UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE SISTEMAS DE INFORMAÇÃO

DAVID GLEYSON RAMOS

UM ESTUDO SOBRE FERRAMENTAS DE INTRUSÃO EM AMBIENTES COMPUTACIONAIS: UM MAPEAMENTO SISTEMÁTICO

Itacoatiara – Amazonas
Julho – 2021

DAVID GLEYSON RAMOS

UM ESTUDO SOBRE FERRAMENTAS DE INTRUSÃO EM AMBIENTES COMPUTACIONAIS: UM MAPEAMENTO SISTEMÁTICO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

PROF. DR. RAINER XAVIER DE AMORIM

Itacoatiara – Amazonas

Julho – 2021

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Ramos, David Gleyson
R175e Um estudo sobre ferramentas de intrusão em ambientes computacionais: um mapeamento sistemático / David Gleyson Ramos . 2021
35 f.: il. color; 31 cm.

Orientador: Rainer Xavier de Amorim
TCC de Graduação (Sistemas de Informação) - Universidade Federal do Amazonas.

1. Pentest. 2. Vulnerabilidade Computacional. 3. Ameaça Computacional. 4. Teste de Intrusão. 5. Segurança da Informação. I. Amorim, Rainer Xavier de. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Curso de Sistema de Informação - ICET

FOLHA DE APROVAÇÃO

DAVID GLEYSON RAMOS

UM ESTUDO SOBRE FERRAMENTAS DE INTRUSÃO EM AMBIENTES COMPUTACIONAIS: UM MAPEAMENTO SISTEMÁTICO

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

Aprovada em 28 de Junho de 2021

BANCA EXAMINADORA

Prof. Dr. Rainer Xavier de Amorim, Presidente
Universidade Federal do Amazonas

Prof. Esp. Kleyson Lima Maciel, Membro
Universidade Federal do Amazonas

Prof. Me. Adriano Honorato de Souza, Membro
Instituto Federal do Amazonas

Folha de Aprovação assinada pela Profa. Odette Mestrinho Passos, responsável pela disciplina de Trabalho de Conclusão de Curso (Período: 2020.1), onde atesta a defesa do(a) aluno(a) e a presença dos membros da banca examinadora.

Documento assinado eletronicamente por **Odette Mestrinho Passos**, **Professor do Magistério Superior**, em 06/07/2021, às 11:11, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0596520** e o código CRC **CF19645B**.

Rua Nossa Senhora do Rosário - Bairro Tiradentes nº 3836 - Telefone: (92) (92) 99318-2549
CEP 69103-128 Itacoatiara/AM - ccsiicet@ufam.edu.br

A Deus e a minha família que foram fundamentais para a minha formação acadêmica.

AGRADECIMENTOS

Dedico todos os meus esforços primeiramente a Deus, que sem Ele nada poderia ter sido feito. Em segundo, aos meus pais que foram os alicerces que possibilitaram essa oportunidade de realizar este curso de Sistemas de Informação no Município de Itacoatiara e também a minha família, esposa e filha, que foram as minhas forças para continuar na labuta para a conclusão deste trabalho.

Deixo também a minha gratidão aos meus professores que foram fundamentais na minha formação acadêmica e arcabouço de conhecimento, em especial, o professor Dr. Rainer Xavier de Amorim, que foi meu orientador neste trabalho e me ajudou a despertar o interesse por essa área de pesquisa, a segurança da informação e de redes.

O SENHOR firma os passos de todo aquele cuja conduta lhe agrada!

Salmos 37:23

Um Estudo Sobre Ferramentas de Intrusão em Ambientes Computacionais: Um Mapeamento Sistemático

David Gleyson Ramos, Rainer Xavier de Amorim

Instituto de Ciências Exatas e Tecnologia – Universidade Federal do Amazonas (ICET/UFAM) – Itacoatiara – Amazonas – Brasil

davidgleyson46@gmail.com, raineramorim@ufam.edu.br

Resumo. *Com o aumento de ataques cibernéticos a grandes empresas e entidades governamentais, tornou-se imprescindível tomar as devidas medidas de segurança. Neste trabalho o foco é abordar as principais ferramentas utilizadas por invasores e profissionais que realizam testes de intrusão, como consequência, apresentar os principais ataques oriundos destas ferramentas. A metodologia de pesquisa adotada está fundamentada nos princípios da Engenharia de Software Experimental que se baseia na condução de um estudo secundário: o Mapeamento Sistemático. Os resultados revelam as ferramentas e ataques mais frequentes e os caminhos que são tratados por esses indivíduos ou grupos.*

1. Introdução

Com o aumento de incidentes cibernéticos a grandes empresas, sendo alvos de ataques, tornou-se imprescindível tomar as devidas medidas de segurança, evitando assim brechas contra invasores. Essas organizações estão sendo vítimas de uma imensa perda de dados e com isso, colocando em riscos as suas informações internas e de seus clientes (WEIDMAN, 2014).

Diante deste cenário, a segurança de computadores é um fator preponderante como tentativa de inibir eventuais problemas, onde o responsável pela rede ou sistema, tenta fechar as portas contra um possível invasor, um verdadeiro confronto de intelectos, onde de um lado o atacante procura encontrar uma vulnerabilidade e do outro lado o defensor tentando assegurar que todas as possibilidades de ataque estão fechadas, ou seja, neutralizadas (STALLINGS, 2015).

Desta maneira, é necessário que seja feita a análise de vulnerabilidades, que consiste em um processo periódico de testes para detectar possíveis ameaças. As principais características são decorrentes de falhas de programação, erros de configuração de dispositivos de rede e principalmente, por falhas humanas, resultante de falta de conhecimento em segurança da informação na organização (MELO, 2017).

Desta maneira, para se ter um ambiente seguro, deve-se adotar os conceitos de segurança da informação, assegurando que os três principais alicerces da segurança da informação não sejam violados. São eles: a integridade, a disponibilidade e a confidencialidade. Sem os quais, fica inviável a segurança e proteção da informação (FOROUZAN e MOSHARRAF, 2013).

A metodologia de pesquisa adotada neste trabalho, para coletar as informações de forma a cumprir o objetivo, está fundamentada nos princípios da Engenharia de Software Experimental que se baseia na condução de um estudo secundário: Mapeamento Sistemático (MS). O MS fornece uma visão geral de uma área de pesquisa, identificando a quantidade, os tipos de pesquisas realizadas, os resultados disponíveis, além das frequências de publicações ao longo do tempo para identificar tendências (Petersen et al., 2008).

Kitchenham e Charters (2007), afirmam que estudos de MS em engenharia de software têm sido recomendados, sobretudo para áreas de pesquisa onde é difícil visualizar a gama de materiais, relevantes e de alta qualidade, que possam estar disponíveis. Assim sendo, a escolha do MS como proposta para a condução desta pesquisa, justifica-se pelo fato do objetivo de a pesquisa ser apenas identificar e utilizar os resultados obtidos para futuras pesquisas.

Desse modo, este artigo tem como objetivo apresentar os principais estudos de ferramentas de detecção usadas na exploração de vulnerabilidades e ameaças em ambientes computacionais, a fim de lhes fornecer um entendimento sobre como funcionam as tentativas de intrusão, ou seja, como um ataque cibernético pode acontecer. Com isso, elucidar as maneiras que um atacante pode agir, com o auxílio das diversas ferramentas existentes.

Como resultado, foi possível identificar as diversas ferramentas de intrusão para detecção de vulnerabilidades em sistemas computacionais, que podem ser utilizadas em vários ambientes, tanto real como virtualizado. Considerando o lado introspectivo, a própria padronização do processo de invasão entre outros. Além disso, foram elencados os diversos tipos de ataques, todos com suas características e particularidades únicas.

O restante do artigo está organizado da seguinte maneira: a Seção 2 apresenta alguns conceitos relacionados e discute os trabalhos relacionados. A Seção 3 apresenta a metodologia utilizada, enquanto a Seção 4 mostra os resultados e as discussões. A Seção 5 apresenta as conclusões e as propostas de trabalhos futuros.

2. Fundamentação Teórica

2.1. Conceitos Relacionados

Por meio da política de segurança, os mecanismos de segurança visam responsabilizar todos aqueles que dispõem dos recursos computacionais, sejam eles usuários ou instituições. Além disso, a política de segurança pode possuir outras políticas específicas, como a política de senhas, política de backup, política de privacidade, política de confidencialidade e política de uso aceitável, visando garantir a segurança da informação (CERT.br, 2012).

Segundo a norma ABNT NBR ISO/IEC 17799:2005, a informação é o principal ativo a ser protegida e resguardada pelas organizações. Considerando o aumento da

interconectividade, a preocupação com a informação se tornou acentuada, devido às ameaças e as vulnerabilidades.

Desta forma, a vulnerabilidade consiste em uma falha computacional, geralmente, esse problema é consequente de software, onde o atacante desvirtua o funcionamento do sistema para usufruir do acesso não autorizado e privilegiado (FERREIRA et al., 2012).

Uma forma de identificar essas vulnerabilidades é através de testes de intrusão (*pentest*), que consiste em um procedimento para catalogar as falhas do sistema. Tal procedimento, auxilia na averiguação de qual nível um atacante terá acesso à rede e a informação (MARTINS, 2018).

De acordo com Weidman (2014), uma invasão possui 7 fases: 1) preparação; 2) coleta de informações, 3) modelagem de ameaças, 4) análise de vulnerabilidades, 5) exploração de falhas, 6) pós-exploração de falhas e 7) geração de relatórios. Todas essas fases consistem no processo de sucesso de um teste de invasão, onde os *pentesters* não só identificam, como avaliam, exploram todas as possibilidades mapeadas que um possível invasor possa realizar.

2.2. Trabalhos Relacionados

Silva e Pereira (2013) apresentam em seu trabalho uma abordagem com a definição de *pentest* (teste de intrusão), exemplificando como são o processo de um ataque, quais os tipos de exploração de vulnerabilidades. O mesmo abrange também os tipos de *pentesting* existentes e as etapas a serem seguidas até o teste final. A metodologia utilizada foi a de investigações científicas em revistas, artigos, bibliotecas digitais e sites na internet.

A partir das análises, os pesquisadores identificaram que apesar de existirem leis para coibir e divisões dos crimes praticados por meio de computadores, os donos da informação optam por pagar para manter os seus dados protegidos. As ferramentas utilizadas pelos crackers também são utilizadas pelos *pentesting*, sendo que os profissionais de *pentest* utilizam para proteger seus clientes de grandes perdas de dados (SILVA e PEREIRA, 2013).

Cordeiro e Fernandes (2017) abordam um trabalho com o objetivo de mostrar uso de ferramentas gratuitas em busca de vulnerabilidades, aplicando em diversos sites, particulares, governamentais, regionais e nacionais. A metodologia aplicada foi a de fases de reconhecimento*, scanning*, exploração de falhas e preservação de acesso.

Após a análise da pesquisa, os autores notaram que o uso das duas ferramentas se mostrou eficazes na varredura e na detecção de vulnerabilidades, sendo que a primeira ferramenta (Armitage) não encontrou nenhuma falha no decorrer do teste, já a segunda ferramenta (Nmap) encontrou algumas vulnerabilidades nas portas e detectou os tipos de sistemas operacionais (CORDEIRO e FERNANDES, 2017).

O trabalho realizado por Martinelo e Bellezi (2014), apresentou uma abordagem sobre vulnerabilidades, tipos de ataques, softwares maliciosos e utilização de ferramentas de varreduras e escaneamentos. Com isso, verificou-se a necessidade de analisar e corrigir

as eventuais falhas antes que elas sejam exploradas pelos atacantes. Os autores sugeriram que fossem realizadas novas análises e varreduras utilizando as ferramentas OpenVAS e Nessus em uma rede corporativa, a fim de detectar possíveis ameaças e explorar os falsos positivos da rede (MARTINELO e BELLEZI, 2014).

Ferrão e Kreutz (2017) explanaram em seu trabalho a aplicação de scanners de vulnerabilidades, cujas ferramentas são gratuitas e de código aberto, realizando testes de vulnerabilidades. A proposta de combinação de ferramentas foram uma tentativa de garantir a maior cobertura de vulnerabilidades em Sistemas Web, feita através da análise black-box.

Os pesquisadores concluíram, a partir dos resultados obtidos pelos testes, que a combinação do uso de diversas ferramentas de scanners facilita a correção dos erros, que muitas vezes são ocasionados durante a fase de desenvolvimento. A ferramenta que melhor trouxe resultados foi a Zed Attack Proxy dentre as 10 aplicadas, entretanto, é necessário o auxílio das outras para se ter mais precisão em quais procedimentos de segurança precisam ser tomados (FERRÃO e KREUTZ, 2017).

O trabalho de Martins e Cardoso (2018) teve como objetivo mostrar as fases do *pentest* e sua utilidade, demonstrar a capacidade das ferramentas de obter as informações pertinentes. Os resultados foram uma base teórica para trabalhos futuros, devido às questões de segurança não foi possível aplicar no sistema da instituição, somente realizado os testes em ambiente virtual.

As pesquisas de Silva e Pereira (2013) consistiam em uma amostragem conceitual e exemplificação dos termos. Desta maneira, Martins e Cardoso apresentaram de forma teórica os conceitos de *pentest* e esclarecendo os tipos de testes de penetração. Por outro lado, Cordeiro e Fernandes demonstraram através de duas ferramentas como identificar as possíveis vulnerabilidades em um sistema web. Os trabalhos de Martinelo e Bellezi (2014) e Ferrão e Kreutz (2017) se assemelham a este trabalho por se propuserem a identificar e fornecer as informações em torno das análises e formas de exploração de vulnerabilidades, além de apresentarem várias ferramentas no auxílio da detecção de possíveis ameaças e formas de correção do problema no contexto.

2.3 Levantamento das Ferramentas em Ambientes Organizacionais

2.3.1 Planejamento do Levantamento das Informações

A. Definição dos Participantes

Para realizar a pesquisa sobre as principais ferramentas de detecção de intrusão e ataques cibernéticos, o levantamento dessas informações foi através de um questionário com os profissionais de segurança da informação e analistas de Tecnologia da Informação, de empresas privadas e instituições públicas, localizadas na cidade de Manaus-AM, foi necessário planejar o público-alvo para que fosse possível enviar o questionário para os participantes, estes deveriam estar atuando na área afim. A finalidade do questionário é de verificar como os profissionais de TI do mercado de trabalho se protegem contra os

ataques de intrusão, e se já tiveram problemas que poderiam compartilhar e colaborar com esta pesquisa.

Dessa forma, foram contatados 12 (doze) profissionais de computação de empresas/instituições públicas e privadas. Onde, a partir da conversa e explanação sobre o Termo de Consentimento, foi encaminhado um formulário eletrônico para que eles pudessem responder, conforme a realidade em seus respectivos ambientes de trabalho. Mas, somente 04 (quatro) participantes aceitaram responder, pois nem todos os profissionais contatados tinham experiência com o tema desta pesquisa, por isso, não sabiam responder. Sendo assim, logo após o acordo entre as partes, foram escolhidos os dias e horários para a (aplicação/envio) do formulário para a coleta de dados

B. Definição da Instrumentação:

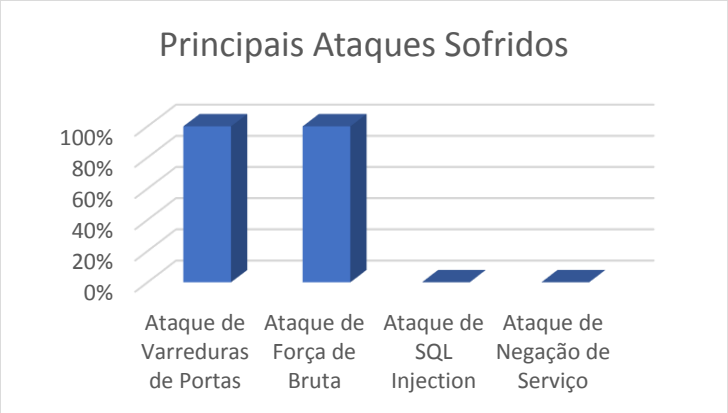
Foi realizada a elaboração de um Termo de Consentimento composto de um questionário, apresentado nos anexos deste trabalho, para realizar a coleta dos dados de acordo com o planejamento. Logo após a elaboração das perguntas foi criado o formulário, via Google Forms.

C. Análise e Resultado da Pesquisa

A pesquisa foi encaminhada para 12 (doze) profissionais de TI, tendo como retorno 4 (quatro) respostas obtidas dos profissionais que trabalham tanto em empresas privadas como instituições públicas.

As informações obtidas na aplicação do questionário são apresentas nas Figuras 1, 2, 3, 4 e 5. Através delas, pode-se visualizar as incidências e ocorrências de ataques, as principais ferramentas e mecanismos para inibir as intrusões, além das informações de tipos de licenças e políticas de segurança como medida de coibir ações internas e externas de agentes mal-intencionados.

Figura 1. Principais Ataques sofridos



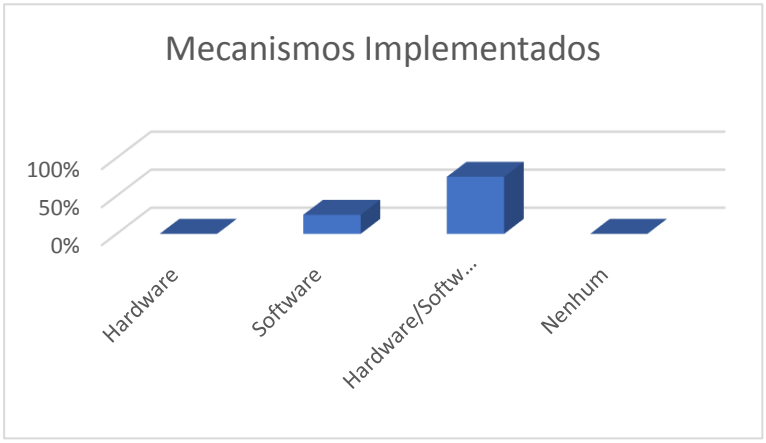
Fonte: O autor (2021).

Percebe-se que as maiores tentativas de ataques sofridos pelas organizações são decorrentes de ataques de força-bruta, ou seja, o invasor usa de um software que age por

tentativas incansáveis, com o objetivo de forçar a quebra de uma senha de um possível usuário do sistema, e assim invadi-lo. Outra forma é através do ataque de varreduras de Portas, conhecido como *Scan*, esse tipo de ataque visa encontrar uma vulnerabilidade de alguma porta, serviço ou sistemas operacionais ativos, para assim tentar com auxílio de outras ferramentas concretizar o ataque.

A seguir é apresentada a Figura 2, que traz como base de informação quais tipos de mecanismos as organizações utilizam como barreira de segurança, sendo implementações em Hardware ou Software. A implementação em Hardware, dispõe de um dispositivo físico que trabalha especificamente para proteger a infraestrutura de rede da organização. Já a implementação em Software pode ser feita por meio de um servidor de firewall ou proxy, que podem trabalhar simultaneamente para proteger o acesso e dados da empresa.

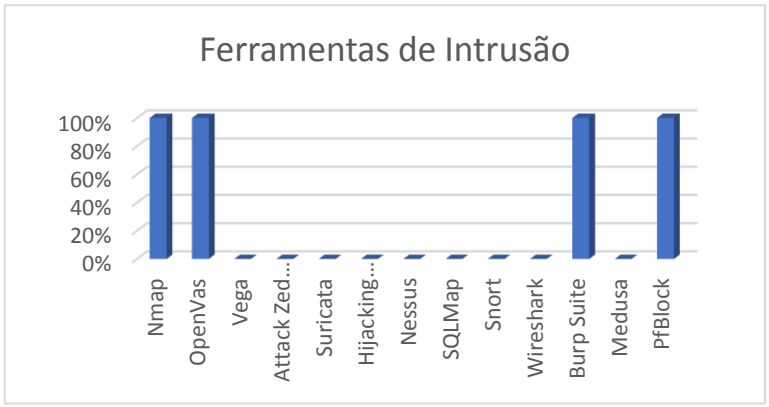
Figura 2. Mecanismos Implementados



Fonte: O autor (2021).

Na Figura 3 é apresentado o gráfico com as principais ferramentas utilizadas pelos profissionais para auxiliá-los no ambiente de trabalho para localizar e coibir um possível invasor na rede, ou sistema.

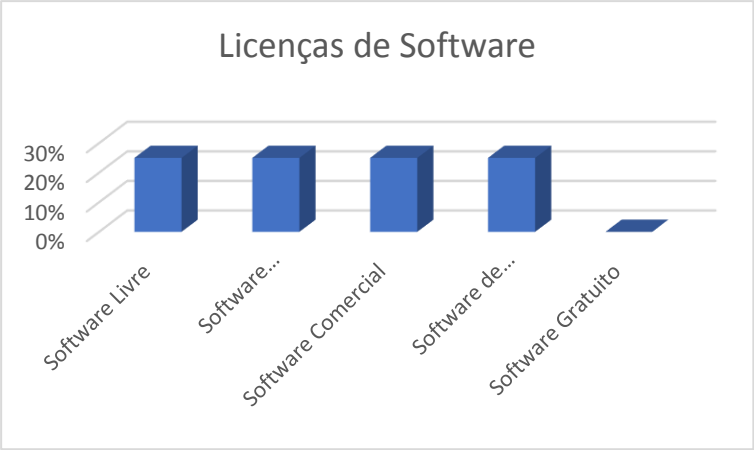
Figura 3. Ferramentas de detecção



Fonte: O autor (2021).

Na Figura 4 obteve-se um equilíbrio de 25% para cada tipo de licença de software utilizada pelos profissionais, ressalta-se a importância de sempre manter a legalidade do uso do software, respeitando os direitos autorais e a comunidade desenvolvedora.

Figura 4. Licenças dos Softwares de Intrusão



Fonte: O autor (2021).

Com isso, conclui-se que há um equilíbrio por partes das organizações em utilizar os diversos tipos de softwares: proprietário, softwares livres ou de código aberto. O fator que pode ser o diferencial entre uma organização e outra, deve-se considerar o nível de capacitação da equipe de TI, os incentivos em aprimoramentos do conhecimento em novas tecnologias.

Figura 5. Comportamento Organizacional dos Funcionários

Fonte: O autor (2021).

Apesar de se ter todos os meios para implementar uma boa infraestrutura de Tecnologia da Informação, tanto em hardware como em software, é necessário desenvolver uma política de segurança institucional, visando abarcar todas as possíveis ameaças, sejam elas internas ou externas. Na Figura 5, analisou-se a relação ao comportamento de risco dos funcionários, de forma que pudesse afirmar que existe uma conscientização a respeito do sigilo, integridade e confidencialidade das informações trocadas.

Portanto, com o conjunto de respostas obtidas, foi possível alcançar os resultados esperados. O questionário trouxe uma visão panorâmica de como as organizações estão atentas para as ameaças e vulnerabilidades em sua infraestrutura, o cuidado em manter uma política de segurança com os funcionários, e a capacitação destes para lidar com as tecnologias de intrusão.

3. Método da Pesquisa

O MS foi baseado no guidelines desenvolvido por Kitchenham e Chartes (2007) e definido em três etapas: (a) Planejamento do Mapeamento: nesse passo, os objetivos da pesquisa são listados e o protocolo do mapeamento é definido; (b) Condução do Mapeamento: durante essa fase, as fontes para o mapeamento são selecionadas, os estudos são identificados, selecionados e avaliados de acordo com os critérios estabelecidos no protocolo do mapeamento e (c) Resultado do Mapeamento: nessa fase, os dados dos estudos são extraídos e sintetizados para serem publicados.

3.1 Planejamento do Mapeamento Sistemático

Nesta etapa foi definido o protocolo de pesquisa, que consiste em definir o objetivo do estudo, especificar as questões da pesquisa, formular a expressão de busca, além de mencionar os procedimentos de extração dos dados e os critérios de seleção de cada publicação. A estrutura do protocolo foi baseada nos trabalhos de Kitchenham e Charters (2007), conforme descrito a seguir. Para cada uma das subseções a seguir serão apresentados o que se esperava a partir do protocolo e o conteúdo de fato utilizado no estudo em questão.

3.1.1 Objetivo e Questões de Pesquisa

O objetivo deste mapeamento sistemático é analisar publicações científicas com o propósito de investigar quais as principais ferramentas utilizadas nos testes de intrusão, a fim de detectar vulnerabilidades e ameaças em um ambiente computacional, pois algumas demonstram de certa forma, como os invasores realizam os ataques cibernéticos e assim perscrutando o ponto de vista dos pesquisadores no contexto da segurança da informação.

Sendo assim, este MS busca respostas para as seguintes questões de pesquisa (QP): QP1: Quais as principais ferramentas utilizadas para a detecção de vulnerabilidades e ameaças em sistemas computacionais? e QP2: Quais as principais tentativas de ataque identificadas nos ambientes computacionais?

3.1.2 Fontes, Idioma e Expressão de Busca.

a. Fontes

Os locais de busca definidos para esta pesquisa serão feitos a partir da busca manual nos anais das conferências nacionais relacionadas à Segurança da Informação apoiada pela SBC (Sociedade Brasileira de Computação) que possui relação com o tema a ser pesquisado: Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg) e o Workshop de Segurança Cibernética em Dispositivos Conectados

(WSCDC). A busca automática realizar-se-á por meio de investigação nas bibliotecas digitais pertencentes a uma das editoras listadas no Portal de Periódicos da CAPES: a Scopus. Além das pesquisas realizadas no Google Acadêmico e em sites e blogs pela internet.

Nos anais de conferências foram identificados relatos de experiência e artigos técnicos, nos repositórios das instituições foram pesquisados: monografias, teses e dissertações, nas bibliotecas digitais foram considerados artigos científicos. Serão analisados somente os anais das conferências que estavam acessíveis na Internet.

b. Idioma e Expressão de Busca

Os idiomas escolhidos foram o Inglês (devido à sua adoção pela maioria das conferências, periódicos e editoras da área de pesquisa) e o Português (para incluir trabalhos técnicos publicados em conferências nacionais).

A busca foi restringida usando-se palavras-chave específicas para encontrar as publicações de interesse. A expressão de busca foi definida de acordo com dois dos quatro aspectos indicados em [Peterson et al., 2008]: População e Intervenção, conforme a Tabela 1.

Para investigação por expressão de busca (para a consulta das bases foi adicionado o conectivo lógico AND entre a População e Intervenção):

Tabela 1. Expressão de busca utilizada para identificar as publicações

Para investigação por busca manual (no idioma Português):

População: publicações que fazem referências às principais vulnerabilidades e ameaças computacionais (e sinônimos):

Palavras-chave: "vulnerabilidade computacional" OU "ameaça computacional" OU "segurança da informação"

Intervenção: publicações que fazem referências quais as principais técnicas de intrusão utilizada (e sinônimos)

Palavras-chave: "teste de intrusão" OU "*pentest*" OU "teste de penetração"

Para investigação por expressão de busca (no idioma Inglês):

População: publicações que fazem referências às principais ferramentas aplicadas na busca por vulnerabilidades e ameaças computacionais (e sinônimos):

Palavras-chave: "Cyber threat" OR "computational vulnerability" OR "information security"

Intervenção: publicações que fazem referências quais os principais testes de intrusão utilizados (e sinônimos)

Palavras-chave: "intrusion test" OR "penetration tests" OR "pentesting"

3.1.3 Critérios de Seleção

Esta pesquisa se restringe à análise de publicações disponíveis até a data presente da execução do estudo. A seleção das publicações foi realizada em três etapas:

(1) Busca preliminar das publicações coletadas nas fontes definidas;

(2) Primeiro Filtro de Seleção: por meio de análise do título, o resumo e as palavras-chave e aplicando o critério de seleção "CS1: As publicações devem possuir informações sobre quais ferramentas são empregadas na detecção das vulnerabilidades em sistemas computacionais ou possuir evidência de quais os principais mecanismos utilizados para identificar as ameaças no cenário computacional";

(3) Segundo Filtro de Seleção: por meio da leitura completa das publicações e aplicando o critério de seleção "CS2: As publicações devem apresentar evidências de quais foram os ataques realizados para explorar as vulnerabilidades com o auxílio das ferramentas de intrusão".

3.1.4 Procedimentos de Extração de Dados

Serão extraídas informações de publicações relevantes para a pesquisa, que serão registradas em tabelas, conforme os campos abaixo, descritos na Tabela 2:

Tabela 2. Campos de coleta de dados

A) Dados da publicação:	
Título:	indica o título do trabalho
Autor(es):	nome dos autores
Fonte de Publicação:	local de publicação
Ano da Publicação:	ano de publicação
Resumo:	texto contendo uma descrição do resumo
B) Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Descrever o contexto de aplicação das ferramentas, em qual cenário ou fases da exploração as ferramentas são aplicadas
Quais as consequências dos ataques:	Identificar as ocorrências dos ataques e suas consequências
Os resultados dos testes mostraram eficiência:	O uso das ferramentas se mostrou eficiente em sua finalidade de emprego

3.2 Condução do Mapeamento Sistemático

Na etapa da Condução do Mapeamento Sistemático, a execução do MS ocorreu entre os meses de março a junho de 2021, e as publicações foram selecionadas de acordo com os critérios estabelecidos no protocolo. Publicações duplicadas, inacessíveis ou mesmo indisponíveis na internet foram descartadas. Além disso, não foram consideradas as publicações que abordaram outros assuntos não relevantes para a pesquisa.

Foram investigados por buscas manuais os anais do SBSeg de 2012 a 2020, obtendo um total de 513 publicações. Na biblioteca digital da Scopus foi identificado um total de 54 publicações no período de 2015 a 2021. Nos anais do WSCDC foram encontradas 18 publicações no período de 2018 a 2019. Nas buscas automáticas no Google Acadêmico foram reportadas 97 publicações, onde foram consideradas as 5 primeiras páginas restringidas nas publicações de 2014 a 2021, entretanto, nas pesquisas nos sites e blogs foram encontradas 100 publicações, entre o intervalo de publicações de 2017 a 2021, considerando as 5 primeiras páginas.

Após a primeira análise, de acordo com o 1º filtro (leitura do título, resumo da publicação e palavras chaves), 75 publicações foram selecionadas pelo critério CS1, como apresentado na Tabela 2. Do total das publicações que resultaram do 1º filtro, 12 publicações foram selecionadas por estarem de acordo com o critério CS2, como apresentado na Tabela 3, onde todas foram lidas na íntegra.

Tabela 3. Publicações encontradas por etapa

Fontes	Pesquisas	Após o 1º Filtro	Após o 2º Filtro
SBSeg	513	20	2
Scopus	54	3	1
WSCDC	18	5	1
Google Acadêmico	97	29	7
Sites/Blogs	100	18	1
Total	**682**	**75**	**12**

Das 12 publicações identificadas, foi possível extrair uma quantidade significativa de ferramentas utilizadas durante as pesquisas. Essas ferramentas representam a frequência e a preferência dos usuários, dependendo do contexto a ser empregado. Segue a tabela com as publicações identificadas durante o Mapeamento Sistemático:

Tabela 4. Publicações selecionadas após o 2º filtro

ID	Títulos	Autores	Ano
[P01]	Internal Threat Defense using Network Access Control and Intrusion Prevention System	Putra, A. S.; Surantha, N.	2019
[P02]	Análise conceitual e comparativa entre Sistemas de Detecção de Intrusão	Beraldo, L.; Pedroso, D.; Bruno, F. G.; Ito, F. T.	2018
[P03]	Estudo e Análise de Vulnerabilidades Web	Monteverde W. A.; Campiolo, R.	2014
[P04]	Identificando vulnerabilidades de segurança em uma aplicação web	Coelho, M. S.; Tomasi, L. A.; Idalino, T. B.; Martina, J. E.	2015
[P05]	O uso da ferramenta de honeypot para a segurança de redes	Silva, P. R.; Martins, D. M. S.	2014
[P06]	Análise de Vulnerabilidades com OpenVAS e Nessus	Martinelo, C. A. G.; Bellezi, M. A.	2014
[P07]	Um Estudo Sobre a Análise de Vulnerabilidades em Sistemas Computacionais - das Ferramentas ao Uso	Jacobsen, W.;Freitas, M. P.; Rotondo, G.; Almeida, D.; Camargo, A.; Amaral, É.	2014
[P08]	Auditoria de Segurança da Informação em Sistemas e Aplicações	Cruz, C. M. B. R.	2017
[P9]	Detecção e análise de vulnerabilidades em um servidor OJS utilizando teste de penetração	Maciel, D. P.	2019
[P10]	Teste de invasão em aplicações web utilizando SQL Injection: Um estudo Epistemológico	Carneiro, A. S. L.	2017
[P11]	Aplicação de técnicas de Ethical Hacking – Demonstração do uso de ferramentas e ambiente de Estudo para acadêmicos ou iniciantes em segurança Web	Cordeiro, F. A.	2020
[P12]	Os 7 principais tipos de vulnerabilidades em uma empresa	Oliveira, Rodrigo	2017

4. Resultados e Discussões

A última etapa do Mapeamento Sistemático é referente à análise dos dados coletados durante a busca automática, aos dados sintetizados são demonstrados nas subseções a seguir.

4.1 Análise e Discussões da QP1

Com relação à primeira questão de pesquisa: *"Quais as principais ferramentas utilizadas para a detecção de vulnerabilidades e ameaças em sistemas computacionais?"*, foram identificadas várias ferramentas nas publicações, onde a finalidade de detecção de vulnerabilidades e ameaças foi explanada pelos autores, mostrando a sua utilização e aplicabilidade nos cenários fictícios e reais.

A Tabela 5 contém a quantidade de ferramentas extraídas das publicações, ressalta-se que algumas foram empregadas com o intuito de mapear vulnerabilidades e possíveis ameaças, enquanto outras foram utilizadas para realizar ataques, a partir da posse do levantamento de fragilidades computacionais detectadas.

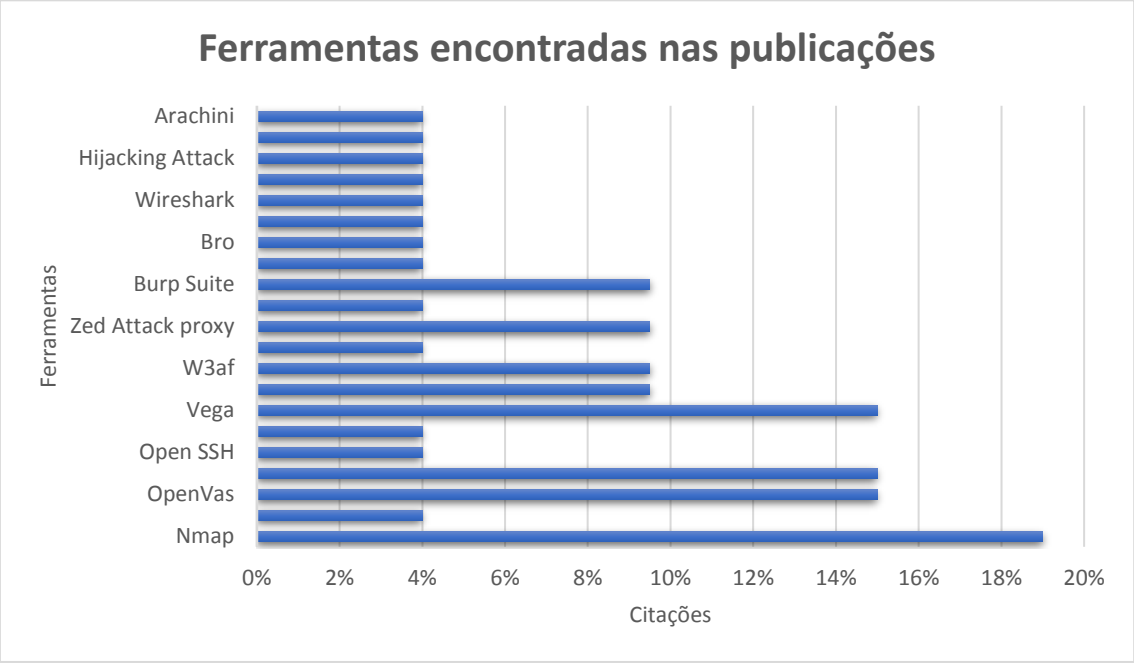
Tabela 5. Lista das ferramentas mais utilizadas nas publicações

ID	Ferramentas	Citações	% de Citações	Funcionalidade | Tipo de Ataque
[F01]	Nmap	P[05], P[09], P[11],P[12]	19% (4/21)	Ataque de Varredura
[F02]	Medusa	P[05]	4% (1/21)	Ataque de Força Bruta
[F03]	OpenVAS	P[06], P[07], P[08]	15% (3/21)	Ferramenta de Escaneamento
[F04]	Nessus	P[06], P[07], P[08],P[12]	15% (3/21)	Ferramenta de Escaneamento
[F05]	Open SSH	P[05]	4% (1/21)	Ferramenta de Conexão SSH
[F06]	WhatWeb	P[08]	4% (1/21)	Ferramenta de Escaneamento
[F07]	VEGA	P[01], P[03], P[08]	15% (3/21)	Ferramenta de Escaneamento
[F08]	SQLMap	P[03], P[08]	9,5% (2/21)	Ataque SQL Injection
[F09]	W3af	P[03], P[08]	9,5% (2/21)	Ferramenta de Escaneamento
[F10]	Metasploit	P[11]	4% (1/21)	Kit de ferramentas de intrusão
[F11]	Zed Attack Proxy	P[04], P[09]	9,5% (2/21)	Ferramenta de Escaneamento
[F12]	Acutinex	P[9]	4% (1/21)	Ferramenta de Escaneamento
[F13]	Burp Suite	P[03], P[09]	9,5% (2/21)	Análise e Capturador de Pacotes
[F14]	Snort	P[02]	4% (1/21)	Ataque de Varredura
[F15]	Bro	P[02]	4% (1/21)	Ataque de Varredura
[F16]	Suricata	P[02]	4% (1/21)	Ataque de Varredura
[F17]	Wireshark	P[03]	4% (1/21)	Análise e Capturador de Pacotes
[F18]	John The Ripper	P[03]	4% (1/21)	Ataque de Força Bruta
[F19]	Hijacking Attack	P[03]	4% (1/21)	Ataque de Roubo de Sessão
[F20]	SQL Injection Attack	P[01]	4% (1/21)	Ataque SQL Injection
F[21]	Arachni	P[02]	4% (1/21)	Ataque de Força Bruta

A análise dos dados nos mostra que temos o Nmap, o OpenVAS, o Nessus e o VEGA, como sendo as ferramentas mais usadas para mapear as vulnerabilidades computacionais. Isso significa que para realizar um ataque é necessário primeiro explorar e obter as informações suficientes do nosso alvo, ou seja, uma varredura completa em

busca de mecanismos de controle, dispositivos e serviços ativos (GIAVAROTO e SANTOS 2013). De acordo com Silva e Martins (2014) as medidas de combate são necessárias quando os sistemas estão em comportamento inesperado, as ações de mapear os métodos e ações dos atacantes são essenciais para evitar um ataque. A seguir é apresentado na Figura 6, o gráfico com as ferramentas identificadas nas publicações.

Figura 6. Gráfico com as ferramentas de detecção de intrusão



A ferramenta Nmap é um software de código aberto muito utilizado para auditar sistemas. Ele utiliza pacotes de IP para localizar dispositivos e serviços, sua principal função é realizar varreduras por hosts em rede (CRUZ, 2017). Nos trabalhos de Silva e Martins (2014), o Nmap realizou a varredura de host na rede, e no escaneamento detectou o Honeypot que neutralizou as ações das ferramentas de intrusão. Com isso, as melhores práticas de segurança que um administrador de redes deve tomar é colocar barreiras para inibir ações indesejáveis, como um ataque de *Scan* e para não expor as vulnerabilidades da infraestrutura, sejam Honeypot, IDS, IPS, firewall, etc.

Na publicação de Oliveira (2017) as vulnerabilidades encontradas em redes e sistemas de informação estão as ferramentas Nmap e o (Nessus - software proprietário), que fazem o trabalho de checagem em range de IPs, portas e serviços (sistemas operacionais ativos). Um mecanismo fundamental para a identificação de ameaças é a implementação de um firewall para controle de fluxo de dados, portas e serviços.

O software OpenVAS é uma ferramenta gratuita, ela foi derivada do Nessus, tem a característica de realizar a varredura em portas e serviços, a fim de encontrar vulnerabilidades, pode ser utilizado independentemente da quantidade de computadores conectados na rede. Nos trabalhos de Jacobsen et. al (2014) o OpenVAS foi o mais indicado em relação ao seu concorrente de uso o Nessus, ele exige um conhecimento

técnico mais aprimorado tornando-se mais complexo, todavia, o seu funcionamento permite que possa ser feito a análise e a correção das vulnerabilidades de forma efetiva.

Outra ferramenta muito utilizada como está na Tabela 5 para realizar os testes de intrusão é o VEGA. No trabalho de Cruz (2017), o VEGA foi utilizado para vasculhar as vulnerabilidades da aplicação que estava na plataforma do sistema governamental, onde gerou um relatório contendo todas as fragilidades auditadas, com o total de 84 vulnerabilidades encontradas, elencadas através de níveis de gravidade de risco: grave, média e baixa, onde após os testes foram reportadas aos administradores para correção.

Muitas ferramentas de detecção de vulnerabilidades também são usadas para fins de invasão, elas estão acessíveis para qualquer usuário que navega na internet, seja ele um conhecedor dos processos de penetração em sistemas (*pentest*) ou não. Como se pode perceber na Tabela 5 o rol de oportunidades de uso destas ferramentas é lastro, bastando, a dedicação e o esforço em pesquisar para aprender a manusear cada uma, enfatizando sempre que consciência dos atos que podem acarretar pelo mau uso delas.

4.2 Análise e Discussões da QP2

Com relação à segunda questão de pesquisa: *"Quais as principais tentativas de ataque identificadas nos ambientes computacionais?"*. Durante a pesquisa em busca do levantamento de informações das ferramentas de detecção de vulnerabilidades, foi possível encontrar os testes sendo realizados com diversos tipos de ataques. Alguns foram em ambientes virtualizados e outros em ambientes reais, com a devida autorização.

O ataque cibernético pode ser considerado a partir do momento em que o atacante começa a explorar falhas, utilizando todo meio para conseguir o controle total da vítima, seja por ferramentas, engenharia social, entre outras técnicas (CARNEIRO, 2017). De fato, o ataque pode ser considerado o ultimato de sucesso de qualquer invasor ou *pentesters*, pois confirma todo o esforço e a rastreabilidade de todo o processo de invasão.

Conforme ilustra a Tabela 6, as informações realizadas no Mapeamento Sistemático contendo os ataques mais realizados pelos autores nas publicações.

De acordo com a Tabela 6, percebe-se a quantidade de ataques mais praticados, onde o ataque de Força Bruta com 83,3% e o ataque de *Scan* com o mesmo percentual, são os mais realizados pelos *pentesters* e pelos invasores, por se tratar de práticas que exploram e concretizam uma invasão.

Conforme Coelho et. al (2015), o ataque de força bruta (*brute force*) consiste no ataque de tentativa de quebra de senha, exploração de senhas fracas, realizando testes até encontrar a correta, o software só termina de processar quando encontra a combinação de senha certa, este método precisa ter um usuário validado. No trabalho de Silva e Martins (2014), a ferramenta Medusa foi utilizada para obter acesso aos serviços remotos através de uma lista de senhas por padrão, mas que pode ser editada, o software compara as senhas

até encontrar, quando identifica exibe o usuário e senha para o atacante. A partir daí o atacante tem total acesso ao sistema invadido.

Tabela 6. Ataques encontrados nas publicações

ID	Tipo de Ataque	Citações	% de Citações
[A01]	Ataque de Força Bruta	[P02],[P03],[P04],[P05][P11]	83,3% (5/6)
[A02]	Ataque de Scan	[P02],[P03],[P05],[P06],[P07]	83,3% (5/6)
[A03]	Ataque de SQL Injection	[P01],[P03],[P04],[P09]	66,6% (4/6)
[A04]	Ataque de Denial of Service – DoS	[P02].[P11]	33,3% (2/6)
[A05]	Ataque de Cross-Site Scription	[P09]	16,6% (1/6)
[A06]	Ataque CSRF	[P09]	16,6% (1/6)

O ataque *Scan* pode ser considerado como o primeiro a ser utilizado quando não se tem as informações suficientes do alvo. No trabalho de Cordeiro (2020), ele utilizou a ferramenta Nmap para saber quais hosts estavam ativos, depois usou para verificar quais serviços ainda persistia ativo, após a obtenção das informações ele explorou o escaneamento para saber qual o sistema operacional e a sua versão, para assim poder extrair informações de vulnerabilidades do sistema. De posse dessas informações, o próximo passo é utilizar outras ferramentas com características específicas para determinado tipo de ataque.

5. Conclusão

A maioria das pesquisas relacionadas à segurança da informação aborda a necessidade de proteção do maior bem de uma organização, a informação. Dentro destas ramificações, o campo de pesquisa das ferramentas limita-se apenas em comparar o uso de uma ferramenta com outra similar, a fim de quantificar a sua eficiência ou até mesmo demonstrar quais as vulnerabilidades expostas na rede ou sistema. Uma vulnerabilidade computacional pode ser composta, principalmente, de sete potenciais ameaças: físicas, naturais, humanas, hardware, software, mídias digitais e a comunicação (engenharia social).

Através da percepção obtida do levantamento das ferramentas de detecção de intrusão em ambientes organizacionais, percebeu-se que a maioria dos ataques são de força bruta e varredura de portas, sendo essas formas bastante explorada como meio de obter acesso autorizado aos sistemas e redes. Poucas empresas se preocupam com estes tipos de ataques, pois algumas não tem a visão de capacitar e incentivar em seus profissionais a lidar com esses tipos problemas específicos e que exigem um grau de conhecimento técnico e amplo, não imaginam que um possível ataque venha comprometer a integridade de seus sistemas e infraestrutura. Uma forma de se prevenir em investir em soluções que auxiliem na identificação dessas ameaças, conquanto, não as evitem totalmente, todavia tornará os trabalhos do mal-intencionado mais difícil.

Além da percepção do mercado, este trabalho também realizou uma pesquisa da literatura, baseada no Mapeamento Sistemático, cujo objetivo foi realizar um levantamento das principais ferramentas utilizadas nos processos de *pentest*, utilizado por

usuários profissionais e estudantes, dotados com o conhecimento na área de segurança da informação.

Durante as análises realizadas na literatura, constatou-se nos trabalhos que a maioria das ferramentas utilizadas foram empregadas em ambientes controlados, ou seja, alguns testes foram realizados em laboratórios virtuais, a fim de ser possível mensurar o nível de eficiência das ferramentas e levantar as principais vulnerabilidades detectadas nos sistemas. Alguns ataques foram implementados para verificar o comportamento das máquinas de destino, também em servidores para detectar as portas e serviços ativos.

Com isso, percebe-se a importância dos cuidados relacionados à segurança da informação. Atualmente, existem vários métodos de ataques, dentre eles: a Engenharia Social, que não precisa de software para extrair dados, apenas uma conversa é o suficiente para comprometer a integridade de um sistema ou até mesmo de uma organização. Quase todos os dias, somos noticiados de ataques hackers a órgãos públicos e entidades privadas que têm seus dados usurpados por criminosos, que tentam receber uma recompensa em troca dos dados. A falta de incentivos de políticas e capacitação na área, pode ser um gargalo nesses momentos. As tecnologias sempre virão acompanhadas de suas vulnerabilidades, cabendo ao profissional de segurança da informação estar preparado para esse esforço contínuo.

Não obstante, com a leitura dos artigos analisou-se as recomendações de teste com outras ferramentas e outros tipos de ataque a serem pesquisados. Pois, certamente valerão e grande cunho de conhecimento para muitos que tem o interesse na área de segurança da informação.

5.1 Limitações

As limitações encontradas foram a escassez de artigos relacionados ao assunto de ferramentas de detecção de intrusão nos últimos anos nas publicações nacionais tanto em revistas como em sites, que abordassem todo o processo, aplicação e usabilidade.

Nas publicações de revistas internacionais foram mínimos os artigos que versassem sobre o tema, talvez por se tratar de um assunto que possa comprometer a integridade de organizações e sistemas, caso seja utilizado por pessoas mal-intencionadas.

5.2 Perspectivas Futuras

Com o intuito de estender a linha de pesquisa nessa área, recomenda-se a realização de experimentos na prática, simulando os ataques e medindo o tempo que leva para que um ataque se concretize, desde a fase de preparação até a fase de geração de relatórios.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2005.120p.

BASILI, V.; CALDEIRA, G.; ROMBACH, H. **The Experience Factory**. In: Encyclopedia of Software Engineering, New York, 1994.

CERT.BR (São Paulo). Comitê Gestor da Internet No Brasil. **Cartilha de Segurança para Internet**. Versão 4.0. São Paulo, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 07 mar 2021.

COELHO, M. S.; TOMASI, L. A.; IDALINO, T. B.; MARTINA, J. E. **Identificando vulnerabilidades de segurança em uma aplicação web**. Anais do XV Simpósio Brasileiro Em Segurança Da Informação E De Sistemas Computacionais, pg. 486-489.

CORDEIRO, D. L. S.; FERNANDES, S. R. **"Análise de Vulnerabilidades de Sites Web"**. Seminário de Trabalho de Conclusão de Curso do Bacharelado de Sistemas de Informação - Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas - Campus Juiz de Fora, 2017. Disponível em: http://periodicos.jf.ifsudestemg.edu.br/revistabsi/article/view/199/90. Acesso em: 05 abr 2021.

FERREIRA, M. F. T.; ROCHA, T. de S.; MARTINS, G. B.; SOUTO, E. **"Análise de Vulnerabilidades em Sistemas Computacionais Modernos: Conceitos, Exploits e Proteções"**. Minicursos do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2012.

FERRÃO, I. G.; KREUTZ, D. **"Segurança na Web: análise black-box de scanners de vulnerabilidades"**. Anais da 1ª Escola Regional Engenharia de Software (ERES 2017). ALEGRETE, RS - BRASIL, 2017.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores: Uma abordagem Top-Down**. McGraw-Hill, 2013.

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

JACOBSEN, W.; FREITAS, M. P.; ROTONDO, G.; ALMEIDA, D.; CAMARGO, A.; AMARAL, E. Um Estudo Sobre a Análise de Vulnerabilidades em Sistemas Computacionais - das Ferramentas ao Uso. Disponível em: https://www.researchgate.net/publication/279590036_Um_Estudo_Sobre_a_Analise

_de_Vulnerabilidades_em_Sistemas_Computacionais_-_das_Ferramentas_ao_Uso. Acesso em: 30 mar 2021.

KITCHENHAM, B.; CHARTERS, S. **"Guidelines for Performing Systematic Literature Reviews in Software Engineering"**. Relatório Técnico Evidence-Based Software Engineering (EBSE), v. 2.3, 2007.

K. PETERSEN, R. FELDT, S. MUJTABA, M. MATTSSON, **"Systematic Mapping Studies in Software Engineering"**, in: 12th International Conference on Evaluation and Assessment in Software Engineering, Australia, 2008.

MARTINELO, C. A. G.; BELLEZI, M. A. **"Análise de Vulnerabilidades com OpenVAS e Nessus"**. T.I.S. São Carlos, v. 3, n. 1, p. 34-44, jan-abr 2014. Disponível em: http://revistatis.dc.ufscar.br/index.php/revista/article/download/74/68. Acesso em: 07 abr 2021.

MARTINS, J. DOS S.; **"Exploração de Vulnerabilidades em Redes IOT"**. Fundação Educacional do Município de Assis e Instituto Municipal de Ensino Superior de Assis - Campus José Santilli Sobrinho. Assis - São Paulo, 2018. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1511420616.pdf. Acesso em: 06 abr 2021.

MARTINS, H. DOS S.; CARDOSO, F. E. **"Testes de Vulnerabilidades em Sistemas Web"**. Fundação Educacional do Município de Assis e Instituto Municipal de Ensino Superior de Assis - Campus José Santilli Sobrinho. Assis - São Paulo, 2018. Disponível em: https://cepein.femanet.com.br/BDigital/arqPics/1811550301P887.pdf. Acesso em: 06 abr 2021.

MELO, SANDRO. **Exploração de Vulnerabilidades em Redes TCP/IP** / Sandro Melo. 3ª ed. - Rio de Janeiro : Alta Books, 2017.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATISSON, M. **"Systematic Mapping Studies in Software Engineering"**. In Proceedings of the Evaluation and Assessment in Software Engireening (EASE), Bari, Italy, 2008.

OLIVEIRA, R. **Os 7 principais tipos de vulnerabilidades em uma empresa.** NEC Latin America S.A. 2017. Disponível em: https://blog.nec.com.br/os-7-principais-tipos-de-vulnerabilidades-em-uma-empresa. Acesso em: 05 mai 2021

SILVA, R. F. ; PEREIRA, J. C. **"Identificando Vulnerabilidades de Segurança Computacional"**. Universidade Paranaense - UNIPAR, 2013. Disponível em:

http://antigo.unipar.br/~seinpar/2013/artigos/Raquel%20Fonseca%20da%20Silva.pdf . Acesso em: 07 mai 2021.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes: Princípios e Práticas**; tradução Daniel Vieira, revisão técnica Paulo Sérgio Licciardi Messeder Barreto, Rafael Misoczki - 6 ed. - São Paulo: Pearson Education do Brasil, 2015.

WEIDMAN, GEORGIA. **Testes de Invasão: Uma introdução prática ao hacking**. Novatec Editora Ltda. São Paulo, 2014.

APÊNDICE I – QUESTIONÁRIO APLICADO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIMENTO

Prezado(a) Participante,

Meu nome é David Gleyson Ramos, sou aluno da Universidade Federal do Amazonas e do curso de Sistemas de Informação. Estou realizando um levantamento sobre as principais ferramentas de detecção de intrusão e principais ataques cibernéticos contra as empresas, todas essas informações serão utilizadas para o meu Trabalho de Conclusão de Curso, sob a orientação do Prof. Dr. Rainer Xavier de Amorim, cujo objetivo é construir um artigo científico que explore essa área da Tecnologia da Informação pouco abordada e contribuir para prevenção e segurança dos sistemas.

A participação na pesquisa é voluntária e a qualquer momento você pode retirar o seu consentimento em participar, se o desejar. Caso concorde em participar, você será solicitado a responder um questionário, dedicando cerca de 10 minutos para isso. Um dos riscos associados à pesquisa são o desconforto ao responder alguma pergunta, e nesse caso você pode deixar de responder à pergunta caso ela seja opcional, ou retirar seu consentimento em participar caso ela não seja opcional, sem qualquer prejuízo para você. Outro risco é o de vazamento de dados de suas respostas ao questionário. Contudo, garantimos que seus dados serão tratados com sigilo e confidencialidade, de forma a preservar sua privacidade.

Além disso, na divulgação dos resultados as respostas dos questionários serão apresentadas de forma agregada aos dados para fortalecer ainda mais o anonimato, evitando que seja possível vincular comportamentos/respostas a indivíduos. Eventualmente, será feita a citação de trechos das respostas às questões abertas no texto de artigos científicos que resultem dessa pesquisa. Contudo, qualquer citação será feita em total anonimato, sem associação com o nome dos envolvidos.

Sua participação nos ajudará no esclarecimento de soluções tecnológicas para combater e proteger os ambientes computacionais, através deste questionário. Sua contribuição é muito importante para a conclusão deste trabalho.

Sua participação nos ajudará no esclarecimento de soluções tecnológicas para combater e proteger os ambientes computacionais, através deste questionário. Sua contribuição é muito importante para a conclusão deste trabalho.

*Obrigatório

1. E-mail *

_____

2. Declaração de Consentimento: Li ou alguém leu para mim as informações contidas neste documento antes de assinar este termo de consentimento. Declaro que toda a linguagem técnica utilizada na descrição deste estudo de pesquisa foi explicada satisfatoriamente e que recebi respostas para todas as minhas dúvidas. Confirmo também que recebi uma cópia deste Termo de Consentimento Livre e Esclarecido. Compreendo que sou livre para me retirar do estudo em qualquer momento, sem qualquer penalidade. Declaro ter mais de 18 anos e dou meu consentimento de livre e espontânea vontade para participar deste estudo. *

Marcar apenas uma oval.

[ ] Li e concordo

[ ] Não Concordo

Questionário sobre as principais ferramentas de detecção de intrusão e principais ataques sofridos nas empresas que tenham uma infraestrutura de redes

1. Quais os principais tipos de ataques que são detectados diariamente/semanalmente? *

Marcar apenas uma oval.

[ ] Ataque varredura de portas

[ ] Ataque de Força Bruta

[ ] Ataque de SQL Injection

[ ] Ataque de Negação de Serviço

Outro: _____

2. Na empresa/instituição em que eu trabalho e/ou presto serviços é utilizado algum mecanismo de segurança para conter esses ataques. *

Marcar apenas uma oval.

[ ] Discordo totalmente

[ ] Discordo em grande parte

[ ] Discordo em parte

[ ] Neutro

[ ] Concordo em parte

[ ] Concordo em grande parte

[ ] Concordo totalmente

3. Caso a empresa/instituição em que você trabalha e/ou presta serviços implementa algum mecanismo de segurança, que tipos são implementados? *

Marcar apenas uma oval.

[ ] Hardware

[ ] Software

[ ] Hardware/Software

[ ] Nenhum

Outro: _____

4. Qual a incidência de ataques de força bruta em relação a outros ataques? *

Marcar apenas uma oval.

[ ] 50%

[ ] acima de 50%

[ ] abaixo de 50%

Outro: _____

5. Qual a frequência dos ataques de SQL Injection em relação a outros ataques? *

Marcar apenas uma oval.

[ ] 50%

[ ] acima de 50%

[ ] abaixo de 50%

Outro: _____

6. Qual a incidência de ataques de Negação de Serviço (DoS/DDoS) em relação a outros ataques? *

Marcar apenas uma oval.

[ ] 50%

[ ] acima de 50%

[ ] abaixo de 50%

Outro: _____

7. As ferramentas para detecção de intrusão utilizadas na organização possuem qual tipo de licença de software? *

Marcar apenas uma oval.

[ ] Software Livre

[ ] Software Proprietário

[ ] Software Comercial

[ ] Software de Código Aberto

[ ] Software Gratuito

Outro: _____

8. Na organização já foram utilizadas algumas dessas ferramentas elencadas abaixo para detecção de algum ataque? *

Marcar apenas uma oval.

[ ] Nmap

[ ] OpenVAS

[ ] VEGA

[ ] Attack Zed Proxy

[ ] Suricata

[ ] Hijacking Attack

[ ] Acutinex

[ ] Medusa

[ ] Nessus

[ ] SQLMap

[ ] Snort

[ ] Wireshark

[ ] Burp Suite

Outro: _____

9. Na empresa/instituição em que eu trabalho e/ou presto serviços existe alguma uma política organizacional que garanta a capacitação dos profissionais, que nela atuam, através de cursos e certificações na área de segurança da informação e de redes. *

Marcar apenas uma oval.

[ ] Discordo totalmente

[ ] Discordo em grande parte

[ ] Discordo em parte

[ ] Neutro

[ ] Concordo em parte

[ ] Concordo em grande parte

[ ] Concordo totalmente

10. Na política organizacional de segurança da informação da empresa/instituição em que eu trabalho e/ou presto serviços há algo previsto que em relação ao comportamento de risco dos funcionários, de forma que pode-se afirmar que existe uma conscientização a respeito do sigilo, integridade e confidencialidade das informações trocadas. *

Marcar apenas uma oval.

[ ] Discordo totalmente

[ ] Discordo em grande parte

[ ] Discordo em parte

[ ] Neutro

[ ] Concordo em parte

[ ] Concordo em grande parte

[ ] Concordo totalmente

11. Fique à vontade para contribuir com relatos de experiências e/ou sugestões para a nossa pesquisa:

_____

_____

APÊNDICE II – TABELA DE EXTRAÇÃO DE DADOS

1) Dados da publicação:	
Título:	Internal Threat Defense using Network Access Control and Intrusion Prevention System
Autor(es):	Putra, A. S.; Surantha, N.
Fonte de Publicação:	SCOPUS
Ano da Publicação:	2019
Resumo:	No estudo é criado um sistema de segurança de rede para realizar testes de ataques internos e para reduzir ameaças internas.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foi utilizado a ferramentas de varredura de portas para verificar os serviços ativos e dispositivos presentes na rede interna.
Quais as consequências dos ataques:	Os ataques tentaram invadir uma infraestrutura implementada com NAC e IPS em uma rede interna.
Os resultados dos testes mostraram eficiência:	Os resultados obtidos com os testes mostraram que a integração de NAC e IPS é melhor do que apenas o NAC, ou seja, os mecanismos trabalhando juntos evitam ataques internos.

2) Dados da publicação:	
Título:	Análise conceitual e comparativa entre Sistemas de Detecção de Intrusão
Autor(es):	Beraldo, L.; Pedroso, D.; Bruno, F. G.; Ito, F. T.
Fonte de Publicação:	WSCDC - SBSeg
Ano da Publicação:	2018
Resumo:	O estudo apresentou as ferramentas utilizadas como sistema de detecção de intrusão para analisar tráfego suspeito em redes.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	As ferramentas empregadas foram Snort, Suricata e o Bro.
Quais as consequências dos ataques:	Realizar captura de pacotes de ataques legítimos misturados com atividades maliciosas.
Os resultados dos testes mostraram eficiência:	Os testes apresentaram relatórios com alertas gerados e recursos de processamento e memória utilizado pelos IDS.

3) Dados da publicação:	
Título:	Estudo e Análise de Vulnerabilidades Web
Autor(es):	Monteverde W. A.; Campiolo, R.
Fonte de Publicação:	SBSEG
Ano da Publicação:	2014
Resumo:	O trabalho é realizado um estudo e a análise de vulnerabilidades em diferentes tipos de aplicações Web.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	As ferramentas aplicadas no estudo foram W3af, Vega, Burp Suite, Wireshark, SqlMap e John The Ripper.
Quais as consequências dos ataques:	Os scanners possibilitaram a identificação das vulnerabilidades existentes nos sítios da Web, bem como as URLs e parâmetros vulneráveis nas aplicações.
Os resultados dos testes mostraram eficiência:	Os experimentos foram realizados em cenários reais, as vulnerabilidades encontradas foram reportas as responsáveis pelos sítios Web.

4) Dados da publicação:	
Título:	Identificando vulnerabilidades de segurança em uma aplicação web
Autor(es):	Coelho, M. S.; Tomasi, L. A.; Idalino, T. B.; Martina, J. E.
Fonte de Publicação:	SBSEG
Ano da Publicação:	2015
Resumo:	O artigo teve como objetivo apresentar testes realizados por ferramentas descritas no Manual Padrão OAWASP, para verificar a eficiência delas em ambientes virtuais.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	As ferramentas aplicadas foram conforme o guia padrão da OAWASP.
Quais as consequências dos ataques:	Foram realizados ataques de força bruta e Cross Site Scripting, os ataques emitiram alertas de invasão.
Os resultados dos testes mostraram eficiência:	O uso das ferramentas se mostrou eficiente mostrando os avisos de invasão através das ferramentas de detecção.

5) Dados da publicação:	
Título:	O uso da ferramenta de honeypot para a segurança de redes
Autor(es):	Silva, P. R.; Martins, D. M. S.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2014
Resumo:	O estudo apresentou a coleta de informações de ataques a redes computacionais.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foi utilizado um dispositivo Raspberry PI para hospedar um Honeypot que ia ser usado para ser atacado.
Quais as consequências dos ataques:	Mostrar a exploração de uma senha fraca.
Os resultados dos testes mostraram eficiência:	Os resultados demonstraram o potencial uso da ferramenta para apoiar a segurança de redes computacionais

6) Dados da publicação:	
Título:	Análise de Vulnerabilidades com OpenVAS e Nessus
Autor(es):	Martinelo, C. A. G.; Bellezi, M. A.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2014
Resumo:	O trabalho teve como objetivo utilizar ferramentas de varreduras para identificar possíveis vulnerabilidades em uma rede.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foram utilizados os softwares OpenVAS e Nessus para realizar comparar resultados de varreduras.
Quais as consequências dos ataques:	Identificar as vulnerabilidades presentes em uma rede e automatizar as correções antes de ser exploradas por um atacante.
Os resultados dos testes mostraram eficiência:	Foi possível verificar que os softwares testados foram capazes de detectar as vulnerabilidades no ambiente.

7) Dados da publicação:	
Título:	Um Estudo Sobre a Análise de Vulnerabilidades em Sistemas Computacionais - das Ferramentas ao Uso
Autor(es):	Jacobsen, W.;Freitas, M. P.; Rotondo, G.; Almeida, D.; Camargo, A.; Amaral, É.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2014
Resumo:	O trabalho aborda a importância da segurança da informação e análise de vulnerabilidades em sistemas computacionais.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foi aplicado um conjunto de experimentos com os scanners Nessus e OpenVas.
Quais as consequências dos ataques:	Foi feita uma comparação dos ataques de scanners para mensurar as características entre os dois softwares.
Os resultados dos testes mostraram eficiência:	Foram propostos e implementados experimentos, com diferentes ferramentas, a fim de identificar as vulnerabilidades.

8) Dados da publicação:	
Título:	Auditoria de Segurança da Informação em Sistemas e Aplicações
Autor(es):	Cruz, C. M. B. R.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2017
Resumo:	O trabalho contribui para o uso de auditoria de segurança da informação em sistemas e aplicações web, usando o processo de análise de vulnerabilidade, através dos testes de penetração.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foram utilizadas as ferramentas Nmap, WhatWeb, Vega, Nessus, OpenVas,W3af, Sqlmap.
Quais as consequências dos ataques:	Foram realizados diversos ataques em um data center de um órgão público, com isso detectou várias vulnerabilidades em serviços e portas.
Os resultados dos testes mostraram eficiência:	Os experimentos foram realizados em sistema em produção e resultados foram apresentados aos gestores para possibilitar a mitigação das vulnerabilidades encontradas.

9) Dados da publicação:	
Título:	Detecção e análise de vulnerabilidades em um servidor OJS utilizando teste de penetração
Autor(es):	Maciel, D. P.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2019
Resumo:	O trabalho teve como objetivo detectar e analisar possíveis vulnerabilidades existentes em um servidor OJS local.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foram realizados vários ataques com as ferramentas Acutinex e o OAWASP ZAP.
Quais as consequências dos ataques:	O Acutinex encontrou mais vulnerabilidades que potencial de prejudicar o servidor OJS, em comparação ao OAWASP ZAP.
Os resultados dos testes mostraram eficiência:	O uso das ferramentas se mostraram eficiente em sua finalidade de emprego.

10) Dados da publicação:	
Título:	Teste de invasão em aplicações web utilizando SQL Injection: Um estudo Epistemológico
Autor(es):	Carneiro, A. S. L.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2017
Resumo:	A trabalho investiga como realizar teste de invasão em aplicações web utilizando SQL Injection.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	Foi utilizada ferramentas para automatizar o *pentesting* em aplicações web com Sql Injection.
Quais as consequências dos ataques:	A utilização desses ataques se torna perigoso, pois é difícil de ser descoberto em aplicações web.
Os resultados dos testes mostraram eficiência:	O uso das ferramentas se mostrou eficiente atendendo a finalidade atacar por meio do SQl Injection.

11) Dados da publicação:	
Título:	Aplicação de técnicas de Ethical Hacking – Demonstração do uso de ferramentas e ambiente de Estudo para acadêmicos ou iniciantes em segurança Web
Autor(es):	Cordeiro, F. A.
Fonte de Publicação:	Google Acadêmico
Ano da Publicação:	2020
Resumo:	O trabalho propôs um manual contendo técnicas de escaneamento, enumeração de vulnerabilidades e testes de penetração.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	As ferramentas aplicadas foram o Nmap e Metasploit.
Quais as consequências dos ataques:	Foram realizados testes em máquinas virtuais, para evitar danos em algum ambiente em produção.
Os resultados dos testes mostraram eficiência:	O uso das ferramentas exploraram as vulnerabilidades e apresentaram as falhas no sistema, tornando o processo eficiente.

12) Dados da publicação:	
Título:	Os 7 principais tipos de vulnerabilidades em uma empresa
Autor(es):	Oliveira, Rodrigo
Fonte de Publicação:	Sites
Ano da Publicação:	2017
Resumo:	O site apresenta os conceitos de Segurança da Informação e as principais ferramentas utilizadas como scanners.
Dados derivados do objetivo:	
Identificar o contexto de aplicação das ferramentas:	As ferramentas apresentadas são o Nessus e o Nmap para monitoração de vulnerabilidades e gestão do ambiente de redes.
Quais as consequências dos ataques:	Encontrar vulnerabilidades ativas pela rede.
Os resultados dos testes mostraram eficiência:	O uso das ferramentas se mostrou eficiente em sua finalidade de emprego.