:00:00:00:00:00
172.24.70.32     <unknown>                  <unknown>
172.24.70.29     <unknown>                  <unknown>
172.24.243.37    <unknown>                  <unknown>
172.24.71.255   Sendto failed: Permission denied
172.24.240.0    Sendto failed: Permission denied
172.24.240.154   MACBOOKAPPLEMAC            <unknown>        00:23:6c:84:89:3a
172.24.241.34    THAYNA           <server>  <unknown>        38:b1:db:ce:18:4f
172.24.241.135   DESKTOP-0PREJT5  <server>  <unknown>        b0:52:16:fe:d6:45
172.24.241.151   LAPTOP-4HBUCNMP  <server>  <unknown>        98:83:89:d5:27:59
172.24.242.65    VALKIRIA         <server>  <unknown>        74:de:2b:4b:12:7c
172.24.243.137   <unknown>                  <unknown>
172.24.242.150   <unknown>                  <unknown>
root@KALI-LINUX:~#
```

(b)

Fonte: Elaborada pelo autor a partir do Kali Linux

Figura 5.4 – Lista de IPs

Host	Local
172.24.0.0/24	**Não identificado**
172.24.1.0/24	NTI-STORAGE/SERVIDORES/WIRELESS
172.24.3.0/24	**Não identificado**
172.24.4.0/24	NTI
172.24.5.0/24	IMPs
172.24.6.0/24	DESKTOPs/IMPRESSORAS
172.24.7.0/24	NTI/DESKTOPs/IMP-DIR-GERAL&COORD-GERAL
172.24.8.0/24	IMPs/WIRELESS
172.24.12.0/24	DESKTOPSs/
172.24.15.0/24	IMP-DOC3/WIRELESS
172.24.16.0/24	IMP-CASA
172.24.32.0/24	LABORATÓRIO/_gateway
172.24.33.0/24	KALI-LINUX
172.24.34.0/24	LABORATÓRIO
172.24.35.0/24	LABORATÓRIO
172.24.36.0/24	**Não identificado**
172.24.39.0/24	PROFESSOR
172.24.47.0/24	IMP-BIBLIOTECA
172.24.51.0/24	**Não identificado**
172.24.54.0/24	IMP-BIBLIOTECA
172.24.64.0/24	DESKTOP-LETRAS
172.24.66.0/24	**Não identificado**
172.24.68.0/24	LABORATÓRIO
172.24.70.0/24	LABORATÓRIO
172.24.71.0/24	IMPs
172.24.74.0/24	**Não identificado**
172.24.75.0/24	IMP-DOCT/DESKTOPs
172.24.101.0/24	PROFESSORES/WIRELESS
172.24.103.0/24	IMPs-COORDENAÇÃO
172.24.123.0/24	IMP-APOIO&COORD-GERAL
172.24.124.0/24	IMPs/WIRELESS
172.24.127.0/24	IMPs
172.24.128.0/24	IMPs/WIRELESS
172.24.129.0/24	IMPs
172.24.130.0/24	IMPs/WIRELESS
172.24.131.0/24	IMP-PROTOCOLO/IMP-ADMIN/DIR.ADMIN/IMPs
172.24.240.0/24	PROFESSORES/WIRELESS/_gateway
172.24.241.0/24	PROFESSORES/WIRELESS
172.24.242.0/24	PROFESSORES/WIRELESS
172.24.243.0/24	COORDENAÇÃO/WIRELESS

Fonte: Elaborada pelo autor

Scanners de vulnerabilidades são ferramentas valiosas, principalmente porque a maioria dos testes de invasão é realizada em um período menor do que se gostaria de ter. Para a análise das vulnerabilidades foi utilizado a ferramenta Nessus, classificando as vulnerabilidades de acordo com o *Common Vulnerability Scoring System* (CVSS), versão 2,

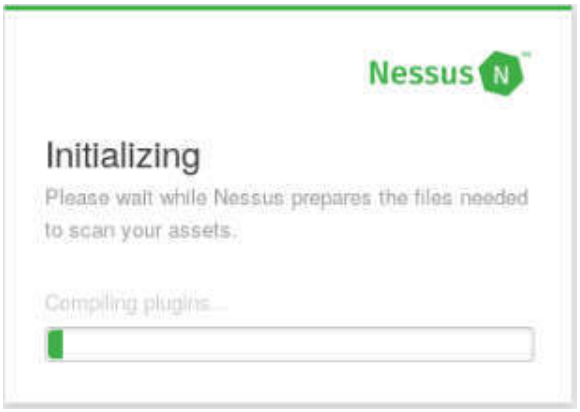
da *National Institute of Standards and Technology* (NIST), que calcula o impacto da vulnerabilidade caso seja explorado.

A ferramenta é iniciada através do comando */etc/init.d/nessusd start*, ilustrado na Figura 5.5. O Nessus é acessado via *Web* através do endereço http://localhost:8834/, após isso será iniciado (Figura 5.6), depois é solicitado a autenticação da conta (Figura 5.7).

Figura 5.5 – Iniciando o Nessus

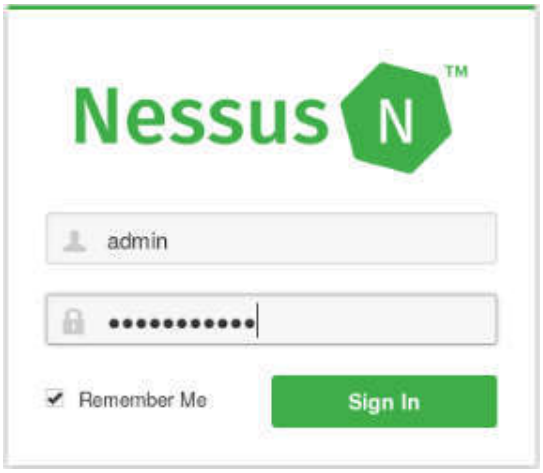
Fonte: Elaborada pelo autor a partir do Kali Linux

Figura 5.6 – Inicializando o Nessus



Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Figura 5.7 – Login do Nessus na interface *Web*

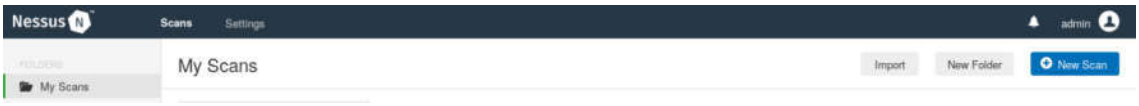


Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Para que o escaneamento fosse iniciado, foi necessária a criação de *scans* (Figura 5.8 e 5.9), criados a partir da lista de IPs estruturada na Figura 5.4.

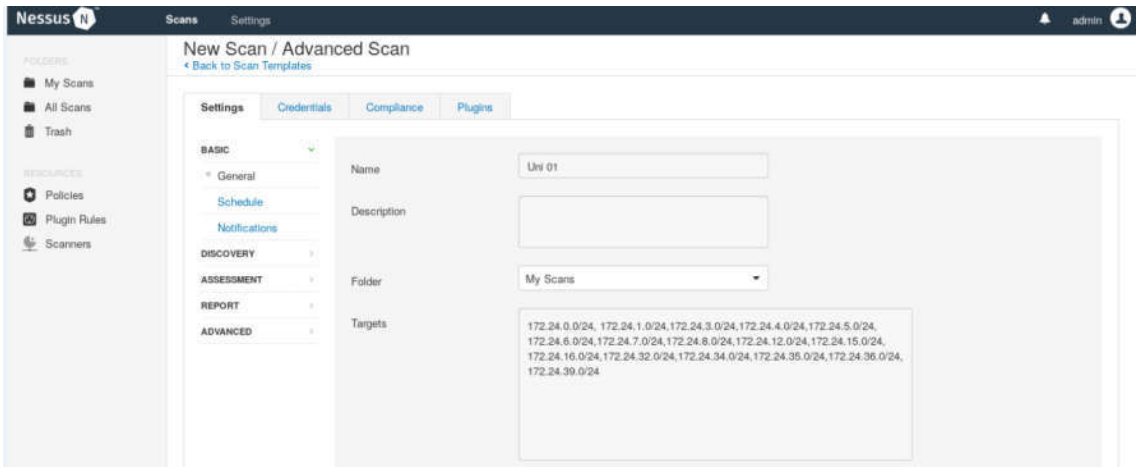
Depois de criados 3 *scans*, foi iniciado o *Scanning* (Figura 5.10), Uni 01, Uni 02 e Uni 03 com 16, 16 e 8 IPs, respectivamente.

Figura 5.8 – Criando um novo *scan* em *New Scan*



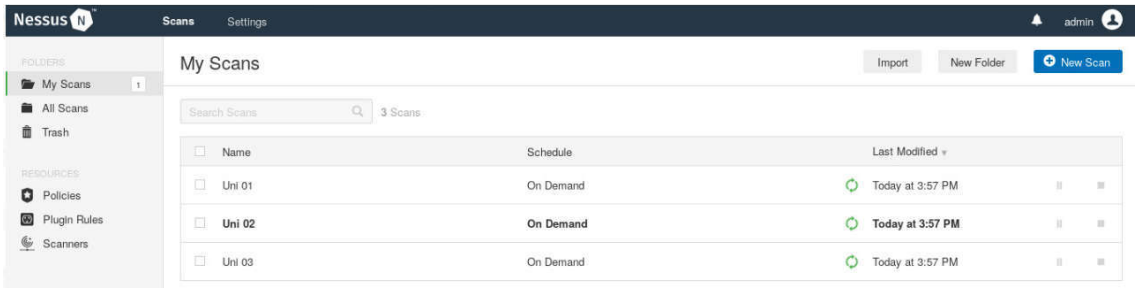
Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Figura 5.9 – Criação novo *scan* em modo avançado



Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Figura 5.10 – Executando *Scanning*

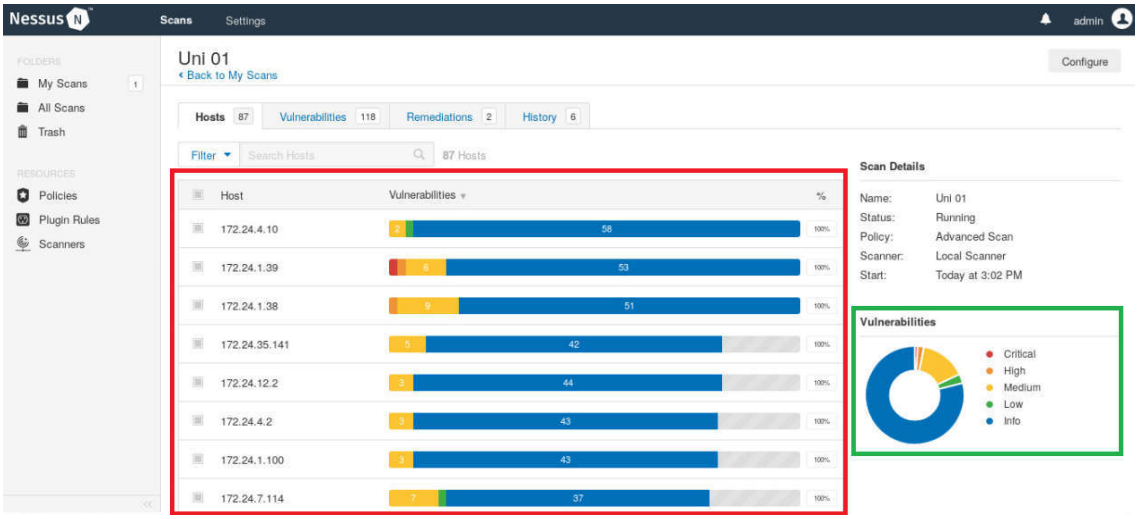


Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Na Figura 5.11 têm-se uma visão geral em um dos *scans* e a quantidade de vulnerabilidades encontradas por *host* (destacado em vermelho) e as encontradas em todo o *scan* (destacado em verde).

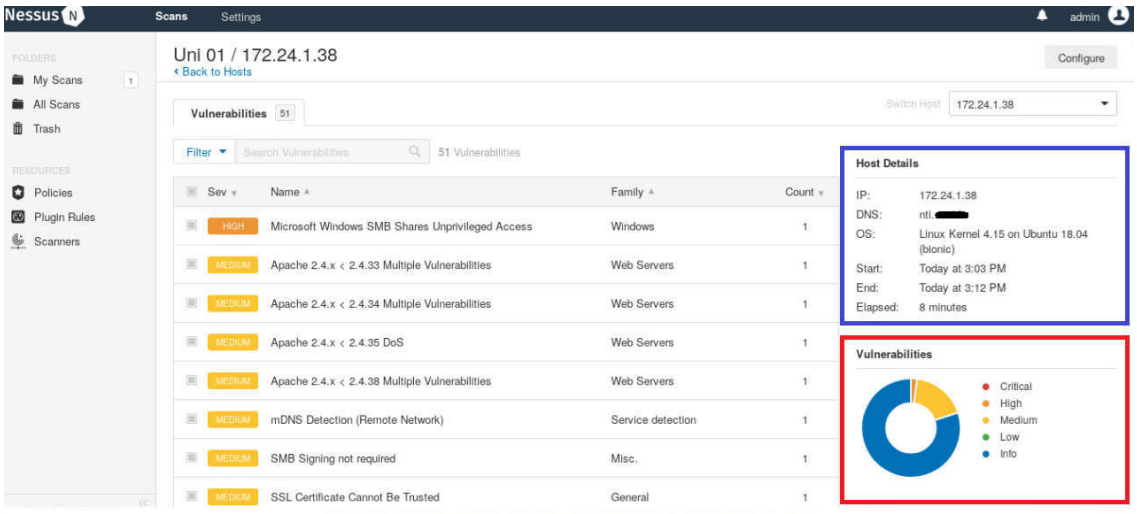
Na Figura 5.12, no *host* 172.24.1.38, é possível obter informações como o nome de DNS e Sistema Operacional Ubuntu do Kernel Linux (destaque azul). Além das vulnerabilidades encontradas naquele *host* (em vermelho). Na Figura 5.13 detalha-se uma das vulnerabilidades do escaneamento como descrição e solução (em verde), módulos *exploits* disponíveis (em vermelho) e o CVE referente a vulnerabilidade (em azul).

Figura 5.11 – Visão geral do escaneamento



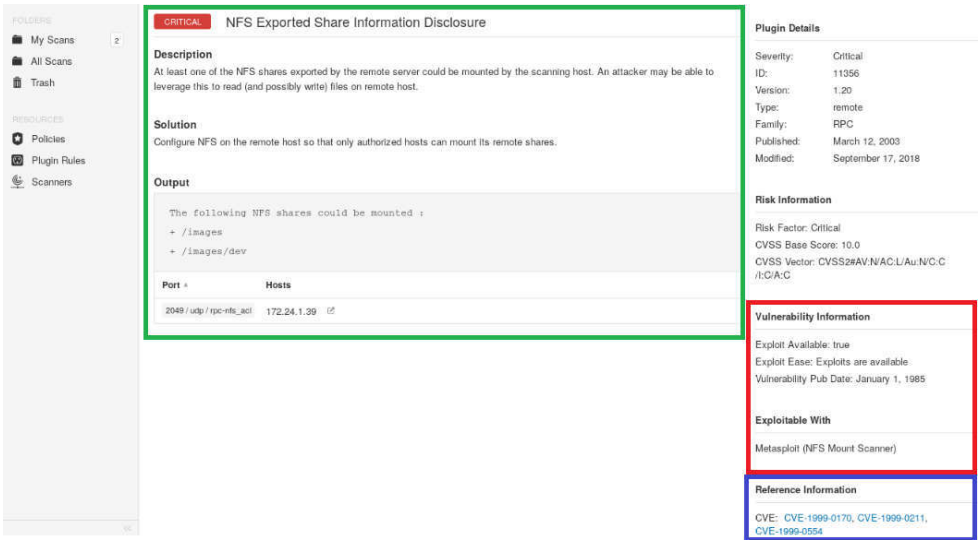
Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Figura 5.12 – Vulnerabilidades encontradas em um host



Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

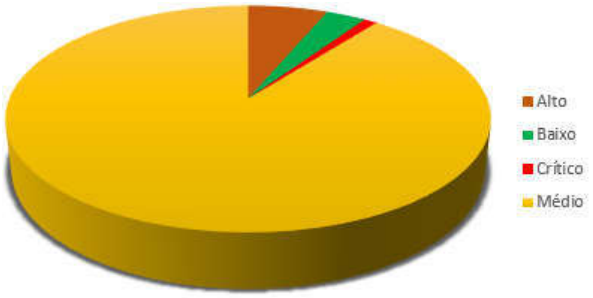
Figura 5.13 – Descrição de vulnerabilidade encontrada



Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

A partir das vulnerabilidades encontradas nos *scans* realizados, foi apresentada uma tabela das vulnerabilidades (Apêndice B), gráfico do total de vulnerabilidades por criticidade (Figura 5.14) e a quantidade de vezes que cada vulnerabilidade foi encontrada (Figura 5.15).

Figura 5.14 – Total de Vulnerabilidades por criticidade



Nível	Quant	%
Crítico	1	1,1%
Alto	6	6,3%
Médio	85	89,5%
Baixo	3	3,2%
Total	**95**	**100%**

Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

Uma vez realizado o levantamento de informações sobre a rede, análise das vulnerabilidades e mapeamento dos seus tipos, foi verificada a possibilidade de exploração. Para este processo a utilização de *exploits* da ferramenta Metasploit foi necessária, a única vulnerabilidade nível crítico encontrada no ambiente NFS *Exported Share Information Disclosure* no *host* 172.24.1.39 (Figura 5.13, em vermelho) informa que há *exploit* disponível *NFS Mount Scanner* no Metasploit. Pode-se ainda realizar uma pesquisa através das referências (em azul) da vulnerabilidade no *Common Vulnerabilities and Exposures* (CVE) a

fim de encontrar mais *exploits* em *sites* como Rapid7 Database[16], Packet Storm[17], Exploit Database[18], CVE Details[19] e Google[20].

Figura 5.15 – Vulnerabilidades por nível de criticidade

Nível	Quantidade
Alto	**6**
Microsoft Windows SMB Shares Unprivileged Access	1
NFS Share User Mountable	1
PHP 7.2.x < 7.2.13 Arbitrary Command Injection Vulnerability	2
PHP 7.2.x < 7.2.14 Multiple vulnerabilities	2
Baixo	**3**
DHCP Server Detection	1
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	1
Web Server HTTP Header Internal IP Disclosure	1
Crítico	**1**
NFS Exported Share Information Disclosure	1
Médio	**85**
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	1
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	3
Apache 2.4.x < 2.4.35 DoS	4
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	4
DNS Server Cache Snooping Remote Information Disclosure	1
HTTP TRACE / TRACK Methods Allowed	3
mDNS Detection (Remote Network)	3
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	1
Network Time Protocol (NTP) Mode 6 Scanner	11
NFS Shares World Readable	1
OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	1
OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities	1
OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	1
PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	2
PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF	2
SMB Signing not required	8
SSL Certificate Cannot Be Trusted	16
SSL Certificate Signed Using Weak Hashing Algorithm	2
SSL Certificate Validity - Duration	1
SSL Certificate with Wrong Hostname	2
SSL Self-Signed Certificate	15
Tenable Nessus < 8.0.0 Multiple Vulnerabilities (TNS-2018-14)	1
Tenable Nessus < 8.1.1 Multiple Vulnerabilities (TNS-2018-16)	1
Total Geral	**95**

Fonte: Elaborada pelo autor a partir da Ferramenta Nessus

[16] Disponível em https://www.rapid7.com/db/

[17] Disponível em https://packetstormsecurity.com/

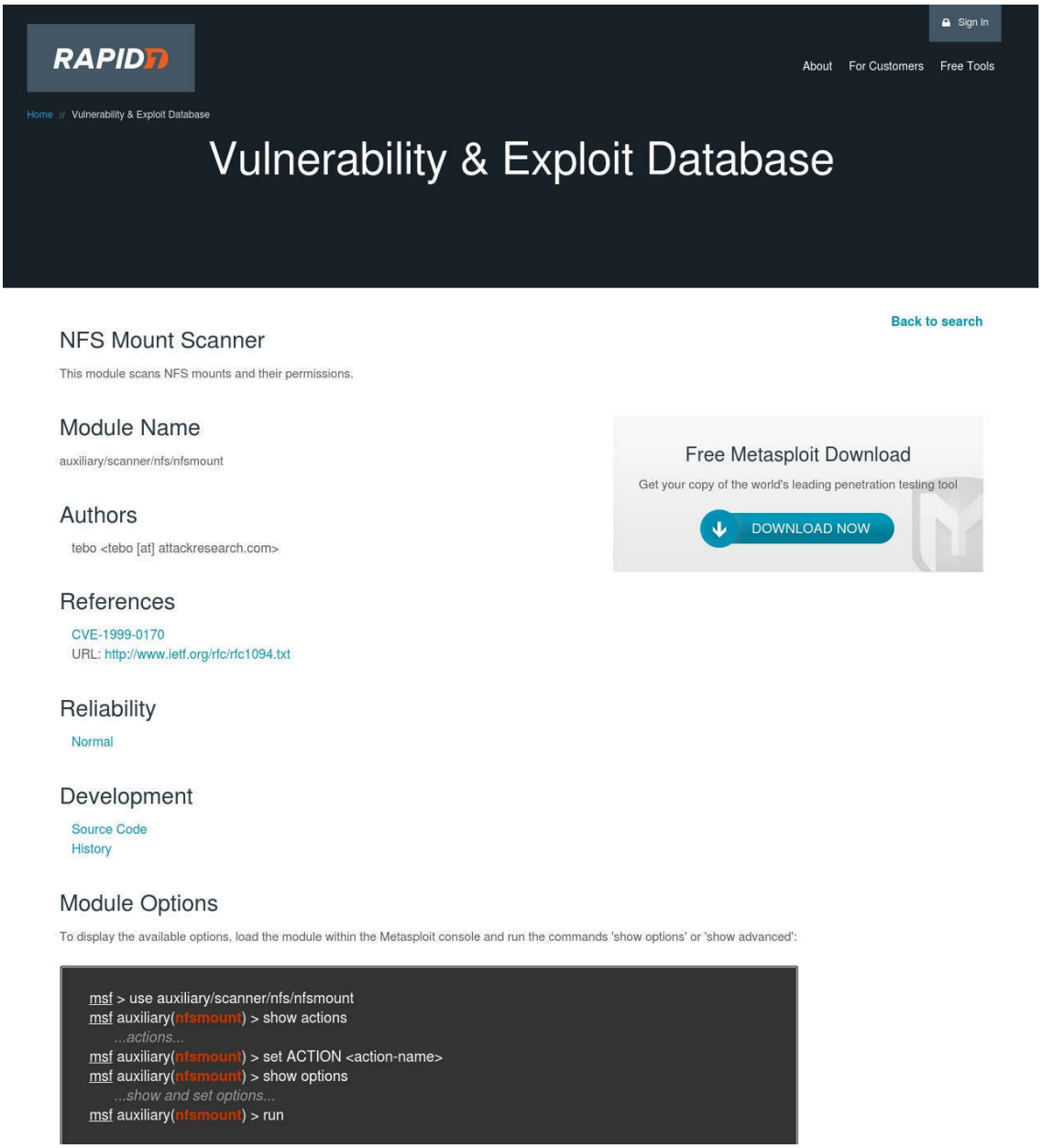
[18] Disponível em https://www.exploit-db.com/

[19] Disponível em https://www.cvedetails.com/

[20] Disponível em https://www.google.com.br/

A Figura 5.16 ilustra a pesquisa no *site* Rapid7 Database na vulnerabilidade pelo código CVE-1999-0170, na qual se encontrou o módulo *NFS Mount Scanner* do Metasploit que foi informado pelo Nessus.

Figura 5.16 – Pesquisa no site Rapid7 DB da vulnerabilidade



Fonte: Rapid7 Database

O serviço do banco de dados Postgresql foi iniciado para monitorar o Metasploit, e fazer com que a busca por *exploits* fosse mais ágil, logo em seguida foi iniciada a própria ferramenta, conforme ilustrado na Figura 5.17. O console é iniciado através do comando *msfconsole* (Figura 5.18).

Figura 5.17 – Iniciando os serviços

```
root@KALI-LINUX:~# service postgresql start
root@KALI-LINUX:~# service metasploit start
```

Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Figura 5.18 – Abrindo console do Metasploit

Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Foi realizada a pesquisa no Metasploit de *exploits* para vulnerabilidade encontrada no Nessus no *host* 172.24.1.39 (Figura 5.13) descrita como *NFS Exported Share Information Disclosure* e **de nível crítico**, o módulo é o *NFS Mount Scanner* uma vulnerabilidade classificada no Nessus como nível crítico, pesquisa Metasploit ilustrada na Figura 5.19.

Figura 5.19 – Pesquisando módulo vulnerabilidade NSF MOUNT

```
msf5 > search nfsmount

Matching Modules
================

   Name                              Disclosure Date  Rank    Check  Description
   ----                              ---------------  ----    -----  -----------
   auxiliary/scanner/nfs/nfsmount                     normal  Yes    NFS Mount Scanner
```

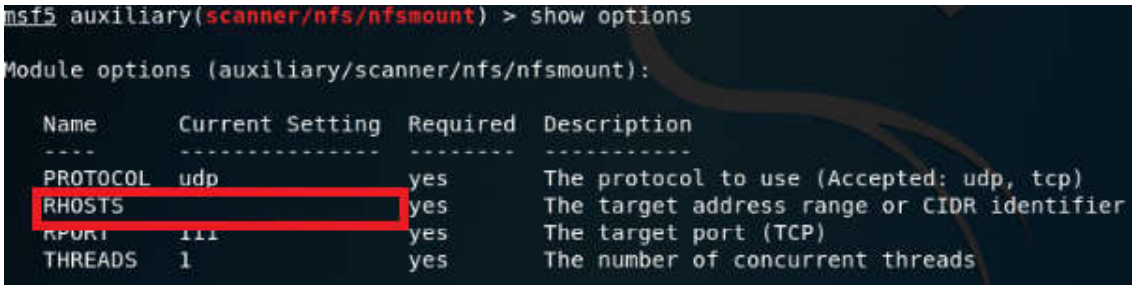
Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Este é um módulo auxiliar, não permitindo controlar o alvo, mas apresenta informações sobre o mesmo e confirma a vulnerabilidade existente. Na Figura 5.20 o *exploit* é selecionado para execução e na Figura 5.21 são mostradas as opções do *exploit*, enquanto na Figura 5.22 é definido o *host* remoto alvo.

Figura 5.20 – Selecionando o *exploit*, assim a interface o console é alterada

Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Figura 5.21 – Opções do módulo auxiliar NSF *MOUNT*



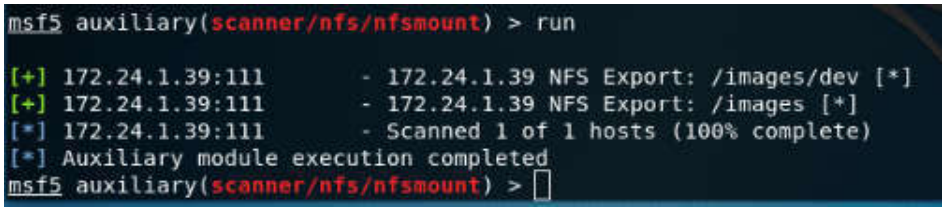
Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Figura 5.22 – Definindo o *host* alvo

Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Na Figura 5.23 têm-se as informações exibidas pela execução do módulo *exploit*, possivelmente um servidor para armazenamento de imagens.

Figura 5.23 – Executando o *exploit*



Fonte: Elaborada pelo autor a partir da Ferramenta Metasploit

Dentre as vulnerabilidades de nível alto encontradas, têm-se:

- *Microsoft a Windows SMB Shares Unprivileged Access* que permite acesso às pastas compartilhadas pelo *host* alvo, provavelmente pastas estas que tem permissão proposital pelo administrador da rede. Não existem *exploits* disponíveis para esta vulnerabilidade, pesquisa no CVE Details, assim a vulnerabilidade *PHP 7.2.x < 7.2.14 Multiple vulnerabilities* não possui *exploits* relatados.
- *PHP 7.2.x < 7.2.13 Arbitrary Command Injection Vulnerability* possui *exploits* apenas para o alvo Linux. Mas o alvo em questão possui sistema operacional *Microsoft Windows*.

Foram encontradas 85 vulnerabilidades de **nível médio** (Figura 5.24), representando 89,5%. Destas, 19 possuem *exploits* com módulos auxiliares, 1 possui *exploit* pago, 47 não possuem relatados e 18 não foram encontradas mais informações.

Figura 5.24 – Vulnerabilidades nível médio

Nível	Quantidade
Médio	**85**
Exploit Auxiliares/Scanner	**19**
Network Time Protocol (NTP) Mode 6 Scanner	11
SMB Signing not required	8
Exploits Pagos	**1**
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	1
Não Existem Exploits Relatados	**47**
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	1
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	3
Apache 2.4.x < 2.4.35 DoS	4
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	4
DNS Server Cache Snooping Remote Information Disclosure	1
HTTP TRACE / TRACK Methods Allowed	3
mDNS Detection (Remote Network)	3
NFS Shares World Readable	1
OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	1
OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities	1
OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	1
PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	2
PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF	2
SSL Certificate Cannot Be Trusted	16
SSL Certificate Signed Using Weak Hashing Algorithm	2
Tenable Nessus < 8.0.0 Multiple Vulnerabilities (TNS-2018-14)	1
Tenable Nessus < 8.1.1 Multiple Vulnerabilities (TNS-2018-16)	1
Não Foram Encontradas + informações	**18**
SSL Certificate Validity - Duration	1
SSL Certificate with Wrong Hostname	2
SSL Self-Signed Certificate	15
Total Geral	**85**

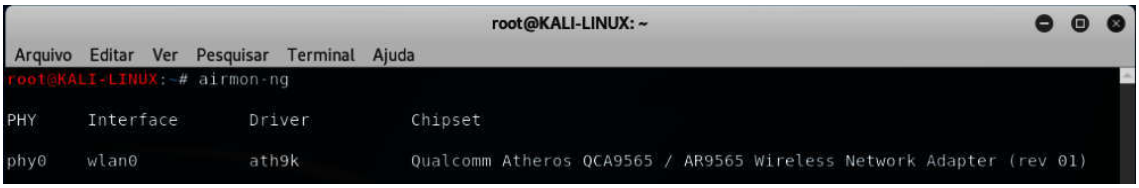
Fonte: Elaborada pelo autor

Dentre as vulnerabilidades de nível baixo encontradas, nenhuma das vulnerabilidades possui módulos *exploits* relatados até o momento da conclusão deste trabalho.

Para a etapa de exploração da rede *Wireless* foi utilizado o conjunto de ferramentas do Aircrack-ng, através do método de força bruta para quebra de senhas. Foi usada uma *wordlist* no processo de quebra de senhas.

Na Figura 5.25 verifica-se a interface de rede na máquina que está realizando o teste, na Figura 5.26 finalizando todos os processos que podem interferir neste momento e para iniciar o modo monitor, na Figura 5.27 o modo permite capturar o tráfego destinado na rede.

Figura 5.25 – Verificando a interface de rede *Wireless*



Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Figura 5.26 – Finalizando todos os processos

Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

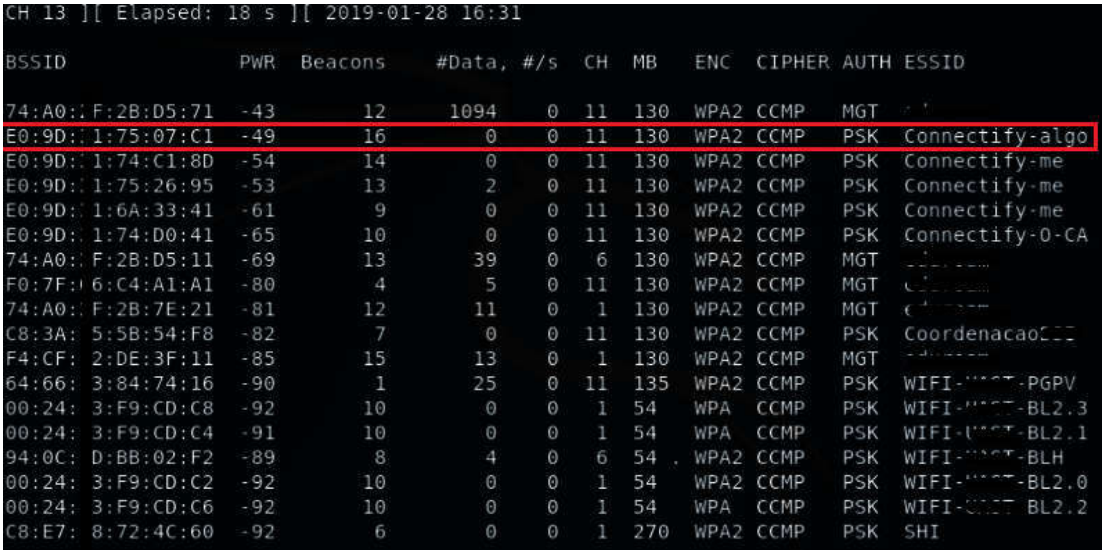
Figura 5.27 – Iniciando o modo monitor da interface

Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Após iniciar o modo monitor, executou-se o comando para detectar pontos de acesso disponíveis (Figura 5.28(a)) e os pontos disponíveis (Figura 5.28 (b)). Escolhendo a rede, se fez necessário as informações do BSSID e CH, endereço MAC do roteador e o canal de transmissão de dados, respectivamente.

Figura 5.28 – Aircrack-ng: (a) Detectando pontos de acesso *Wireless* e (b) Pontos de acesso

(a)



(b)

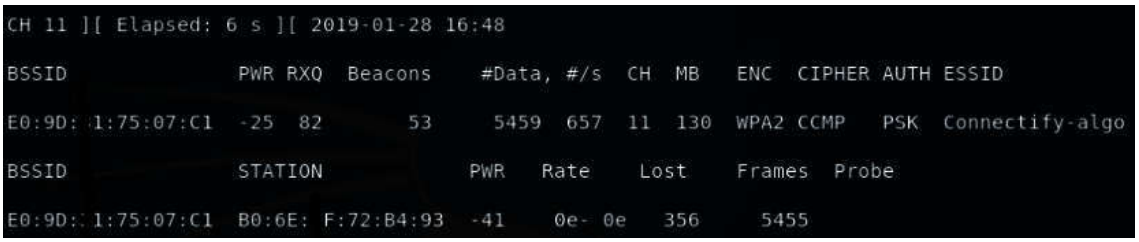
Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Na rede escolhida Connectify-algo, com BSSID E0:9D:31:75:07:C1 e CH 11, iniciou-se a captura conforme ilustrado na Figura 5.29, os dados da captura foram salvos no arquivo algo, conforme ilustrado na Figura 5.30 têm-se os dados a serem capturados e para isso que isso acontecesse foi necessário que algum dispositivo (computadores, *smartphones* ou *tablets*) fizesse autenticação na rede para que o *WPA Handshake* fosse capturado. Logo foi necessário forçar a desautenticação dos dispositivos na rede (Figura 5.31), ao realizar uma nova autenticação o *WPA Handshake* foi capturado, conforme ilustrado na Figura 5.32.

Figura 5.29 – Iniciando captura

Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Figura 5.30 – Capturando os dados da redes



Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Figura 5.31 – Desautenticação os usuários da rede para que eles reconectem

Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Figura 5.32 – WPA *Handshake* capturado

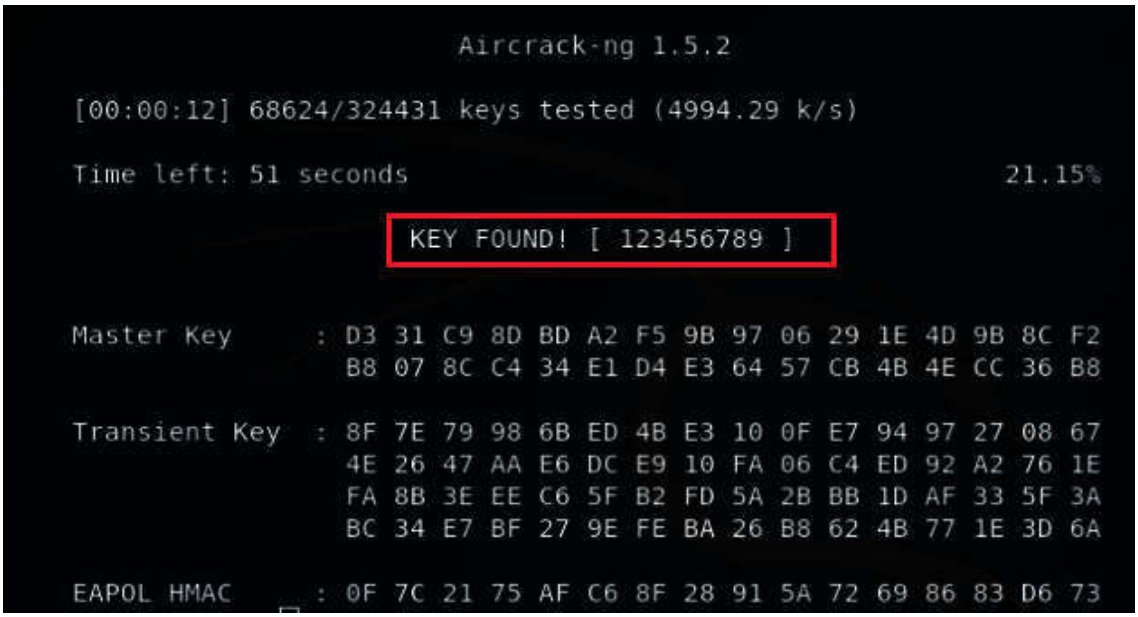
Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

A partir da captura do *WPA Handshake*, iniciou-se o processo de quebra de senha, fazendo uso de uma *wordlist* previamente montada (Figura 5.33), e assim obteve-se a senha do ponto de acesso localizada na Figura 5.34.

Figura 5.33 – Iniciando a quebra de senha com a *wordlist* e informações capturadas no WPA *Handshake*

Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

Figura 5.34 – Senha encontrada



Fonte: Elaborada pelo autor a partir da Ferramenta Aircrack-ng

5.1 Considerações Finais

Após a realização dos testes, é perceptível que mesmo que a Instituição possua uma equipe de técnicos responsáveis pela manutenção dos ativos tecnológicos ainda assim é possível identificar inúmeras vulnerabilidades presentes no ambiente no qual foi realizado.

Com isso se faz necessário executar periodicamente testes com o intuito de identificar, mapear e corrigir quaisquer que sejam as falhas encontradas. Impossibilitando que pessoas mal-intencionadas se aproveitem das mesmas.

Dentre as vulnerabilidades encontradas classificadas em nível crítico, alto, médio e baixo, dentre estas maiores representadas pelas vulnerabilidades de nível **médio** que correspondem a 89,5%, seguido de 6,3% de nível **alto**, 3,2% de nível **baixa** e 1,1% de nível **crítico**.

Foi feito o levantamento sobre como explorar as vulnerabilidades, mas essas, em sua maioria, não possuem módulos de *exploits* no Metasploit relatados. As demais possuem apenas módulos auxiliares que permitem ao atacante confirmar a vulnerabilidades, foi feito um mapeamento com descrição e possíveis soluções para as vulnerabilidades, descritos no Apêndice A deste trabalho.

Foram realizados testes *Wireless* para quebra de senhas, no qual foi possível facilmente encontrar senhas de pontos de acesso de terceiros, estes em sua maioria com senhas muito fracas e que uma pessoa mal-intencionada pode usar como meio de entrar na rede e assim utilizar de meios para aumentar sua exploração no ambiente.

6 Conclusão

6.1 Considerações Finais

Apesar da maior limitação durante a realização deste trabalho ter sido o tempo, identificaram-se inúmeros tipos de falhas da quais que foram classificadas em seu nível de criticidade, resultando em um mapeamento com um breve detalhamento das vulnerabilidades.

Dentre as vulnerabilidades encontradas não foi possível realizar maiores ataques, uma vez que as vulnerabilidades encontradas, em sua maioria, não possuem módulos *exploits* relatados na literatura pesquisada. Aponta-se apenas a existência de módulos auxiliares que servem para confirmar a existência de uma vulnerabilidade e o seu respectivo nível crítico, mas sem ganho de acesso ao alvo.

Por fim, destaca-se a vulnerabilidade da rede *Wireless*, em que foi possível verificar a facilidade do invasor adentrar a rede interna da Instituição. Em conversa informal com alguns usuários do serviço, estes apontaram desconhecer a possibilidade de um ataque por essa vulnerabilidade e/ou desconhecem quaisquer regras de proteção a este tipo de rede.

6.2 Contribuições da Monografia

Este trabalho teve como contribuições principais difundir técnicas de segurança, como os testes de invasão para que vulnerabilidades possam ser encontradas, descrevendo-as e definindo-as sob que níveis podem afetar uma organização.

Os resultados serão compartilhados ao setor de segurança responsável, no intuito de contribuir com a segurança da informação da Instituição.

A metodologia empregada e as recomendações para vulnerabilidades encontradas poderão servir de referencial teórico-prático para futuras pesquisas.

6.3 Trabalhos Futuros

Para trabalhos futuros, sugere-se a realização de novos testes:

- Na instituição com um maior período de testes utilizando-se de um maior número de ferramentas, podendo-se fazer um comparativo para verificar qual a maior eficácia de cada ferramenta;
- Dispositivos móveis com foco em sistemas *Android*, visto que estes estão presentes em ambientes em grandes números em ambientes institucionais;
- Em sistemas *Web*, principalmente em instituições de ensino que usam o gerenciamento acadêmico e de informações; e
- De Engenharia Social usando técnicas que exploram a fraqueza humana, utilizando-se ou não de tecnologias.

REFERÊNCIAS

ALERTA SECURITY. **Entenda já o aumento no investimento em segurança da informação.** [S. l.], 2017. Disponível em: <https://alertasecurity.com.br/blog/202-entenda-ja-o-aumento-no-investimento-em-seguranca-da-informacao>. Acesso em: 20 nov. 2018.

BUZZATTE, P. M. Análise de Vulnerabilidades Através de Scanners Detectores. 2014. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) - Universidade Federal de Santa Maria, Santa Maria, 2014.

CRUZ, C. M. B. R. Auditoria de Segurança da Informação em Sistemas e Aplicações. 2017. Dissertação (Mestre em Computação Aplicada) - Universidade de Brasília, Brasília, 2017.

DELGADO, V. M. S.; SANTTOS, W. M. O. Estudos de Testes de Penetração. 2011. Iniciação à Pesquisa (Engenheiro da Computação) - Instituto Militar de Engenharia, Rio de Janeiro, 2011.

DOMINGUES, D. E. R. Testes de Invasão em Ambiente Corporativo. 2012. Trabalho de Conclusão de Curso (Especialista em Perícia Digital) - Universidade Católica de Brasília, Brasília, 2012.

FEDERAL OFFICE FOR INFORMATION SECURITY (BSI). **Study: A Penetration Testing Model.** Bonn, 2003. Disponível em: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile&v=1>. Acesso em: 21 nov. 2018.

GIAVAROTO, S. C. R.; SANTOS, G. R. D. **Backtrack Linux - Auditoria e Teste de Invasão em Redes de Computadores.** Rio de Janeiro: Editora Ciência Moderna, 2013.

HINTZBERGEN, J.; HITNTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de segurança da informação.** Tradução Alan de Sá. Rio de Janeiro: Brasport Editora, 2018.

INOVA DADOS, Blog. **4 Motivos para investir na segurança da informação da sua empresa.** [S. l.], 2017. Disponível em: <https://inovedados.com.br/investir-na-seguranca-da-informacao>. Acesso em: 19 out. 2018.

LEPESQUEUR, A.M.A.; OLIVEIRA, I. D. R. Pentest, Análise e Mitigação de Vulnerabilidades. 2012. Monografia (Engenheiro em Redes de Comunicação) - Universidade de Brasília, Faculdade de Tecnologia, Distrito Federal, 2012.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers expostos 7: Segredos e soluções para a segurança de redes.** Tradução João Eduardo Nóbrega Tortello. 7. ed. São Paulo: Bookman Editora, 2014.

MORENO, D. **Introdução ao Pentest.** 1. ed. São Paulo: Novatec Editora, 2015.

_____. **Pentest em Redes Sem Fio.** 1. ed. São Paulo: Novatec Editora, 2016.

NAREZZI, R. **Sem cibersegurança, instituições de ensino serão alvos fáceis.** Inoveduc Folha Dirigida [S. l.], 2017. Disponível em: <http://inoveduc.com.br/ciberseguranca-e-ciberataques-em-instituicoes-de-ensino/>. Acesso em: 2 nov. 2018.

NUNES, R. O. **Man In The Middle.** beBee producer [S. l.], 2017. Disponível em: < https://www.bebee.com/producer/@renata-oliveira-nunes-06wVjc/man-in-the-middle>. Acesso em: 20 out. 2018.

PSAFE. **Relatório da Segurança Digital no Brasil.** dfndr lab. [S. l.], 2018. Disponível em: <https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf>. Acesso em: 20 out. 2018.

SANTOS, R. **O setor de educação é um dos mais vulneráveis a ataques de segurança.** Ti Inside Online Segurança. [S. l.], 2017. Disponível em: <http://tiinside.com.br/tiinside/seguranca/artigos-seguranca/11/07/2017/o-setor-de-educacao-e-um-dos-mais-vulneraveis-ataques-de-seguranca/>. Acesso em: 2 nov. 2018.

SOMMERVILLE, I. **Engenharia de Software.** Tradução Selma Shin Shimuzu Melnikoff, Reginaldo Arakaki, Edilson de Andrade Barbosa. São Paulo: Pearson Addison Wesley, 2007.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas.** Rio de Janeiro: Elsevier, 2005.

_____. **Criptografia e Segurança de Redes: Princípios e Práticas.** Tradução Daniel Vieira. São Paulo: Pearson Education do Brasil, 2015.

_____; BROWN, L. **Segurança de Computadores: Princípios e Práticas.** Rio de Janeiro: Elsevier, 2008.

VIEIRA, Y. D. B. Utilização de Pentest na Prevenção de Ataques Cibernéticos às Organizações. 2018. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Universidade Federal Rural de Pernambuco, Serra Talhada, 2018.

WACK, J.; TRACY, M.; SOUPPAYA, M. Guideline on Network Security Testing. Washington: [s. n.], 2008.

WEIDMAN, G. **Testes de Invasão: Uma Introdução Prática ao Hacking.** São Paulo: Novatec Editora, 2014.

ZANI, B. **O gerenciamento da segurança da informação em escolas e universidades.** Ti Inside Online Segurança. [S. l.], 2014. Disponível em: <http://tiinside.com.br/tiinside/seguranca/artigos-seguranca/16/12/2014/o-gerenciamento-da-seguranca-da-informacao-em-escolas-e-universidades/>. Acesso em: 21 out. 2018.

APÊNDICE A – Recomendações para Vulnerabilidades Encontradas

Quadro A.1 – Sugestões de Recomendações para as vulnerabilidade encontradas

Nível	Vulnerabilidade	Recomendação	Quantidade
Crítico	NFS Exported Share Information Disclosure	Configure o NFS no *host* remoto para que somente *hosts* autorizados possam montar seus compartilhamentos remotos.	1
Alto	Microsoft Windows SMB Shares Unprivileged Access	Para restringir o acesso no Windows, abra o Explorer, clique com o botão direito em cada compartilhamento, vá para a guia "compartilhamento" e clique em 'permissões'.	1
Alto	NFS Share User Mountable	Configure o NFS no *host* remoto para que somente os *hosts* autorizados possam montar os compartilhamentos remotos. O NFS remoto servidor deve evitar solicitações de montagem originadas de uma porta não privilegiada.	1
Alto	PHP 7.2.x < 7.2.13 Arbitrary Command Injection Vulnerability	Atualize versão do PHP para 7.2.13 ou superior.	2
Alto	PHP 7.2.x < 7.2.14 Multiple vulnerabilities	Atualize versão do PHP para 7.2.14 ou superior.	2
Médio	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Atualize a versão do Apache para a 2.4.33 ou posterior.	1
Médio	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	Atualize a versão do Apache para a 2.4.34 ou posterior.	3
Médio	Apache 2.4.x < 2.4.35 DoS	Atualize a versão do Apache para 2.4.35 ou posterior.	4
Médio	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	Atualize a versão do Apache para a 2.4.38 ou posterior.	4
Médio	DNS Server Cache Snooping Remote Information Disclosure	Entre em contato com o fornecedor do *software* DNS para obter uma correção.	1
Médio	HTTP TRACE / TRACK Methods Allowed	Desative esses métodos. Consulte a saída do *plugin* para mais informações.	3

Médio	mDNS Detection (Remote Network)	Filtre o tráfego de entrada para a porta UDP 5353, se desejar.	3
Médio	Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	Não há solução conhecida neste momento.	1
Médio	Network Time Protocol (NTP) Mode 6 Scanner	Restringir o modo NTP 6 consultas.	11
Médio	NFS Shares World Readable	Coloque as restrições apropriadas em todos os compartilhamentos NFS.	1
Médio	OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	Atualize versão do OpenSSL para 1.0.2q ou superior.	1
Médio	OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities	Aplique o *patch* do fornecedor ou atualize para o OpenSSL versão 1.1.0i ou superior.	1
Médio	OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	Aplique o *patch* do fornecedor ou atualize para o OpenSSL versão 1.1.0j ou superior.	1
Médio	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	Atualize versão do PHP para 7.2.10 ou superior.	2
Médio	PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF	Atualize versão do PHP para 7.2.8 ou superior.	2
Médio	SMB Signing not required	Impor a assinatura de mensagens na configuração do *host*. No Windows, isso é encontrado na configuração de diretiva 'Microsoft servidor de rede: assinar digitalmente as comunicações (sempre) '. No Samba, a configuração é chamada de 'assinatura do servidor'. Veja o 'ver também' links para mais detalhes.	8
Médio	SSL Certificate Cannot Be Trusted	Adquira ou gere um certificado apropriado para este serviço.	16
Médio	SSL Certificate Signed Using Weak Hashing Algorithm	Entre em contato com a autoridade de certificação para reemitir o certificado	2
Médio	SSL Certificate Validity - Duration	Substitua o certificado SSL por um certificado com um período de validade menor ou igual a 825 dias.	1
Médio	SSL Certificate with Wrong Hostname	Adquira ou gere um certificado apropriado para este serviço.	2

Médio	SSL Self-Signed Certificate	Adquira ou gere um certificado apropriado para este serviço.	15
Médio	Tenable Nessus < 8.0.0 Multiple Vulnerabilities (TNS-2018-14)	Atualizar a versão do Tenable Nessus para 8.0.0 ou superior.	1
Médio	Tenable Nessus < 8.1.1 Multiple Vulnerabilities (TNS-2018-16)	Atualize o Tenable Nessus para versão 8.1.1 ou superior.	1
Baixo	DHCP Server Detection	Aplicar filtragem para manter essas informações fora da rede e remover quaisquer opções que não estejam em uso.	1
Baixo	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Reconfigure o serviço para usar um módulo Diffie-Hellman exclusivo de 2048 bits ou mais.	1
Baixo	Web Server HTTP Header Internal IP Disclosure	Não há solução conhecida neste momento.	1

Fonte: Elaborado pelo autor

APÊNDICE B - Vulnerabilidades Encontradas

Quadro B.2 – Vulnerabilidades encontradas no Nessus

IP	Sistema Operacional	Vulnerabilidade	Resumo	Nível	Referência	Porta	Exploit:
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Microsoft Windows SMB Shares Unprivileged Access	É possível acessar um compartilhamento de rede.	Alto	CVE-1999-0519; CVE-1999-0520.	tcp/445	Não Existem Exploits Relatados
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	mDNS Detection (Remote Network)	É possível obter informações sobre o host remoto.	Médio		udp/5353	Não Existem Exploits Relatados
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	SSL Certificate with Wrong Hostname	O certificado SSL para este serviço é para um host diferente.	Médio		tcp/10000	Não Foram Encontradas + informações
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/10000	Não Existem Exploits Relatados
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/10000	Não Foram Encontradas + informações
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/80	Não Existem Exploits Relatados
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/80	Não Existem Exploits Relatados
172.24.1.38	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Apache 2.4.x < 2.4.35 DoS	O servidor WEB remoto é afetado por uma vulnerabilidade de Negação de Serviço.	Médio	CVE-2018-11763	tcp/80	Não Existem Exploits Relatados
172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Apache 2.4.x < 2.4.35 DoS	O servidor WEB remoto é afetado por uma vulnerabilidade de Negação de Serviço.	Médio	CVE-2018-11763	tcp/443	Não Existem Exploits Relatados
172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/443	Não Existem Exploits Relatados

172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	NFS Shares World Readable	O servidor NFS remoto exporta compartilhamentos de fácil leitura.	Médio	CVE-1999-1546	tcp/2049	Não Existem Exploits Relatados
172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	NFS Exported Share Information Disclosure	É possível acessar compartilhamentos NFS no host remoto.	Crítico	CVE-1999-0170; CVE-1999-0211; CVE-1999-0554	udp/2049	Exploit: NFS Mount
172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	NFS Share User Mountable	O Nessus pôde acessar informações confidenciais de compartilhamentos remotos do NFS sem ter privilégios de root.	Alto	CVE-1999-0170; CVE-1999-0211; CVE-1999-0554	udp/2049	Exploit: NFS Mount
172.24.1.39	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)	mDNS Detection (Remote Network)	É possível obter informações sobre o host remoto.	Médio		udp/5353	Não Existem Exploits Relatados
172.24.1.100	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.1.100	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.1.100	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.4.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.4.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.4.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.4.10	Linux Kernel 2.6	DNS Server Cache Snooping Remote Information Disclosure	O servidor DNS remoto é vulnerável a ataques de rastreamento de cache.	Médio		udp/53	Não Existem Exploits Relatados
172.24.4.10	Linux Kernel 2.6	Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	O servidor da Web remoto é afetado por uma vulnerabilidade de divulgação de informações.	Médio	CVE-2001-1248; CVE-2007-3407.	tcp/5081	Exploits Pagos
172.24.4.10	Linux Kernel 2.6	Web Server HTTP Header Internal IP Disclosure	Esse servidor da web vaza um endereço IP privado por meio de seus cabeçalhos HTTP.	Baixo	CVE-2000-0649	tcp/5081	Não Existem Exploits Relatados
172.24.7.128	Microsoft Windows	HTTP TRACE / TRACK Methods Allowed	As funções de depuração estão ativadas no servidor da web remoto.	Médio	CVE-2003-1567; CVE-2004-2320; CVE-2010-0386.	tcp/80	Não Existem Exploits Relatados
172.24.7.128	Microsoft Windows	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/80	Não Existem Exploits Relatados

172.24.7.128	Microsoft Windows	OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	Um serviço em execução no host remoto é afetado por várias vulnerabilidades.	Médio	CVE-2018-5407; CVE-2018-0734.	tcp/80	Não Existem Exploits Relatados
172.24.7.128	Microsoft Windows	SSL Certificate Signed Using Weak Hashing Algorithm	Um certificado SSL na cadeia de certificados foi assinado usando um algoritmo de hash fraco.	Médio	CVE-2004-2761	tcp/443	Não Existem Exploits Relatados
172.24.7.128	Microsoft Windows	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.7.128	Microsoft Windows	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.13 Arbitrary Command Injection Vulnerability	Um aplicativo instalado no host remoto é afetado por uma vulnerabilidade de injeção de comando arbitrária.	Alto	CVE-2018-19518.	tcp/80	Não Existe Exploit para Windows
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.14 Multiple vulnerabilities	Um aplicativo instalado no host remoto é afetado por várias vulnerabilidades.	Alto	CVE-2016-10166; CVE-2018-19935.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	HTTP TRACE / TRACK Methods Allowed	As funções de depuração estão ativadas no servidor da web remoto.	Médio	CVE-2003-1567; CVE-2004-2320; CVE-2010-0386.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF	A versão do PHP em execução no servidor da web remoto é afetada por uma execução de código arbitrário de uso após a liberação Vulnerabilidade.	Médio	CVE-2018-12882; CVE-2018-14851; CVE-2018-14883; CVE-2018-15132.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	A versão do PHP em execução no servidor Web remoto é afetada por uma vulnerabilidade de script entre sites.	Médio	CVE-2018-17082	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.35 DoS	O servidor WEB remoto é afetado por uma vulnerabilidade de Negação de Serviço.	Médio	CVE-2018-11763	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.13 Arbitrary Command Injection Vulnerability	Um aplicativo instalado no host remoto é afetado por uma vulnerabilidade de injeção de comando arbitrária.	Alto	CVE-2018-19518.	tcp/443	Não Existe Exploit para Windows
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.14 Multiple vulnerabilities	Um aplicativo instalado no host remoto é afetado por várias vulnerabilidades.	Alto	CVE-2016-10166; CVE-2018-19935.	tcp/443	Não Existem Exploits Relatados

172.24.7.109	Microsoft Windows	HTTP TRACE / TRACK Methods Allowed	As funções de depuração estão ativadas no servidor da web remoto.	Médio	CVE-2003-1567; CVE-2004-2320; CVE-2010-0386.	tcp/80	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	SSL Certificate Signed Using Weak Hashing Algorithm	Um certificado SSL na cadeia de certificados foi assinado usando um algoritmo de hash fraco.	Médio	CVE-2004-2761	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF	A versão do PHP em execução no servidor da web remoto é afetada por uma execução de código arbitrário de uso após a liberação Vulnerabilidade.	Médio	CVE-2018-12882; CVE-2018-14851; CVE-2018-14883; CVE-2018-15132.	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities	Um serviço em execução no host remoto é afetado por várias vulnerabilidades	Médio	CVE-2018-0732; CVE-2018-0737; CVE-2018-5407.	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	A versão do PHP em execução no servidor Web remoto é afetada por uma vulnerabilidade de script entre sites.	Médio	CVE-2018-17082	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.35 DoS	O servidor WEB remoto é afetado por uma vulnerabilidade de Negação de Serviço.	Médio	CVE-2018-11763	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	O servidor WEB remoto é afetado por várias vulnerabilidades.	Médio	CVE-2017-15710; CVE-2017-15715; CVE-2018-1283.	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities	Um serviço em execução no host remoto é afetado por várias vulnerabilidades.	Médio	CVE-2018-0734; CVE-2018-0735.	tcp/443	Não Existem Exploits Relatados
172.24.7.109	Microsoft Windows	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	O host remoto permite conexões SSL / TLS com um ou mais módulos Diffie-Hellman menores ou iguais a 1024 bits.	Baixo	CVE-2015-4000	tcp/443	Não Existem Exploits Relatados
172.24.8.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.8.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados

172.24.8.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.12.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.12.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.12.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.16.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.16.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.16.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.32.2	FreeBSD 11.2-RELEASE-p3 (amd64)	DHCP Server Detection	O servidor DHCP remoto pode expor informações sobre a rede associada.	Baixo		udp/67	Não Foram Encontradas + informações
172.24.32.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.32.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.32.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.32.26	Microsoft Windows 7 Professional	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.32.30	Microsoft Windows 7 Professional	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.35.42	Microsoft Windows 7 Professional	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.35.46	Microsoft Windows 7 Professional	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.36.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner

172.24.36.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.36.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.64.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.64.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.64.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.68.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.68.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.68.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.101.217	Microsoft Windows 7, Microsoft Windows Server 2008 R2	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.101.217	Microsoft Windows 7, Microsoft Windows Server 2008 R2	mDNS Detection (Remote Network)	É possível obter informações sobre o host remoto.	Médio		udp/5353	Não Existem Exploits Relatados
172.24.124.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.124.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.124.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações
172.24.128.2	FreeBSD 11.2-RELEASE-p3 (amd64)	Network Time Protocol (NTP) Mode 6 Scanner	O servidor NTP remoto responde ao modo 6 consultas.	Médio	CVE-2013-5211	udp/123	Exploit Auxiliares/Scanner
172.24.128.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/443	Não Existem Exploits Relatados
172.24.128.2	FreeBSD 11.2-RELEASE-p3 (amd64)	SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/443	Não Foram Encontradas + informações

172.24.33.94	Linux Kernel 4.19.0-kali1-amd64	SSL Certificate with Wrong Hostname	O certificado SSL para este serviço é para um host diferente.	Médio		tcp/8834	Não Foram Encontradas + informações
172.24.33.94	Linux Kernel 4.19.0-kali1-amd64	SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/8834	Não Existem Exploits Relatados
172.24.33.94	Linux Kernel 4.19.0-kali1-amd64	Tenable Nessus < 8.0.0 Multiple Vulnerabilities (TNS-2018-14)	Tenable Nessus em execução no host remoto é afetado por várias vulnerabilidades.	Médio	CVE-2018-0732; CVE-2018-0737.	tcp/8834	Não Existem Exploits Relatados
172.24.33.94	Linux Kernel 4.19.0-kali1-amd64	Tenable Nessus < 8.1.1 Multiple Vulnerabilities (TNS-2018-16)	Tenable Nessus em execução no host remoto é afetado por várias vulnerabilidades.	Médio	CVE-2018-0734; CVE-2018-5407.	tcp/8834	Não Existem Exploits Relatados
172.24.33.94	Linux Kernel 4.19.0-kali1-amd64	SSL Certificate Validity - Duration	O certificado SSL é válido durante um período de tempo que é muito longo.	Médio		tcp/8834	Não Foram Encontradas + informações
172.24.241.98	Microsoft Windows 8.1	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner
172.24.240.199		SSL Certificate Cannot Be Trusted	O certificado SSL para este serviço não é confiável.	Médio		tcp/3389	Não Existem Exploits Relatados
172.24.240.199		SSL Self-Signed Certificate	A cadeia de certificados SSL para este serviço termina em um certificado auto-assinado não reconhecido.	Médio		tcp/3389	Não Foram Encontradas + informações
172.24.241.97	Microsoft Windows 8.1	SMB Signing not required	A assinatura não é necessária no servidor SMB remoto.	Médio		tcp/445	Exploit Auxiliares/Scanner

Fonte: Elaborada pelo autor a partir da Ferramenta Nessus