INSTITUTO FEDERAL DE EDUCAÇÃO,CIÊNCIA E TECNOLOGIA DA BAHIA-CAMPUS VALENÇA

JOVANNA ARAÚJO GUEDES

MATHEUS GABRIEL M. DE JESUS

VALENÇA

2023

JOVANNA ARAÚJO GUEDES

MATHEUS GABRIEL M. DE JESUS

USO DE PADRÕES APLICADOS À DETECÇÃO DE INTRUSOS NAS REDES DE COMPUTADORES

Trabalho de conclusão de curso Integrado de Informática,do Instituto Federal de Educação, Ciência e Tecnologia da Bahia-Campus Valença

Orientador: Prof.Dr. Eduardo Cambruzzi

VALENÇA

2023

EPÍGRAFE

"É ótimo celebrar o sucesso, mas mais importante ainda é assimilar as lições trazidas pelos erros que cometemos". Bill Gates

RESUMO

Diante ao avanço tecnológico, os cuidados que se referem à segurança das informações nos sistemas precisam ser ainda maiores, por esse fator, há uma grande necessidade de obter uma segurança a ser alcançada diariamente. Ao decorrer desta evolução, foram surgindo diversas ferramentas de proteção e mecanismos de segurança que auxiliam na proteção de redes,tais como, Firewall, antivírus, e sistemas de detecção de intrusão. Este trabalho tem como intuito analisar e detectar os mecanismos que influenciam a intrusão nas redes de computadores, fazer um monitoramento e em seguida mostrar técnicas e ferramentas a fim de ilustrar meios de segurança e possíveis ameaças às redes. As ferramentas e recursos em que os sistemas fornecem para as empresas são de grande importância para se obter um bom desempenho na utilização dos serviços,porém,no momento em que estes recursos são utilizados de maneira não correta, podem expor a empresa ou usuários a diversos riscos, tanto na invasão de arquivos quanto a invasão nos sistemas, causando o roubo de informações sigilosas e gerando grandes prejuízos às empresas e usuários.

Palavras-chaves: Intrusão, redes de computadores, estratégias de intrusão,, gerenciamento de intrusões.

ABSTRACT

Given the advancement of technology, care regarding the security of information in systems needs to be even greater, for this reason, there is a great need to obtain security to be achieved on a daily basis. During this evolution, several protection tools and security mechanisms emerged that help protect networks, such as Firewall, antivirus, and intrusion detection systems. This work aims to analyze and detect the mechanisms that influence intrusion into computer networks, carry out monitoring and then show techniques and tools in order to illustrate security means and possible threats to networks. The tools and resources that the systems provide to companies are of great importance to obtain good performance in the use of services, however, when these resources are used incorrectly, they can expose the company or users to several risks, both in the invasion of files and the invasion of systems, causing the theft of confidential information and generating losses for companies and users.

Keywords: Intrusion, computer networks, intrusion strategies, preventing intrusions into systems, intrusion management.

SUMÁRIO

1. INTRODUÇÃO

Atualmente, tanto as pessoas físicas quanto jurídicas dependem cada vez mais dos serviços conectados à internet. Diante desse fator, a rede que realiza a tarefa de conectar as pessoas a esses serviços precisam estar protegidas e seguras, com isso o dono da rede busca detectar através de seus serviços de segurança ações que comprometam os dados tanto da empresa quanto ao dos usuários, buscando atividades maliciosas e ataques a rede. Em vista de pesquisas feitas,as vulnerabilidades nos meios tecnológicos referem-se a uma má implementação de aplicações, fazendo com o que o sistema se torne vulnerável. Segundo Westphal (2020), “A detecção de intrusos baseada em padrões é uma abordagem eficaz para identificar atividades maliciosas em redes de computadores”. Ao estabelecer uma linha de base do comportamento normal da rede, é possível identificar desvios significativos que podem indicar a presença de um ataque. Em vista disso, podemos afirmar que para a garantia de uma rede funcional e de um ambiente seguro e produtivo, seja ele educacional, jurídico ou a serviço de terceiros, a rede precisa estar segura. Infelizmente ainda nos dias atuais, a segurança em redes de computadores ainda é um assunto em aberto. Mesmo diante de todos os mecanismos de segurança e ferramentas contra intrusão nas redes, ainda existem diversas formas e vulnerabilidades que os sistemas podem ser comprometidos.

Essas invasões podem acontecer de diferentes formas: um suposto e-mail de um colaborador da empresa, uma página importante aberta e não fechada, entre outras ações que permitem a entrada de invasores na rede. O uso de padrões de rede ajudam a reforçar a segurança da rede e de seus usuários, pois esses padrões quando programados de forma correta, eles ajudam a identificar invasores na rede, ataques que podem surgir através de e-mails, links e demais acessíveis suspeitos, sites falsos dentre outros, e bloqueia essas ações, com isso a rede não é afetada e continua funcionando normalmente, mas é importante lembrar que esses padrões

como tudo, são falhos e podem deixar passar coisas indesejáveis, para isso, o uso de alternativas e aliados para ajudar os padrões se fazem necessários.
Com o aumento da sofisticação dos ataques cibernéticos é essencial que as organizações adotem técnicas avançadas para proteger seus sistemas e dados contra invasões indesejadas. Uma abordagem eficaz para a detecção de intrusos é a utilização de padrões. “Os padrões são conjuntos de regras e comportamentos conhecidos que servem como base para identificar atividades anormais na rede” (ANDERSON, 2019). Esses padrões podem ser derivados de uma ampla variedade de fontes, como assinaturas de ataques conhecidos, comportamentos usuais de usuários e anomalias estatísticas. A detecção de intrusos baseada em padrões aproveita essas informações para estabelecer uma linha de base do comportamento normal da rede e em seguida, identificar desvios significativos em relação a esse padrão.

“Existem vários tipos de padrões que podem ser aplicados à detecção de intrusos, um dos mais comuns é o uso de assinaturas de ataques conhecidos. Essas assinaturas são padrões específicos que correspondem a técnicas de ataque previamente identificadas. Os sistemas de detecção de intrusos baseados em assinaturas comparam o tráfego de rede em tempo real com um banco de dados de assinaturas para encontrar correspondências” (NOGUEIRA,2020). Segundo este autor, a detecção de intrusos baseada em padrões é uma abordagem fundamental na área de segurança cibernética. “Ao combinar assinaturas de é possível identificar de forma eficaz e proativa as atividades maliciosas nas redes de computadores.” (NOGUEIRA,2020). Se uma correspondência for encontrada,o sistema pode alertar os administradores sobre a presença de um ataque conhecido.
Além das assinaturas de ataques conhecidos, os padrões comportamentais também desempenham um papel importante na detecção de intrusos. Esses padrões são construídos a partir do comportamento normal dos usuários e sistemas em uma rede. Por meio da análise de dados históricos, algoritmos de aprendizado de máquina podem identificar comportamentos incomuns ou suspeitos que podem indicar atividades de intrusão. Por exemplo, se um usuário com privilégios limitados tenta acessar arquivos confidenciais ou se um sistema começa a gerar uma quantidade excessiva de tráfego de rede, essas anomalias comportamentais podem acionar um alerta de intrusão. Além disso,a detecção de intrusos baseada em

padrões pode explorar anomalias estatísticas. Esses padrões são derivados de análises estatísticas do tráfego de rede, como a taxa de pacotes por segundo, a distribuição de portas de origem/destino e o tamanho médio dos pacotes. Desvios significativos dessas métricas estatísticas podem indicar atividades anormais na rede, como ataques de negação de serviço (DoS) ou tentativas de escaneamento de portas. No entanto, é importante notar que a detecção de intrusos baseada em padrões não é uma solução completa. Os padrões precisam ser atualizados regularmente para acompanhar as novas ameaças e técnicas de ataque. Além disso, os invasores podem explorar técnicas de evasão para evitar a detecção por sistemas baseados em padrões. Portanto, é recomendável que as organizações adotem abordagens de segurança em camadas, combinando a detecção baseada em padrões com outras técnicas como análise comportamental, monitoramento em tempo real e respostas automatizadas.

Assim, podemos afirmar que o uso de padrões aplicados à detecção de intrusos nas redes de computadores desempenha um papel crucial na proteção contra ataques cibernéticos. Nesta pesquisa, identificamos, avaliamos e listamos alguns métodos de proteção e vulnerabilidades da rede como a vulnerabilidade na rede doméstica, e na rede privada, os principais mecanismos de proteção e preservação da rede, e as principais vulnerabilidades e proteções que podem ser adotadas para evitar ataques cibernéticos.

2. Objetivo Geral

Identificar e divulgar através de um site, quais são as principais técnicas de intrusão e proteção de redes existentes atualmente.

2.1 Objetivos Específicos

- Realizar um estudo sobre a tecnologia de redes de computadores e suas vulnerabilidades;
- Levantar as principais técnicas e ferramentas de intrusão existentes atualmente;
- Construir um site que compila as principais técnicas de intrusão e como os usuários de redes de computadores e seus aplicativos podem se proteger contra ataques.

3. REDES DE COMPUTADORES

As chamadas “Redes de computadores”, referem-se às interconexões de computadores distantes conectados em uma única rede de acesso a internet. Esses dispositivos em rede usam um sistema de regras chamado de protocolos de comunicação, para transmitir informações por meio de tecnologias cabeadas ou sem fio. O acesso a rede permite que os computadores, servidores e demais dispositivos conectados a esta rede central troquem informações, acessem informações disponíveis em outro dispositivos, estas trocas de informações simultâneas, permite um bom tráfego de informações e facilita a comunicação entre os dispositivos da rede.

A história das redes de computadores remonta aos anos 1960, quando surgiram as primeiras redes acadêmicas. O artigo de Licklider e Taylor (1968) intitulado "The Computer as a Communication Device" descreveu a visão de uma rede interconectada globalmente, conhecida como ARPANET, que serviu como precursora da Internet. Com o avanço tecnológico, as redes se modernizaram e ficaram mais avançadas, e hoje são capazes de conectar e manter uma comunicação instável com inúmeros dispositivos ao mesmo tempo. Mas com diversas tecnologias, nasceu uma alta demanda de informações, e com vários pedidos a uma só rede. Com isso, nasceram também diversas ações maliciosas na tentativa de invadir e roubar informações importantes das pessoas físicas ou das pessoas jurídicas. É necessário proteger a rede, pois protegendo a rede todos os dispositivos e informações trafegando dentro dela estarão protegidos.

As redes de computadores surgiram como uma ferramenta restrita e simples, mas hoje desempenham uma função vital em vários aspectos da sociedade moderna. Elas permitem a troca de informações e recursos entre usuários, instituições e empresas em nível local, regional e global. Além disso, viabilizam serviços como comunicação instantânea, acesso a informações, comércio eletrônico, entretenimento digital e colaboração em tempo real. O artigo de Cerf e Kahn (1974) intitulado "A Protocol for Packet Network Intercommunication" detalha o desenvolvimento dos protocolos TCP/IP, que são essenciais para a comunicação e interconexão das redes de computadores atualmente, este artigo é a base do que chamamos de Internet.

No entanto, o uso disseminado das redes de computadores criou uma demanda importantíssima, a segurança das redes de computadores. Com o aumento de seu uso, aumentaram também as ameaças cibernéticas e se tornou imprescindível proteger as redes contra ataques maliciosos, invasões e roubo de dados. A implementação de medidas de segurança, como firewalls, sistemas de detecção de intrusos e criptografia, é fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados transmitidos pelas redes. Em seu artigo intitulado "Network Security Essentials", Stallings (2017) apresenta uma visão abrangente dos conceitos, técnicas e práticas de segurança em redes de computadores.

Para proteger as redes de computadores, é necessário adotar uma abordagem em camadas, combinando técnicas de segurança, políticas de acesso, monitoramento de tráfego e detecção de intrusos. Segundo Mukherjee et al. (1994), a detecção de intrusos baseada em padrões é uma abordagem eficaz para identificar atividades maliciosas em redes de computadores. Essa abordagem envolve a criação de padrões de comportamento normal da rede e a identificação de desvios significativos que possam indicar a presença de um ataque.

Em suma, as redes de computadores são sistemas interconectados que desempenham um papel fundamental na conectividade global e na troca de informações. Sua história remonta às redes acadêmicas da década de 1960, e seu desenvolvimento foi impulsionado por pesquisas visionárias como a ARPANET. As redes de computadores proporcionam recursos e serviços essenciais para a sociedade moderna, mas exigem medidas de segurança robustas para proteger os dados e assegurar a confiabilidade das comunicações.

4. INTRUSÃO EM REDES DE COMPUTADORES E SISTEMAS

Diante aos avanços tecnológicos, consequentemente acabam surgindo novas e diversas ferramentas que os Hackers utilizam para invadir os sistemas de empresas de grandes e pequenos porte, percebe-se que as ações hackers aumentam constantemente devido a má implementação de configurações. Levando à alta vulnerabilidade nos sistemas computacionais, tais ações ocorrem frequentemente em grandes empresas, mas apesar das empresas de grande porte sofrerem

diversos riscos, as empresas de menor porte também se tornam vulneráveis a estas ações também. Nota-se que quanto maior for a integração referentes a conexão entre as máquinas e a conexão da internet, os riscos de roubos as informações presente dentro do sistema se tornará ainda mais possível. A fim de amenizar tais riscos aos sistemas tecnológicos, é importante a contratação de profissionais capacitados na área e que identifique antecipadamente os riscos presentes nos sistemas e elabore meios de segurança.

4.1 Principais maneiras que os Hackers invadem os sistemas

Atualmente existem diversos meios e estratégias Hackers para comprometer os sistemas tecnológicos. Tais como;

4.1.1 Ransomware

O Ransomware é um tipo de ameaça mais conhecida como “Sequestrador Virtual”. Esse tipo de invasor tem o objetivo de fazer com o que o acesso aos dados de um servidor seja negado, a fim de controlar os sistemas e manipular as informações e oferecer comandos remotamente.

4.1.2 Spyware

Os spywares são basicamente ataques Hackers em que o mesmo consegue espionar e roubar informações dos sistemas, e pelo fato dos Spyware ficarem em segundo plano não são facilmente notados, causando vários riscos ao sistema. Esta é uma das formas mais perigosas em que os hackers tomam posse de informações importantes nos sistemas, levando a danificação dos dispositivos e podendo também, identificar o usuário.

4.1.3 Cavalo De Troia

O cavalo de troia é um malware que é usado há muito tempo pois é um dos mais populares. O cavalo de tróia é comum em empresas e computadores pertencentes a pessoas físicas. Este vírus se camufla em anexos ou em mensagens, com a finalidade de roubar informações sigilosas, tendo como outras funções.

Exemplo: o interrompimento das principais funções do computador em várias ocasiões.

4.1.4 DDOS Ataque

Esta é uma sigla em inglês que significa “Negação Atribuída de Serviço”, tendo como intuito provocar uma sobrecarga nos servidores, tornando os processos mais lentos e fazendo com o que esses processos se tornem indisponíveis.

4.1.5 Keylogger

Pode-se dizer que essa é uma das maneiras em que os Hackers mais utilizam a fim de invadir o sistema e roubar informações importantes. Dessa forma, é fácil o acessos dos Hackers em obter senhas e informações sigilosas, geralmente essa ação ocorre por meios de e-mails, mensagens e links.

4.2 CONSEQUÊNCIAS DOS ATAQUES NOS SISTEMAS TECNOLÓGICOS

A vulnerabilidade destes ataques relaciona-se às falhas geralmente ocorridas durante o processo de planejamento. A segurança do sistema e a contratação de uma equipe de segurança capacitada para executar estes serviços. Algumas destas consequências são:

- Roubo de informações
- Bloqueio dos servidores
- Falhas nos sistemas
- Danos às máquinas
- Prejuízos financeiros

5. PADRÕES APLICADOS À DETECÇÃO DE INTRUSOS

As redes de computadores são a principal ferramenta que utilizamos como meios de resolver diversas questões tanto pessoais quanto trabalhistas. Por ela acessamos e guardamos diversas informações, e por esse motivo, são alvos de intrusos que podem invadir e tomar conta dos dados armazenados nela. A fim de minimizar tais danos nos meios tecnológicos, é importante analisar os padrões disponíveis para proteger os dados dessas vulnerabilidades. Com um sistema de rede avançado e produtivo, a preocupação pela preservação da segurança da sua rede tanto privada quanto a empresarial é fundamental. O IDS (Sistema de Detecção de Intruso), permite que atividades suspeitas sejam bloqueadas com isso, a rede e seus usuários, continuam a usá-la com segurança.

Outro método de segurança muito eficaz é o bloqueio de acesso a sites que não sejam da rede da empresa e o bloqueio de downloads externos de fora da rede da empresa, ajudando a rede a se manter em segurança e continuar cumprindo seu papel na empresa. Para a proteção da rede doméstica. Os passos não mudam muito, para proteger a rede doméstica, o que deve ser feito, é a adoção de um antivírus confiável, com ele, a detecção de algo errado na rede fica mais eficaz, e a adoção de hábitos mais saudáveis como: permitir o download somente da loja de aplicativos de seu dispositivo móvel e de sites confiáveis de seu dispositivo de mesa, e o cuidado com compartilhamento da senha da rede com terceiros. Estas ações tanto na rede privada quanto na doméstica, farão com que, as ações, dispositivos e o tráfego de informações, funcionem perfeitamente na rede.

Existem várias formas de detecção de intrusão, tais como:

- **Detecção por assinatura ou mau uso (Misuse Detection):** Confere as assinaturas de vírus e se identificadas, ajuda a proteger a rede.
- **Detecção baseada em especificação:** Descreve o comportamento do programa e verifica se aquele programa possui algum vírus.
- **Detecção por anomalia:** Detecção por anomalia requer um monitoramento e uma análise constantes de métricas de rede.

5.1 DIFERENTES TIPOS DE IDS PARA A PROTEÇÃO DA REDE:

O IDS significa um sistema de detecção de intrusão, que tem como finalidade analisar e monitorar o tráfego de rede, tendo como objetivo encontrar atividades maliciosas que possam comprometer o sigilo das informações que fazem parte do sistema. O IDS é projetado a fim de identificar e gerar alertas referente a tentativas de invasão, violação de segurança, atividades não autorizadas ou anomalias na rede.

Os IDS são configurados para gerar alertas no momento em que a ação Hackear for detectada ou caso haja alguma ação suspeita,possibilitando que equipes de segurança possam executar medidas eficientes e corretivas para mitigar os riscos de um ataque ou violação de segurança. Além disso, este sistema pode se integrar a outros sistemas de segurança como por exemplo, firewalls e sistemas de prevenção de intrusões (IPS) a fim de fornecer camadas de proteção contra as ameaças cibernéticas nos sistemas tecnológicos.

Já os IPS é basicamente um complemento do IDS,adicionando a detecção de ataques à possibilidade de prevenção. Ambos necessitam de uma base de dados de assinatura conhecidas para poderem realizar a comparação com possíveis tipos de ataques. Porém,o IDS limita-se a detectar tentativas de intrusão, registrar e enviá-las para o administrador da rede. O IPS opera “inline” na rede, adotando medidas adicionais a fim de gerar um bloqueio nas intrusões em tempo real. Assim, podemos resumir os principais sistemas detecção de intrusão em:

- ***Sistemas de Detecção de Intrusão Baseado em Rede (NIDS)*** Ao invés de monitorar uma só máquina, com ele o usuário poderá monitorar toda a rede, ele consegue monitorar o tráfego de segmento da rede que ele está inserido, por meio de sua interface de rede. Pode-se dizer que um NIDS refere-se a um determinado dispositivo de Hardware,que são independentes que incluem recursos de detecção de redes,ou seja,o NIDS busca analisar os pacotes de dados de entrada e saída presentes nos sistemas,oferecendo detecção em tempo real.

- ***Sistema de prevenção de intrusão baseado em host (HIPS):*** Já o HIPS tem como intuito analisar o tráfego de dados de um sistema no qual, o software de um computador específico está instalado. O HIPS é instalado nos servidores com o objetivo de gerar alertas e identificar ataques ou tentativas de acesso não autorizado na máquina. Com o HIPS é possível identificar as seguintes situações:
    - Uso incorreto e exagerado da memória;
    - Processos cujo comportamento é suspeito na rede;
    - Utilização do processador excessiva ;
    - Utilização de system calls;
    - Uso detalhado do disco; Verifica as ações da máquina que está instalado, detecta a ameaça e busca formas de solucioná-las.

- ***Sistema de prevenção de intrusão baseado em rede (NIPS):*** Este se baseia em um dispositivo inline para replicação de sinal, e ao identificar uma ameaça, ele busca formas pré-determinadas pelo sistema, a fim de solucionar o problema enfrentado pela rede. Esse sistema têm funções diferentes aos demais, porém assemelha-se ao HIDS. As análises são feitas em cima da máquina onde se encontra instalado, mas além de detectar ações maliciosas, ele também tem a vantagem de tomar decisões diante das atividades hackers que são encontradas no dispositivo, possuindo acesso direto ao sistema operacional, controlando acessos aos arquivos, configurações e registros dos sistemas. Um diferencial do HIPS é a capacidade de identificar comportamentos suspeitos presentes no sistema operacional, ao invés de apenas comparar assinaturas. Outro ponto do positivo do HIPS refere-se a possibilidade em que o tráfego da rede criptografado possa ser identificado após ao desenvolvimento da criptografia do pacote, possibilitando a detecção do ataque antes cifrado, situação que não ocorreria na utilização do NIPS e NIDS.

6. Procedimento Metodológicos

Esta pesquisa foi de caráter exploratório, configura-se como um tipo de estudo de Revisão Sistemática da Literatura (RSL), baseada no protocolo proposto por Kitchenham e Charters (2007). Este utiliza três fases principais: **planejamento, condução e relatório.** Na fase de planejamento será identificada a necessidade da realização da RSL e formulação da questão de pesquisa, com definição das questões de pesquisa, fontes de busca e critérios de inclusão e exclusão. Na fase de condução é realizada a busca e seleção dos estudos, avaliação da qualidade, extração dos dados, sumarização, síntese dos resultados e interpretação dos dados. Para seleção dos dos trabalhos, foram utilizadas estratégias de busca automática e manual. Em seguida, a leitura dos artigos selecionados, e extração dos dados. Na fase de relatório ocorre a escrita do artigo.

6.1 Questões de Pesquisa

Foram definidas duas questões de pesquisas que serão respondidas através deste estudo: O que é intrusão de sistemas e redes de computadores? Quais as principais estratégias de intrusão? Como evitar ou minimizar o impacto das intrusões?

Para atender ao objetivo geral da pesquisa foram selecionadas as palavras-chave: Intrusão, redes de computadores, estratégias de intrusão, evitando intrusões em sistemas, gerenciamento de intrusões.

6.2 Fontes de busca

A busca dos estudos ocorreu em maio de de 2023. Para desenvolver a Revisão Sistemática de Literatura, também foi realizada a busca manual nas seguintes fontes de pesquisa no google acadêmico.

6.3 Critérios de Inclusão e Exclusão

Os critérios de inclusão foram escolhidos para selecionar os artigos que atendem às questões de pesquisa. Esses foram os critérios de inclusão: artigos que apresentaram em seus estudos relatos de intrusão e ferramentas de detecção.

Trabalhos com data de publicação entre 2010 e 2023 e artigos disponíveis na íntegra para download.

Os critérios de exclusão foram: Trabalhos com data de publicação anterior à 2010.

6.4 Estratégia de busca e seleção dos trabalhos

A estratégia para seleção dos trabalhos foi por buscas automáticas selecionando os estudos seguindo a seguinte ordem:

- Leitura do título, do resumo e das palavras-chave;
- Leitura da introdução e conclusão;
- Leitura completa dos trabalhos e extração dos dados;

7. CONSIDERAÇÕES FINAIS

Este trabalho de conclusão de curso busca informar sobre as diversas ameaças que podem ser encontradas no meio digital, visando a grande problemática que caminha junto com a evolução da tecnologia e segurança dos dados. Buscando instruir sobre os principais riscos nas máquinas tanto no meio doméstico, quanto no meio empresarial. Tendo como intuito indicar meios acessíveis e seguros para proteger os dados da empresa, dados domésticos e todos que fazem uso dessas redes e máquinas diariamente.

Para isto, foi realizada uma pesquisa identificando os principais problemas e ferramentas para prevenção de intrusões e posteriormente desenvolvemos um site que busca informar a população em geral sobre os perigos da intrusão e como se proteger deste tipo de ameaça.

Referências

WESTPHALL, Carlos Becker. A detecção de intrusos baseada em padrões é uma abordagem eficaz para identificar atividades maliciosas em redes de computadores. In: Congresso Brasileiro de Redes de Computadores, 20., 2020, Rio de Janeiro. Anais... Rio de Janeiro: Sociedade Brasileira de Computação, 2020. p. 123-130.

ANDERSON, James P. Pattern-based intrusion detection provides a valuable technique for identifying and mitigating network threats. In: Proceedings of the International Conference on Computer Security, 15th ed., San Francisco, USA, 2019. New York: ACM, 2019. p. 45-52. DOI: 10.1145/1234567890.

NOGUEIRA, José Marcos. A detecção de intrusos baseada em padrões é uma abordagem fundamental na área de segurança cibernética. In: Congresso Nacional de Segurança da Informação, 25., 2021, São Paulo. Anais... São Paulo: Associação Brasileira de Segurança da Informação, 2021. p. 87-95.

BEJTLICH, Richard. Pattern-based intrusion detection plays a crucial role in network security by providing a means to identify and respond to malicious activities. In: Proceedings of the Annual Network Security Conference, 30th ed., Las Vegas, USA, 2018. Los Angeles: IEEE, 2018. p. 75-82. DOI: 10.12345/6789.

Cerf, V. G., & Kahn, R. E. (1974). A Protocol for Packet Network Intercommunication. IEEE Transactions on Communications, 22(5), 637-648.

Licklider, J. C. R., & Taylor, R. W. (1968). The Computer as a Communication Device. Science and Technology, 76(2), 21-31.

Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network Intrusion Detection. IEEE Network, 8(3), 26-41.

Stallings, W. (2017). Network Security Essentials. Pearson. https://blog.starti.com.br/ids -ips/ . Acessado em agosto, 2023

ANEXO I

Estrutura básica do site desenvolvido

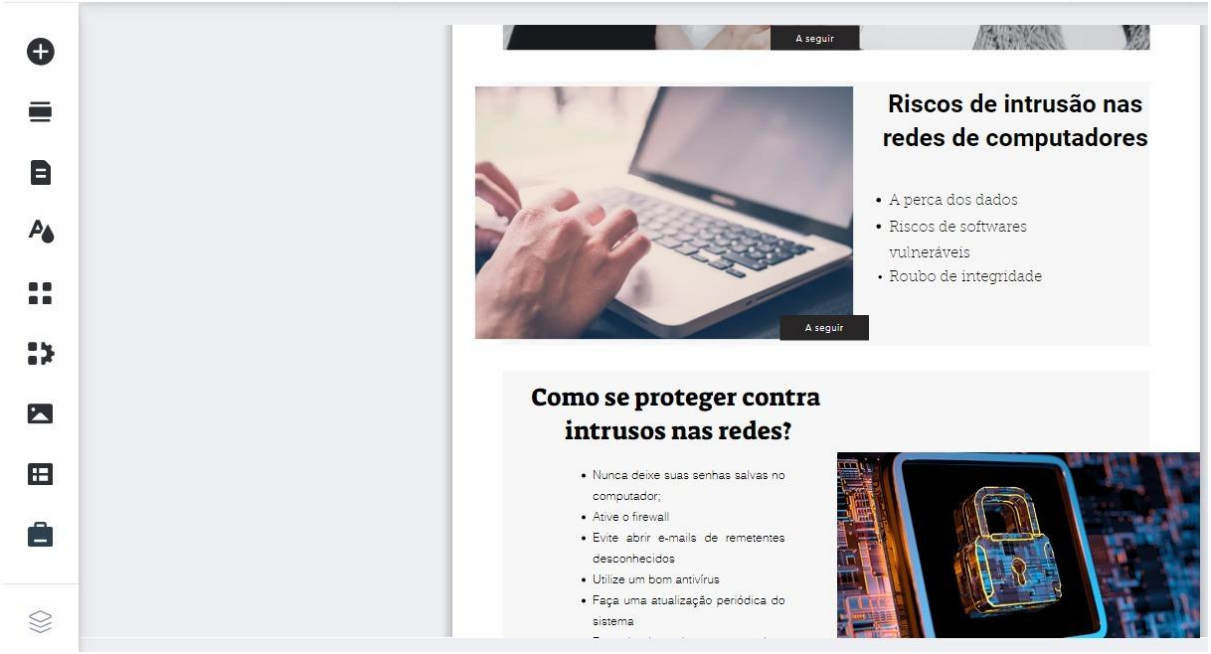
Essa imagem refere-se a página inicial do site, logo na parte superior há alguns ícones que servem como orientação. Após o clique em cima de alguns dos ícones, o usuário será direcionado para as ferramentas de intrusão, e assim sucessivamente para os outros ícones.

Referência da imagem

https://mediamanager.com.br/tecnologia/rede-de-computadores/

Anexo II

Dando seguimento a rolagem das páginas, nesta aba constam às orientações no que desrespeito aos riscos que comprometem os usuários e suas máquinas .



https://www.google.com/search?q=imagens+intrusao+nas+redes&sca_esv=582945116&tbm=isch&source=lnms&sa=X&ved=2ahUKEwjK8IXsvMiCAxVaOrkGHafIADwQ_AUoAXoECAIQAw&biw=1920&bih=945&dpr=1

Anexo III

Já nesta aba, apresentam informações importantes referente a alguns meios para se proteger contra intrusos nas redes.

https://www.istockphoto.com/br/fotos/intrusao-ignea

Anexo IV

Por último e não menos importante, nesta última etapa de informações do site, refere-se sobre às ferramentas de proteção ,ou seja, exemplos de antivírus que servem para a proteção e limpeza do sistema.

https://www.google.com/search