UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

DEPARTAMENTO DE COMPUTAÇÃO
UFRPE

Vanessa Bandeira Lins Teixeira

Security Evaluation of Operating Systems Considering Compliance Policies

Recife

2021

Vanessa Bandeira Lins Teixeira

Security Evaluation of Operating Systems Considering Compliance Policies

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Universidade Federal Rural de Pernambuco – UFRPE

Departamento de Computação

Curso de Bacharelado em Ciência da Computação

Orientador: Fernando Antonio Aires Lins

Coorientador: Obionor de Oliveira Nóbrega

Recife

2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

T266s Teixeira, Vanessa Bandeira Lins
Security Evaluation of Operating Systems Considering Compliance Policies / Vanessa Bandeira Lins Teixeira. - 2021.
28 f. : il.

Orientador: Fernando Antonio Aires Lins.
Coorientador: Obionor de Oliveira Nobrega.
Inclui referências.

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal Rural de Pernambuco, Bacharelado em Ciência da Computação, Recife, 2021.

1. Vulnerability. 2. Mitigation. 3. Compliance policies. 4. Operating systems. 5. Configuration flaws. I. Lins, Fernando Antonio Aires, orient. II. Nobrega, Obionor de Oliveira, coorient. III. Título

CDD 004

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

http://www.bcc.ufrpe.br

FICHA DE APROVAÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO

Trabalho defendido por Vanessa Bandeira Lins Teixeira às 15 horas do dia 01 de março de 2021, no link meet.google.com/mir-atjp-xxo, como requisito para conclusão do curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco, intitulado Security Evaluation of Operating Systems Considering Compliance Policies, orientado por Fernando Antonio Aires Lins e aprovado pela seguinte banca examinadora:

Fernando Antonio Aires Lins
DC/UFRPE

Jeísa Pereira de Oliveira Domingues
DC/UFRPE

Agradecimentos

A Deus, pelo dom da vida, pela capacidade de planejar, sonhar e concretizar mais um sonho em minha caminhada.

Aos meus pais, Elizete Bandeira Lins e Suami Clemente Teixeira, pelos ensinamentos, valores humanos e por acreditarem na minha capacidade de superação e realização de meus sonhos e objetivos.

Ao professor Fernando Antônio Aires, por ser exemplo de profissional, pelas orientações, conselhos e conhecimentos transmitidos que compuseram e contribuíram com minha formação profissional. Agradeço também ao professor Obionor de Oliveira Nóbrega, pelo apoio no desenvolvimento do trabalho e por sempre acreditar no meu potencial como aluna.

Por fim, eu agradeço também ao Departamento de Computação da Universidade Federal Rural de Pernambuco que proporcionou os recursos necessários para a realização do trabalho.

Resumo

Atualmente, pesquisar, mitigar e solucionar vulnerabilidades de segurança é considerada uma tarefa relevante e complexa. Novos softwares são desenvolvidos todos os dias, e cada um deles pode trazer suas próprias vulnerabilidades. Além disso, as configurações desses aplicativos também podem aumentar essas vulnerabilidades. Nesse contexto, faltam configurações orientadas para a segurança em uma parte significativa dos sistemas operacionais atuais. Esses ativos, que geralmente não são configurados corretamente considerando os requisitos de segurança, tornam-se alvos fáceis para um número considerável de ataques à segurança. A aplicação de políticas de conformidade em um sistema operacional ajuda a preservar o ambiente contra explorações maliciosas. O objetivo principal deste trabalho é avaliar o uso de políticas de conformidade para avaliar e melhorar o nível de segurança dos sistemas operacionais. Para isso, uma metodologia é proposta e descrita. Essa metodologia também é aplicada a um estudo de caso com sistemas operacionais para servidores. Para o efeito, foram consideradas as falhas na configuração de fábrica dos sistemas operativos, às quais foram identificadas através das políticas de conformidade do *Center of Internet Security* (CIS). Assim, foi possível avaliar o nível de segurança dos sistemas e classificar as principais recomendações para priorizar as correções que os usuários podem seguir. Essas recomendações visam reduzir a superfície de ataques em sistemas e aumentar o nível de segurança, mitigando as vulnerabilidades às quais os sistemas estão expostos.

Palavras-chave: Vulnerabilidade, Mitigação, Políticas de conformidade, Sistemas operacionais, Falhas de configuração.

Abstract

Currently, to search, mitigate and solve security vulnerabilities is considered a relevant and complex task. New software are being developed everyday, and each one of them may bring its own vulnerabilities. In addition, the configurations of these applications can also increase these vulnerabilities. In this context, there is a lack of security-oriented configurations in a significant part of the current operating systems. These assets, which are usually not properly configured considering security requirements, become easy targets for a considered number of security attacks. The application of compliance policies in an operating system helps to preserve the environment from malicious exploitation. The main objective of this work is to evaluate the use of compliance policies to assess and improve the security level of operating systems. To achieve this, a methodology is proposed and described. This methodology is also applied to a case study with server operating systems. For this purpose, faults in the factory configuration of the operating systems were considered, which were identified using the Center for Internet Security (CIS) compliance policies. Thus, it became possible to evaluate the system security level and to classify the main recommendations for prioritizing the corrections that users can follow. Such recommendations aim to reduce the attacks surface on systems and increase the security level by mitigating the vulnerabilities to which the systems are exposed.

Keywords: Vulnerability, Mitigation, Compliance policies, Operating systems, Configuration flaws.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

Nos dias atuais, é comum a busca por práticas de segurança para tornar a vida mais protegida. É possível perceber a inserção destas práticas desde a criação de uma senha para a utilização de uma conta até o simples ato de se ativar o alarme de um carro. Adicionalmente, em um ambiente computacional, é necessário compreender que a ação de se proteger virtualmente requer protocolos mais específicos que possam prevenir que o usuário venha a ser atacado ou, pelo menos, mitigar os efeitos associados a este ataque. De modo geral, um ambiente com vulnerabilidades permite a um invasor aplicar técnicas que resultem, por exemplo, no acesso a informações confidenciais. Isto resulta na necessidade da adoção de medidas que evitem a ocorrência de incidentes de segurança, tornando os ambientes menos suscetíveis a explorações de vulnerabilidades.

As recorrentes violações de segurança a sistemas de informação e comunicação retratam o crescimento gradual das aberturas de sistemas deixadas pelos usuários, tornando-os alvos de possíveis ataques. Esse fato pode ser ilustrado a partir das 18.638 vulnerabilidades divulgadas no ano de 2020, um aumento de 183% sobre as publicações realizadas em 2015 (CAVEZA; QUINLAN, 2021). Diante deste considerável aumento no número de vulnerabilidades, o usuário se depara com o obstáculo de como priorizar as correções em seus sistemas através de práticas que mitiguem a ocorrência de ataques em sistemas computacionais.

Frequentemente, equipes de segurança, mais especificamente as *blue teams*, trabalham na avaliação diária dos sistemas a fim de proteger os ativos de vulnerabilidades que afetem dispositivos ou sistemas críticos das empresas (Veerasamy, 2009). Esse tipo de avaliação de segurança diária faz parte do contexto presente na gestão de vulnerabilidades e conformidades de um ambiente.

Além da identificação das ameaças, é fundamental que as práticas para mitigar as vulnerabilidades do ambiente sejam conhecidas e configuradas também nos sistemas operacionais, de modo a manter os ambientes das corporações protegidos, tendo em vista que a todo instante alguma vulnerabilidade pode estar sendo explorada por hackers. Um exemplo disso está ligado à vulnerabilidade nomeada como *ZeroLogon*, cujo número de identificação é CVE-2020-1472, a qual o atacante se beneficia a partir de falhas de autenticação de um computador associado a um domínio utilizando o serviço de autenticação *Netlogon*. Por esta razão, se faz possível a falsificação da identidade de qualquer conta de um computador, inclusive a do controlador de domínio, possibilitando a definição de uma senha para essa conta no domínio (The MITRE

Corporation, 2020). Casos como este evidenciam a necessidade de trabalhos que contribuam com a avaliação de segurança dos sistemas operacionais, enfatizando a adoção e melhoria de configurações de segurança, com o objetivo de tornar os ambientes menos expostos a ataques de usuários mal intencionados.

A importância de se avaliar a segurança de sistemas operacionais se torna ainda mais crítica quando essa análise é feita em sistemas operacionais para servidores. Ameaças envolvendo vulnerabilidades encontradas nestes sistemas operacionais tendem a gerar riscos mais significativos, pois estes sistemas em geral são usados para atividades críticas das empresas.

Neste contexto, este artigo tem como principal objetivo avaliar as configurações de segurança de sistemas operacionais atuais, com foco específico em sistemas operacionais para servidores. Através desta avaliação, torna-se possível incentivar boas práticas capazes de facilitar a compreensão dos usuários diante das vulnerabilidades e ameaças presentes e também apresentar as melhores alternativas de correções que os usuários podem seguir, com o intuito de mitigar as vulnerabilidades existentes. Para isto, este trabalho define uma metodologia de avaliação de segurança, e esta metodologia é aplicada a um estudo de caso envolvendo sistemas operacionais utilizados atualmente. Através da análise do estudo de caso, será possível identificar o grau de exposição ao qual os usuários estão ameaçados por não configurarem os sistemas de acordo com as normas e políticas de segurança disponíveis atualmente.

Este artigo está estruturado da forma que se segue. O Capítulo 2 apresenta os conceitos básicos importantes para o entendimento deste trabalho. O Capítulo 3 aborda os trabalhos relacionados a esta pesquisa. O Capítulo 4, descreve a metodologia para avaliação de segurança de sistemas operacionais para servidores observando políticas de conformidade. O Capítulo 5 introduz o estudo de caso, que serve tanto para ilustrar a metodologia como para possibilitar a análise de segurança dos sistemas operacionais escolhidos. Finalmente, as conclusões e os trabalhos futuros são detalhados no Capítulo 6.

2 Conceitos Básicos

2.1 Vulnerabilidade, Ameaça e Risco

Uma falha de segurança que pode ser explorada em um software, causando um impacto negativo na confidencialidade, integridade ou disponibilidade de um componente ou componentes afetados, define o conceito de vulnerabilidade (The MITRE Corporation, 2021).

Atrelado ao conceito de vulnerabilidade, verifica-se que uma ameaça é a causa potencial de um incidente indesejado, que pode resultar em danos para um sistema ou organização (CAVEZA; QUINLAN, 2018). Essas duas definições, estruturam o conceito de risco, que de acordo com a norma ISO/IEC 27000:2018, está associado com o potencial que as ameaças exploram ativos ou grupo de ativos de informação que possuem vulnerabilidades e, consequentemente, causam impactos negativos a uma organização (CAVEZA; QUINLAN, 2018).

É importante notar que estes conceitos estão relacionados. Para a avaliação de um risco, é necessário avaliar as ameaças e vulnerabilidades associadas ao mesmo. Além disso, para que uma vulnerabilidade seja explorada, é necessário que uma ameaça a explore. Desta forma, pode-se afirmar que reduzir o número de vulnerabilidades de um sistema é um passo importante para a melhoria do mesmo. Mas, a identificação e prevenção de possíveis ameaças também contribui para mitigar ou mesmo evitar possíveis riscos.

Vale ressaltar a importância da gestão de vulnerabilidades de um sistema computacional: mesmo que em um dado momento as vulnerabilidades sejam eliminadas, em um futuro pode ser que outras vulnerabilidades surjam por diversos motivos. Dentre esses motivos pode-se citar a criação de novos ataques e a inserção de novas vulnerabilidades decorrentes da aquisição de novos softwares ou mesmo atualização de softwares antigos.

2.2 Políticas de Conformidade de Segurança para Sistemas Operacionais

Grande parte das instituições voltadas à segurança cibernética concentram seus esforços no desenvolvimento de práticas de segurança. O *Center of Internet Security* (CIS) é uma organização sem fins lucrativos que tem como missão a defesa cibernética. Um dos seus principais entregáveis são as políticas de conformidade dos sistemas

operacionais (SECURITY, 2020a). Uma política de conformidade de segurança para sistemas operacionais é um documento que tem por finalidade garantir que estes sistemas sigam um procedimento com as melhores recomendações de segurança, de modo a apoiar os objetivos de segurança da organização (ANGRAINI; ALIAS; OKFALISA, 2019). Ou seja, são recomendações, estruturadas em categorias, compostas por itens de configurações de segurança para os ambientes, impactando na redução e mitigação de vulnerabilidades e ameaças. Essas recomendações são revisadas e atualizadas de maneira minuciosa por analistas de segurança.

3 Trabalhos Relacionados

Gorbenko *et al.* (Gorbenko et al., 2017), em seu trabalho, propõem a criação de um banco de dados com registros de vulnerabilidades de sistemas operacionais. As informações explicitadas pelos autores abrangem de maneira quantitativa as vulnerabilidades descobertas e corrigidas em sistemas operacionais, o tempo médio para a disponibilização de uma correção e uma análise sobre a criticidade das vulnerabilidades mais comuns para diferentes sistemas operacionais. O trabalho evidencia a necessidade de se entender as etapas associadas à gestão de uma vulnerabilidade.

Enquanto há um forte interesse na identificação dos padrões de ocorrências das vulnerabilidades, existe também uma abordagem prática, apresentada por Mounji *et al.* (Mounji; Le Charlier, 1997), voltada para auditoria de sistemas operacionais através da detecção de intrusão. Para esta detecção, se analisa os acessos não autorizados, que podem indicar a entrada de usuários mal-intencionados. Essa abordagem tem o foco no monitoramento do funcionamento do ambiente, e pode ser considerada uma alternativa complementar para a identificação de vulnerabilidades tradicionais.

No entanto, há uma carência de estudos sobre avaliações de conformidade em softwares usando metodologias específicas. Angraini *et al.* (ANGRAINI; ALIAS; OKFALISA, 2019) demonstra a necessidade de alinhamento dos modelos de políticas de conformidade de segurança dos sistemas operacionais com as políticas de segurança adotadas nas empresas por meio de uma revisão sistemática. Paralelamente a esta carência de estudos sobre políticas de conformidade para sistemas operacionais, existem poucos estudos de caso aplicados à área de gestão de conformidades, como foi descrito por Mesquida *et al.* (MESQUIDA; MAS, 2015).

Uma avaliação quantitativa de vulnerabilidades em sistemas operacionais é tratada no trabalho de Alhazmi *et al.* (Alhazmi; Malaiya, 2005), que avalia um banco de dados de vulnerabilidades como parâmetro para aplicação dos modelos matemáticos propostos para os sistemas operacionais abordados pelos autores. Contudo, o trabalho não apresenta avaliação ou estudo prático, seja ele simulado ou real.

Para sintetizar os trabalhos expostos nesta seção, os mesmos se encontram dispostos na Tabela 1. Os critérios para classificação destes trabalhos se baseiam em: 1) se utiliza *benchmarks* padronizados e difundidos, como os fornecidos pela CIS *benchmarks* (SECURITY, 2020a) e OWASP *benchmarks* (FOUNDATION, 2020); 2) se tem foco específico em sistemas operacionais e 3) se o artigo propõe metodologia ou alguma forma sistematizada de se fazer a avaliação.

Tabela 1 – Classificação dos trabalhos relacionados.

Trabalho	Utiliza *benchmarks* padronizados e difundidos?	Avalia sistemas operacionais?	Propõe metodologia?
(Gorbenko et al., 2017)	Não	Sim	Não
(Mounji; Le Charlier, 1997)	Não	Sim	Sim
(ANGRAINI; ALIAS; OKFALISA, 2019)	Não	Não	Não
(MESQUIDA; MAS, 2015)	Sim	Não	Não
(Alhazmi; Malaiya, 2005)	Não	Sim	Não

Dado o exposto na Tabela 1, pode-se observar que existe uma lacuna existente no estado da arte referente a proposta de metodologias que descrevem como fazer a avaliação de segurança de sistemas operacionais tomando como base políticas de conformidade e se utilizando de *benchmarks* padronizados e difundidos.

Baseado nesta lacuna, este trabalho propõe uma metodologia para a avaliação de segurança desejada, e também utiliza *benchmarks* conhecidos para a realização desta avaliação.

4 Metodologia para Avaliação de Segurança de Sistemas Operacionais Observando Políticas de Conformidade

Para a realização da avaliação de segurança proposta neste trabalho, é importante descrever a metodologia utilizada, de modo a detalhar as atividades necessárias para a realização desta. Esta metodologia objetiva também tornar esta pesquisa reproduzível, ou seja, com possibilidade de ser usada como base por outros pesquisadores em seus projetos de avaliação de segurança.

4.1 Visão Geral

Esta subseção tem como objetivo apresentar, de forma resumida, a metodologia proposta neste trabalho. Para a representação da mesma, foi adotado o padrão *Business Process Modeling Notation* (BPMN) (CAMPOS, 2014), que está sendo vastamente usado atualmente para a modelagem de processos. A Fig. 1 apresenta a modelagem da metodologia proposta.

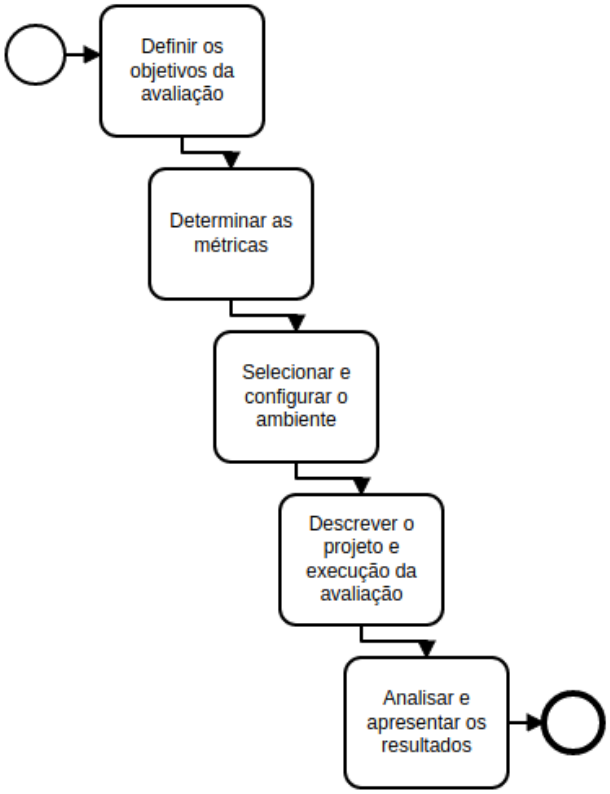

Figura 1 – Fluxograma da metodologia do trabalho.

O processo para a avaliação de segurança de sistemas operacionais considerando políticas de conformidade é disposto da seguinte maneira:

1. Definir objetivos da avaliação, com o intuito de, desde o início, especificar qual o foco da mesma;
2. Determinar as métricas que serão usadas para a realização da avaliação;
3. Selecionar e configurar o ambiente que será utilizado na avaliação;
4. Descrever o projeto e execução da avaliação;
5. Analisar e apresentar os resultados obtidos, de modo a serem geradas informações e recomendações úteis em relação ao nível de segurança atual do sistema.

4.2 Definir os objetivos da avaliação

Nesta atividade inicial, são definidos os objetivos a serem perseguidos dentro da avaliação de segurança. Esses objetivos podem incluir, por exemplo: avaliar a segurança de sistemas operacionais móveis considerando políticas de conformidade, analisar os impactos da aplicação de políticas de conformidade perante as vulnerabilidades do sistema ou classificar o nível de segurança dos sistemas operacionais (desktop) observando diferentes tipos de configurações de usuários. Ao definir os objetivos, a avaliação perde o caráter subjetivo e ganha um caráter prático. Isto é importante porque não é recomendado afirmar que uma configuração está correta ou não sem que existam objetivos e métricas atrelados.

4.3 Determinar as métricas

Nesta atividade, serão definidas as métricas para análise dos resultados, de modo a sistematizar a quantificação destes. Em outras palavras, para a realização de uma avaliação de sistemas utilizando políticas de conformidade, é importante definir como será feita a análise dos resultados. Exemplo de métricas incluem: número de vulnerabilidades (quantificação das vulnerabilidades encontradas baseadas nas suas criticidades) e nível de conformidade (número percentual que indica quantos dos controles de segurança estão aderentes com a política de conformidade adotada).

4.4 Selecionar e configurar o ambiente

Esta atividade consiste na definição e configuração dos ativos que farão parte do ambiente. Por exemplo, nesta atividade se define o hardware utilizado (incluindo

informações como processamento, armazenamento, etc) e softwares instalados (sistemas operacionais, aplicações do usuário, dentre outras).

Um ponto importante a ser ressaltado está ligado à necessidade de se conhecer o perfil ao qual são destinados os ativos tecnológicos. Por exemplo, os sistemas operacionais voltados ao uso como servidores podem ser estruturados com um domínio, ou para os casos de servidores Windows devem ter as configurações de controlador de domínio. Importante ressaltar que nesta atividade também são detalhadas informações como versão do sistema operacional, pois a depender desta versão a quantidade de vulnerabilidades pode diferir. Finalmente, vale destacar que, nesta etapa, toda a configuração do ambiente, incluindo aspectos de rede, como definição do endereço IP, devem ser realizadas.

4.5 Descrever o projeto e execução da avaliação

Nesta atividade ocorrerá a definição e a execução da avaliação, seguindo os objetivos e características definidos nas seções anteriores. A descrição do projeto de avaliação proposto neste artigo é composta, dentre outros artefatos, de arquivos de auditoria do sistema operacional e a definição de uma política de verificação do ambiente.

O processo de criação dos arquivos de auditoria parte da iniciativa de verificar se as configurações do sistema operacional estão de acordo com as recomendações de segurança (SECURITY, 2020a). Mediante os arquivos de auditoria é possível aplicar as políticas de conformidade de maneira a serem interpretadas pelos sistemas operacionais. A partir disso, a avaliação de conformidade pode ser realizada. Um exemplo de estrutura básica de um item presente em um arquivo de auditoria pode ser observado na Fig. 2. Cada item é verificado por meio do marcador *custom_item*. Esses marcadores são estruturados com palavras chaves que serão interpretadas pela ferramenta de varredura de vulnerabilidades, com o intuito de identificar se o sistema operacional está conforme ou não as recomendações de segurança.

```
<custom_item>
          system      : Sistema operacional
          type        : Método de checagem
          description : Descrição do item de configuração
          cmd         : Comando utilizado para a checagem
          expect      : Valor esperado
</custom_item>
```

Figura 2 – Estrutura básica de um item do arquivo de auditoria.

A utilização da ferramenta de varredura de vulnerabilidades é essencial para a coleta de informações relacionadas ao estado do ambiente e na identificação de possíveis não conformidades. Esses dados são obtidos com o uso dos arquivos de auditoria que definem o valor esperado para cada configuração de segurança aplicada aos sistemas operacionais, baseado nas políticas de conformidade desses sistemas. Para isso, é necessário que esta ferramenta receba as configurações necessárias para a sua instalação no ativo que irá hospedá-lo.

A última fase do projeto é instituída com a criação de uma política de verificação do ambiente. Para o procedimento de checagem das configurações de um sistema, atribui-se a ferramenta de varredura de vulnerabilidades as informações de identificação do ativo analisado na rede, como: Endereço IP, credenciais de autenticação, arquivo de auditoria do sistema, domínio ao qual pertence a máquina, caso exista, e uma seleção de plugins de auditoria que são disponibilizados pela ferramenta de varredura de vulnerabilidades escolhida. Essas informações são necessárias para que a ferramenta de varredura de vulnerabilidades, como o Nessus (TENABLE, 2021), identifique o ativo que será avaliado.

4.6 Analisar e apresentar os resultados

A etapa final da metodologia compreende a análise dos dados que foram retornados após a execução da avaliação. As informações retornadas pela ferramenta de varredura podem estar estruturadas em arquivos como html, pdf ou csv, contendo as informações relacionadas às configurações que foram verificadas. Esses dados podem ser constituídos por itens de configuração que falharam quando analisados sob a ótica das políticas de conformidade dos sistemas operacionais escolhidos.

É importante que sejam consideradas as métricas determinadas previamente como descrito na subseção C, relacionando-as com os objetivos definidos para a aplicação da metodologia. Essas métricas auxiliarão na filtragem e organização dos dados, como a criação de gráficos que facilitem a visualização e apresentação das informações, a fim de alcançar os objetivos pretendidos e possíveis resultados.

5 Avaliação

Esta seção visa executar a metodologia proposta através da adoção de um estudo de caso. O estudo de caso adotado visa analisar a segurança de sistemas operacionais voltados para servidores comumente usados por empresas, já que esses tipos de sistemas operacionais, em sua maioria, hospedam serviços compartilhados e a ocorrência de vulnerabilidades nesses sistemas podem impactar em riscos mais altos (The MITRE Corporation, 2020).

5.1 Definição dos objetivos da avaliação

O objetivo principal deste estudo de caso é avaliar a segurança de sistemas operacionais para servidores considerando políticas de conformidade, focando em configurações que não estavam conforme as recomendações de segurança. Além disso, o trabalho busca incentivar boas práticas capazes de facilitar o entendimento dos usuários perante as vulnerabilidades e ameaças presentes, apresentando as principais alternativas de correção das configurações.

5.2 Determinação da métrica

A métrica adotada neste estudo de caso para medir o nível de conformidade é o índice de conformidade, que representa o retorno identificado por cada política de conformidade considerando as configurações dos sistemas operacionais (SECURITY, 2020a). Essa métrica auxilia na análise e categorização dos resultados. Os valores possíveis para esta métrica são: Aceito, para a configuração que está de acordo com as recomendações de segurança, e Falho, para a configuração que não está de acordo com as recomendações de segurança.

5.3 Seleção e configuração do ambiente

Para a seleção dos sistemas operacionais a serem adotados nesta avaliação, foi utilizada uma listagem publicada pelo CVE Details com as 50 principais versões de sistemas operacionais com mais vulnerabilidades de segurança relacionadas a eles (SECURITY, 2020b). Dos 50 sistemas operacionais, dois se destacaram e foram selecionados: o Debian 8 e a versão Windows Server 2012 R2. A partir desta seleção foram criadas máquinas virtuais para a emulação destes sistemas nas configurações de fábrica. A máquina virtual criada para o Windows Server 2012 R2 apresenta as se-

guintes características: Memória RAM de 2GB, disco rígido com 60GB e 1 processador. Já a máquina virtual dedicada ao Debian 8 apresenta a seguinte configuração: Memória RAM de 2GB, disco rígido de 20GB e 1 processador. Para o servidor Windows, foi criada uma diretiva de grupo, ou do inglês, *Group Policy Object* (GPO), definida como UFRPE.br. Essa GPO realiza o gerenciamento das configurações do ambiente de maneira centralizada (MOSKOWITZ, 2015).

5.4 Descrição do projeto e execução da avaliação

A criação dos arquivos de auditoria foi realizada baseada nas políticas de conformidade do Debian 8 e do Windows Server 2012 R2 fornecidos pela CIS *benchmarks*, que é uma organização referência em *benchmarks* de segurança e um dos mais adotados para esta finalidade (SECURITY, 2020a). Além disso, foram consultados os arquivos disponibilizados no site do Nessus (TENABLE, 2021) que direcionam o usuário na criação do arquivo de auditoria do sistema operacional.

```
<custom_item>
      system      : "Linux"
      type        : CMD_EXEC
      description : "3.4.1 Ensure DCCP is disabled - modprobe"
      cmd         : "/sbin/modprobe -n -v dccp"
      expect      : "install[\\s]+/bin/true"
</custom_item>
```

Figura 3 – Item de auditoria de configuração no Debian 8.

A seleção da ferramenta de varredura de vulnerabilidades, para a avaliação das configurações dos sistemas operacionais foi baseada na comparação destes softwares realizada por Chalvatzis *et al.* (Chalvatzis; Karras; Papademetriou, 2019), que descreveram o Nessus como uma alternativa interessante devido ao seu domínio de mercado, documentação acessível e a disponibilidade de um banco de dados de vulnerabilidades atualizado. Baseado nisto, foi feita a instalação do Nessus, na versão 8, no Windows Server 2012 R2 por meio de um arquivo de extensão .msi, próprio para o ambiente Windows. Como as duas máquinas virtuais estavam sob a mesma rede não foi necessária a instalação do Nessus no Debian 8.

Com a instalação do Nessus realizada e os arquivos de auditoria criados, a etapa de criação de uma política de verificação pôde ser iniciada. Essa criação foi realizada com a passagem dos parâmetros relativos aos sistemas operacionais que foram objetos do estudo, sendo o endereço IP e métodos de autenticação as principais informações.

O método de autenticação aplicado ao Debian foi por meio do protocolo seguro para logins remotos, *Secure Shell*, ou simplesmente SSH. Por outro lado, o método de autenticação utilizado para o Windows Server foi por usuário, senha e domínio ao qual pertence o servidor.

Como a ferramenta utilizada foi o Nessus, houve a necessidade da adoção de um nome para identificar a checagem, assim foi definido o padrão Scan_sistemaoperacional_versão Após a realização das atividades anteriores, foi possível dar início ao processo de execução das checagens nos sistemas operacionais, com o objetivo de coletar as informações relacionadas às configurações dos sistemas.

5.5 Análise e apresentação dos resultados

Ao executar a checagem de configurações nos sistemas operacionais, foram levantados dados relevantes para a avaliação de segurança. Esses dados foram extraídos do software de varredura de vulnerabilidades no formato csv e tratados com o uso da biblioteca *dplyr*, que permite a manipulação de dados com funções matemáticas e estatísticas na linguagem R (WICKHAM; FRANçOIS; HENRY, 2021).

5.6 Ambiente Debian 8

Após a checagem foram identificados 415 itens de configuração que a ferramenta foi capaz de checar e que fazem parte das 6 categorias do sistema operacional Debian 8. Essas informações estão explicitadas na Tabela 2 que contém uma descrição resumida da categoria, como é fornecida pela CIS *benchmarks* (SECURITY, 2020a), bem como a quantidade de itens presentes por cada uma dessas categorias.

Tabela 2 – Categorias do Debian 8.

Numeração	Descrição	Itens
1	Configuração Inicial	70
2	Serviços	36
3	Configuração de Rede	89
4	Registro e Auditoria	126
5	Acesso, Autenticação e Autorização	60
6	Manutenção do Sistema	34

Do total de itens verificados, 263 retornaram o status de falho e 152 itens foram aceitos. O resultado pode ser observado na Fig. 4, que apresenta a quantidade de itens por categorias.

Analisando as categorias de Configuração Inicial, Configuração de Rede, Registro e Auditoria, e Acesso, Autenticação e Autorização, pode-se notar o expressivo

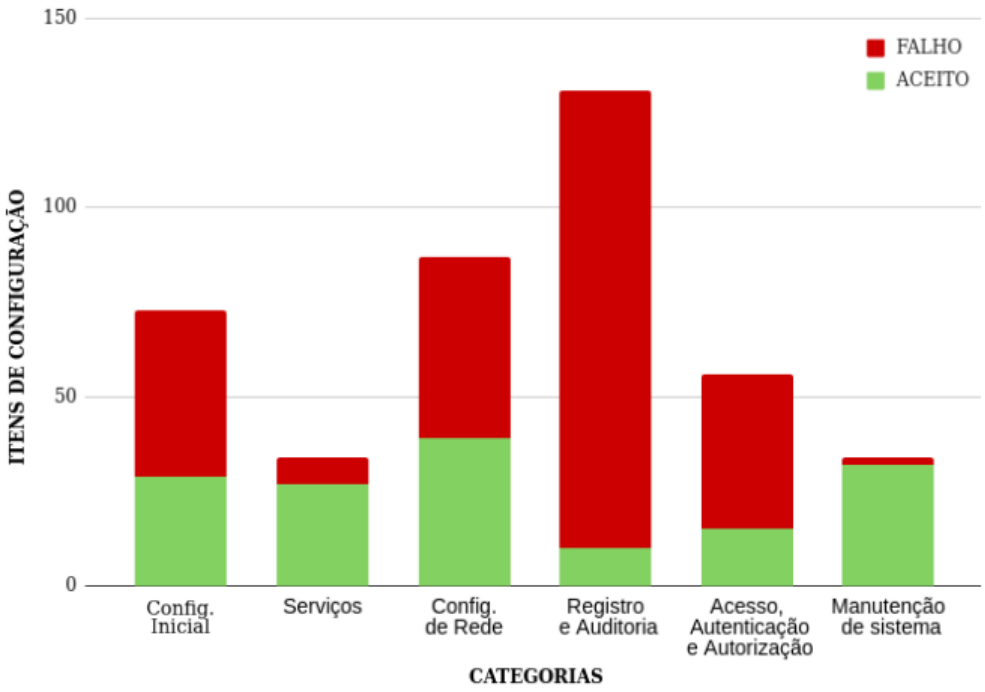

Figura 4 – Conformidade dos itens de configuração no Debian 8.

número de itens falhos que foram identificados nestas categorias. Para a categoria de Configuração Inicial, 44 itens retornaram o status de falho. Esses itens, de maneira geral, correspondem a configurações de partições separadas, permissionamento de usuários a arquivos e gerenciamento de atualização de software. Já a categoria de Configuração de Rede apresentou 48 itens não conformes que são relacionados às recomendações de configurações de rede, como protocolos e regras de firewall.

Por fim, se avalia os itens que demonstraram mais falhas de configuração. Para a categoria de Registro e Auditoria, 121 não conformidades foram detectadas e na categoria de Acesso, Autenticação e Autorização, 41 itens falharam. Esses números podem representar ameaças aos sistemas de registro e auditoria, já que os arquivos pertencentes a essa categoria são responsáveis pelo monitoramento de comportamentos suspeitos no sistema. Nesse sentido, a categoria de Acesso, Autenticação e Autorização configura-se no geral por itens que tratam do gerenciamento de senhas dos usuários, identificação dos usuários e grupos, além dos privilégios de acesso aos recursos do sistema especificados para cada usuário ou grupo.

Apesar das categorias descritas por Serviços e Manutenção do Sistema retornarem 7 e 2 itens falhos, respectivamente, nota-se que o impacto delas foi menor quando relacionadas às quantidades de falhas das outras categorias.

5.7 Ambiente Windows Server 2012 R2

O procedimento realizado para análise dos resultados no Debian 8 foi repetido para o sistema operacional Windows Server 2012 R2. Os resultados alcançados com a ferramenta de varredura foram estruturados dentro das 19 categorias do Windows que estão evidenciadas na Tabela 3.

Tabela 3 – Categorias do Windows Server 2012 R2.

Numeração	Descrição
1	Políticas de Conta
2	Políticas Locais
3	Log de Eventos
4	Grupos Restritos
5	Serviços do Sistema
6	Registro
7	Sistema de Arquivos
8	Políticas de Rede com Fio (IEEE 802.3)
9	Firewall do Windows com Segurança Avançada
10	Políticas do Gerenciador de Lista des Redes
11	Políticas de Rede sem Fio (IEEE 802.11)
12	Políticas de Chave Pública
13	Políticas de Restrição de Software
14	Configuração do *Client* NAP para Proteção de de Acesso à Rede
15	Políticas de Controle de Aplicativos
16	Políticas de Segurança IP
17	Configuração Avançada de Política de Auditoria
18	Modelos Administrativos (computador)
19	Modelos Administrativos (usuário)

Contudo, o objetivo da avaliação, como definido previamente, facilitou a sistematização das informações obtidas, uma vez que as categorias totalmente compostas por itens customizáveis não foram consideradas já que o objetivo são os itens que retornaram o resultado de aceito ou falho. Desta maneira, os itens de configuração das categorias não customizáveis estão dispostas na Tabela 4.

Tabela 4 – Categorias do Windows Server 2012 R2 não customizáveis.

Numeração	Descrição	Itens
1	Políticas de Conta	9
2	Políticas Locais	102
9	Firewall do Windows com Segurança Avançada	26
17	Configuração Avançada de Política de Auditoria	32
18	Modelos Administrativos (computador)	194
19	Modelos Administrativos (usuário)	11

O gráfico exibido pela Fig. 5 aponta o resultado obtido nos itens de configuração do sistema operacional. Em resumo, dos 374 itens de configuração, 284 não estavam de acordo com as recomendações de segurança, e apenas 90 itens estão com configurações conforme as políticas de segurança do Windows Server 2012 R2.

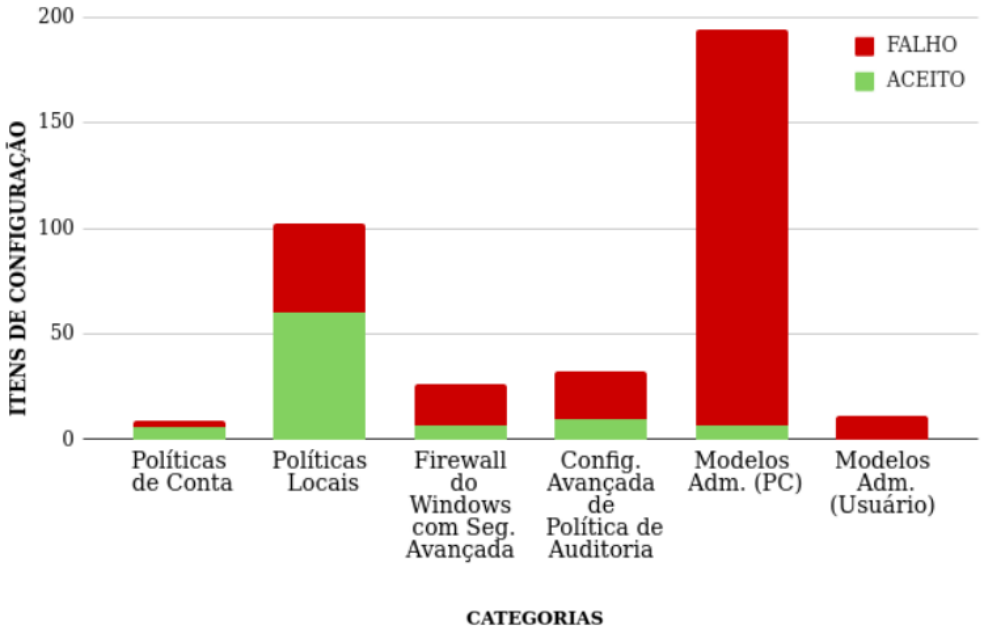

Figura 5 – Itens de configuração do Windows Server 2012 R2.

Ao se avaliar as categorias Firewall do Windows com Segurança Avançada, Configuração Avançada de Política de Auditoria, Modelos Administrativos (computador) e Modelos Administrativos (usuário), pode-se notar o expressivo número de itens falhos que foram identificados nestas categorias. Essas categorias retornaram mais de 60% de falhas no total dos seus itens de configuração. As categorias que descrevem os modelos administrativos retornaram os níveis de falhas acima de 95%, representando um número preocupante diante das ameaças que possam explorar essas aberturas nos sistemas. Os itens destas categorias definem as especificações de usuários e sistemas, como as instalações de softwares, por exemplo, que os ativos de uma organização devem seguir. Além disso, estes modelos administrativos, quando aplicados, tornam o ambiente corporativo menos suscetível a vulnerabilidades.

A categoria de Firewall do Windows com Segurança Avançada apresentou 22 itens com o status de falho. Essa categoria tem um papel importante, pois suas configurações controlam ou bloqueiam o tráfego de rede não autorizado que chega aos computadores e dispositivos de uma empresa, por meio de configurações de segurança apropriadas aos tipos de redes às quais estão conectados.

Outra análise relevante consiste em observar que 19 itens não conformes foram obtidos a partir da análise na categoria de Configuração Avançada de Política de Auditoria. Essa categoria tem como função principal o monitoramento das ações dos

usuários, como o acesso em determinados diretórios, ou as configurações aplicadas pelo mesmo. As seções Políticas de Conta e Políticas Locais apresentaram menos de 50% de itens falhos como resultado. Essas categorias administram configurações relacionadas, por exemplo, a políticas de senhas, bloqueios de telas e permissões dos usuários na rede.

5.8 Avaliação Comparativa

Analisando as avaliações dos sistemas operacionais de maneira cruzada, como exibido na Fig. 6, é perceptível que, apesar dos sistemas serem categorizados de maneira distinta, eles apresentaram números próximos de não conformidades. A diferença é representada por 21 não conformidades identificadas a mais no Windows Server 2012 R2. Este resultado demonstra a importância da avaliação de segurança, independente do sistema operacional adotado na empresa.

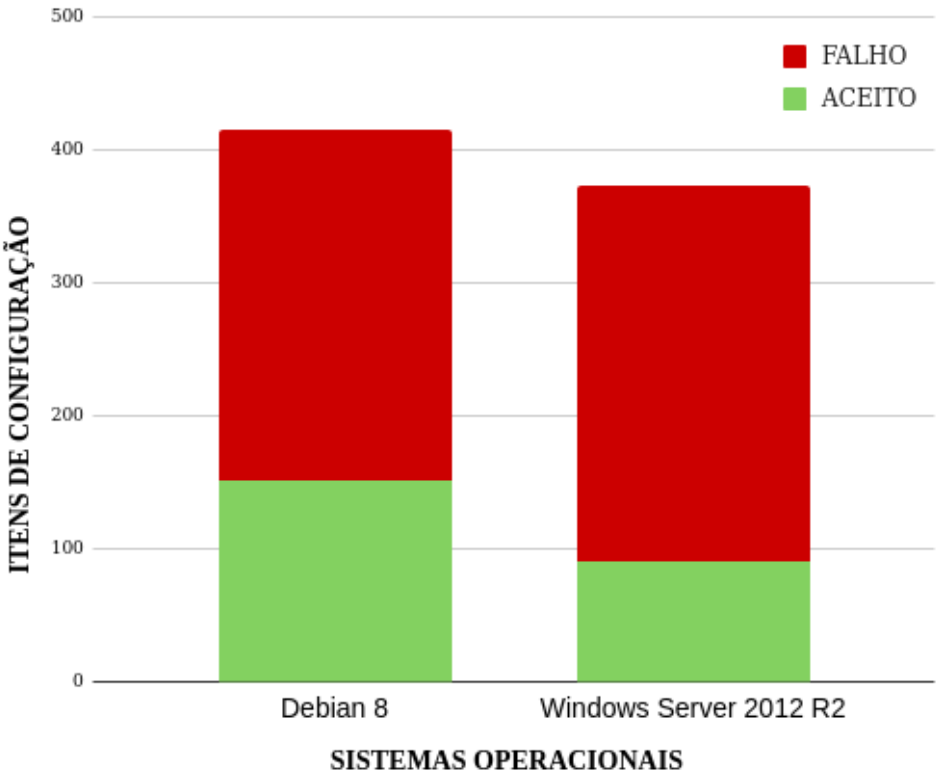

Figura 6 – Comparação dos sistemas operacionais.

Os números extraídos através da avaliação de segurança dos sistemas operacionais possibilitaram a classificação das informações por meio das categorias dos sistemas que obtiveram mais configurações falhas. Essa classificação pode servir como diretriz na organização da aplicação das boas práticas de segurança aos itens que serão priorizados, sendo ela composta por:

- **Políticas relacionadas às senhas dos sistemas.** Apresentam critérios que devem ser seguidos por todos os usuários, assegurando que a segurança durante o acesso aos sistemas corporativos sejam seguidos.
- **Políticas de acesso, autenticação e autorização.** Essas configurações deveriam ser aplicadas a fim de evitar que usuários mal intencionados acessem a rede interna de uma empresa e tenham permissão para acessar dados importantes de uma organização.
- **Políticas de monitoramento das configurações aplicadas por usuários.** As políticas de conformidade relacionadas a essa classificação tratam, basicamente, os acessos e instalações de software realizadas pelos usuários. Esse gerenciamento auxilia na identificação de acessos desconhecidos.
- **Políticas de configurações de rede.** Por meio destas políticas, são feitos os controles de acesso na rede.

6 Conclusões e Trabalhos Futuros

Dentro do contexto atual de Segurança da Informação, a gestão de vulnerabilidades vem tendo um papel de destaque. Neste contexto, este trabalho apresentou uma metodologia voltada especificamente para a avaliação de segurança de sistemas operacionais observando políticas de conformidade, e os resultados obtidos através da execução da metodologia mostraram ser possível tanto a identificação de vulnerabilidades como também a sua mitigação. A descrição desta metodologia, voltada especificamente para sistemas operacionais, e que provê apoio para a realização da gestão de conformidades, se caracteriza como um avanço interessante dentro do estado da arte da área.

Mesmo considerando que as configurações de segurança de sistemas operacionais tenham um caráter subjetivo, é possível que, por meio de métricas, seja definido como essas configurações serão avaliadas. Através da análise dos resultados deste artigo, ficou também evidente que as vulnerabilidades estão presentes mesmo em um sistema com configurações “de fábrica”, e é importante que vulnerabilidades sejam buscadas e corrigidas também neste contexto.

Como trabalhos futuros, se destacam: 1) utilização da metodologia descrita neste trabalho aplicada a sistemas operacionais convencionais e 2) desenvolvimento de um framework voltado para correção das falhas de configurações de sistemas operacionais como meio de automatizar a aplicação das políticas de conformidade.

Referências

Alhazmi, O. H.; Malaiya, Y. K. Quantitative vulnerability assessment of systems software. In: *Annual Reliability and Maintainability Symposium, 2005. Proceedings.* [S.l.: s.n.], 2005. p. 615–620. Citado 2 vezes nas páginas 12 e 13.

ANGRAINI; ALIAS, R. A.; OKFALISA. Information security policy compliance: Systematic literature review. *Procedia Computer Science*, v. 161, p. 1216 – 1224, 2019. ISSN 1877-0509. The Fifth Information Systems International Conference, 23-24 July 2019, Surabaya, Indonesia. Citado 3 vezes nas páginas 11, 12 e 13.

CAMPOS, A. *Modelagem de Processos com BPMN 2ª edição*. [S.l.]: Brasport, 2014. ISBN 9788574526638. Citado na página 14.

CAVEZA, S. N. S.; QUINLAN, R. *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 2018. Disponível em: <https://www.iso.org/standard/73906.html>. Citado na página 10.

CAVEZA, S. N. S.; QUINLAN, R. *TENABLE'S 2020 THREAT LANDSCAPE RETROSPECTIVE*. 2021. Disponível em: <https://pt-br.tenable.com/cyber-exposure/2020-threat-landscape-retrospective>. Citado na página 8.

Chalvatzis, I.; Karras, D. A.; Papademetriou, R. C. Evaluation of security vulnerability scanners for small and medium enterprises business networks resilience towards risk assessment. In: *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*. [S.l.: s.n.], 2019. p. 52–58. Citado na página 19.

FOUNDATION, O. *OWASP Benchmarks Project*. 2020. Acessado em: 2021-02-02. Disponível em: <https://owasp.org/www-project-benchmark/>. Citado na página 12.

Gorbenko, A. et al. Experience report: Study of vulnerabilities of enterprise operating systems. In: *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)*. [S.l.: s.n.], 2017. p. 205–215. ISSN 2332-6549. Citado 2 vezes nas páginas 12 e 13.

MESQUIDA, A. L.; MAS, A. Implementing information security best practices on software lifecycle processes: The iso/iec 15504 security extension. *Computers and Security*, v. 48, p. 19 – 34, 2015. ISSN 0167-4048. Citado 2 vezes nas páginas 12 e 13.

MOSKOWITZ, J. *Group Policy: Fundamentals, Security, and the Managed Desktop*. Wiley, 2015. (Online access with DDA: Askews). ISBN 9781119035589. Disponível em: <https://books.google.com.br/books?id=-6KLBgAAQBAJ>. Citado na página 19.

Mounji, A.; Le Charlier, B. Continuous assessment of a unix configuration: integrating intrusion detection and configuration analysis. In: *Proceedings of SNDSS '97: Internet Society 1997 Symposium on Network and Distributed System Security*. [S.l.: s.n.], 1997. p. 27–35. Citado 2 vezes nas páginas 12 e 13.

SECURITY, C. of I. *CIS Benchmarks*. 2020. Acessado em: 2020-10-24. Disponível em: <https://www.cisecurity.org/cis-benchmarks/>. Citado 6 vezes nas páginas 11, 12, 16, 18, 19 e 20.

SECURITY, C. of I. *CVE Details*. 2020. Acessado em: 2020-12-19. Disponível em: <https://www.cvedetails.com/top-50-versions.php>. Citado na página 18.

TENABLE. *THE NESSUS FAMILY*. 2021. Acessado em: 2020-12-18. Disponível em: <https://www.tenable.com/products/nessus>. Citado 2 vezes nas páginas 17 e 19.

The MITRE Corporation. *CVE-2020-1472*. 2020. Disponível em: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472>. Citado 2 vezes nas páginas 9 e 18.

The MITRE Corporation. *Common Vulnerabilities and Exposures-Terminology*. 2021. Disponível em: <https://cve.mitre.org/about/terminology.html>. Citado na página 10.

Veerasamy, N. High-level methodology for carrying out combined red and blue teams. In: *2009 Second International Conference on Computer and Electrical Engineering*. [S.l.: s.n.], 2009. v. 1, p. 416–420. Citado na página 8.

WICKHAM, H.; FRANçOIS, R.; HENRY, L. *Dplyr - a grammar of data manipulation*. 2021. Acessado em: 2021-01-16. Disponível em: <https://dplyr.tidyverse.org/>. Citado na página 20.