WRSeg 2024 - 8º Workshop Regional de Segurança da Informação e de Sistemas Computacionais (WRSeg). DOI: 10.5753/errc.2024.4685
2024 Creative Commons Attribution 4.0 International License (CC BY 4.0)

Artigo Completo/Full Paper

CyberWatch Guard: SOLUÇÃO INTEGRADA PARA ANÁLISE E MONITORAMENTO DE REDES EMPRESARIAIS

CyberWatch Guard: INTEGRATED SOLUTION FOR ANALYSIS AND MONITORING OF CORPORATE NETWORKS

Mateus Soares • mateus123soares@hotmail.com
Universidade Federal do Pampa (UNIPAMPA)
Marcelo Cordeiro • marcelo_1411@hotmail.com
Universidade Federal do Pampa (UNIPAMPA)
Érico Amaral • ericoamaral@unipampa.edu.br
Universidade Federal do Pampa (UNIPAMPA)
Thiago Leal • thfleal@gmail.com
Universidade Federal do Pampa (UNIPAMPA)
Guilherme Goulart • guilhermedomingues.aluno@unipampa.edu.br
Universidade Federal do Pampa (UNIPAMPA)

resumo. A segurança de redes de computadores consiste em um conjunto de estratégias adotadas pelos administradores para a proteção contra ameaças, por exemplo, tentativa de invasão, ataques de força bruta e escaneamento de portas, entre outros. Deste modo, observa-se, no âmbito empresarial, a imprescindibilidade do estabelecimento de padrões de segurança para prover a garantia da integridade dos seus. O presente trabalho objetiva na construção de um software integrado para o monitoramento de redes visando disponibilizar uma interface única para o controle desses ambientes. Além disso, vislumbra-se disponibilizar através desta ferramenta alertas de incidentes e uma forma pro ativa para a redução dos impactos causados por estes incidentes.

abstract. The security of computer networks consists of a set of strategies adopted by administrators to protect against threats, such as intrusion attempts, brute force attacks, and port scanning, among others. In the business context, the need to establish security standards to ensure the integrity of company resources is evident. This work aims to build an integrated software solution for network monitoring, providing a unified interface for managing these environments. Furthermore, the tool seeks to offer incident alerts and proactive measures to reduce the impact caused by these incidents.

palavras-chave: Análise de protocolos de segurança • Incidentes de segurança: prevenção • detecção e resposta • Segurança em redes
keywords: Security protocol analysis • Security incidents: prevention • Detection and response • Network security

1 Introdução

A segurança de redes de computadores tem se tornado cada vez mais relevante, especialmente com o aumento de ataques cibernéticos e a transformação digital. Pequenas e médias empresas, que frequentemente carecem de estruturas robustas de segurança, estão particularmente vulneráveis. Conforme [1] em números reais, o estudo da empresa Minsait aponta que o número de ataques virtuais cresceu 75% e, em contrapartida, 35% das organizações na América Latina e Europa reduziram seus orçamentos para a segurança digital no mesmo período.

A Figura 1 com base nos dados de [1] deixa claro este cenário, onde se observa o aumento das tentativas de ataques virtuais (75%), referenciadas pela linha azul escura. Os ataques efetivamente realizados estão representados pela linha azul clara com o aumento de 70% no período. Percebe-se a redução dos investimentos por meio da linha vermelha no gráfico, a qual apontou uma queda de 65%. Este trabalho propõe desenvolver uma solução integrada para monitoramento de redes, visando centralizar dados de segurança e oferecer respostas proativas a incidentes. A solução tem em vista simplificar o gerenciamento da infraestrutura de TI, consolidando informações de várias ferramentas em uma interface única e amigável para o usuário. Reconhecendo que as ameaças são considerados elementos que podem explicar vulnerabilidades nos sistemas e, desta forma, causar

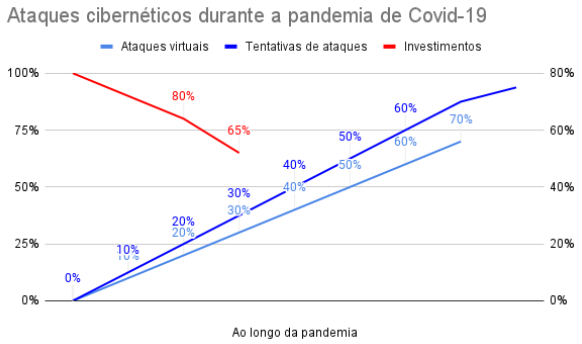


Figura 1. Fonte: Autor (2021). Baseado nos dados de Souza.

sérios impactos ao sistemas, é imprescindível para um nível adequado de segurança que essas ameaças sejam constantemente neutralizadas. Ainda mais, qualquer violação do sistema intencional ou acidental também poderá ser considerada, uma ameaça, conforme [2].

2 Metodologia

A metodologia aplicada é de natureza experimental, com uma abordagem quali-quantitativa. O desenvolvimento do software seguiu etapas definidas, desde a revisão bibliográfica, levantamento de requisitos até a implementação do protótipo e testes de validação. Foram utilizadas ferramentas de monitoramento open-source, como Zabbix[3] e Zeek[4], e a visualização de dados foi realizada com o Grafana [5]. A arquitetura do sistema foi projetada em três camadas: *frontend*, *backend* e módulos de segurança. O *backend* foi responsável pelo processamento dos dados e pela geração de alerta, enquanto o *frontend* proporcionou uma interface para o usuário configurar e visualizar as métricas da rede.

2.1 Referencial Teórico

A segurança de redes de computadores tornou-se uma preocupação central para organizações de todos os tamanhos, diante do aumento contínuo das ameaças cibernéticas, como ataques DDoS, *malwares* e tentativas de invasão. Pequenas e médias empresas, em particular, enfrentam desafios adicionais devido à limitada infraestrutura de segurança, o que as torna alvos mais vulneráveis. Nesse contexto, torna-se essencial adotar práticas de proteção e monitoramento que garantam a integridade dos dados e a disponibilidade dos sistemas, contribuindo para mitigar os riscos e responder rapidamente a possíveis incidentes. Como afirma [2], "as ameaças cibernéticas podem causar sérios impactos aos sistemas, exigindo que sejam neutralizadas constantemente para manter um nível adequado de segurança."

Para mitigar os riscos, técnicas de monitoramento e gerenciamento de redes são essenciais. Ferramentas como IDS (*Intrusion Detection Systems*) e IPS (*Intrusion Prevention Systems*) ajudam a identificar e bloquear atividades suspeitas na rede. Além disso, tecnologias como firewalls e sistemas SIEM (Security Information and Event Management) centralizam a coleta de logs e a análise de eventos, permitindo respostas rápidas a incidentes [6].

O monitoramento de redes também é facilitado por protocolos como o SNMP (*Simple Network Management Protocol*), que permite gerenciar dispositivos conectados e obter métricas de desempenho. Soluções NOC (*Network Operations Center*) centralizam o gerenciamento, oferecendo uma visão completa da infraestrutura de TI [7]

Ferramentas open-source, como Zabbix, Zeek e Grafana, são amplamente utilizadas para monitoramento de redes. O Zabbix fornece recursos para o monitoramento, servidores e serviços [8], enquanto o Zeek é especializado na análise do tráfego de rede. O Grafana, por sua vez, é utilizado para visualização de dados em dashboards interativos. Essas ferramentas, quando integradas, permitem um monitoramento abrangente, com geração de alerta e identificação de anomalias em tempo real [9].

3 Desenvolvimento da aplicação

A solução integrada foi desenvolvida com uma arquitetura modular, composta por três camadas principais: *frontend*, *backend* e módulos de segurança.

Frontend: Responsável pela interface com o usuário, o qual deve ser simples e intuitivo, para esse fim a aplicação Grafana foi utilizado. A interface fornece gráficos e tabelas que mostram o estado atual da rede e os alerta de segurança. O Grafana foi implementado usando bibliotecas JavaScript modernas, aproveitando frameworks como React para facilitar a criação de uma

interface dinâmica e responsiva. Além do mais, o *software* pode ser amplamente personalizado com novas funcionalidades através de *plugins*.

Backend: Implementado em JavaScript (Node.js), o *backend* é o núcleo do sistema, responsável por coletar e processar os dados de monitoramento, gerando alerta em tempo real. Ele também é encarregado de integrar diferentes fontes de dados (Zabbix, Zeek e firewall) e enviar essas informações para o *frontend*. Para a comunicação com os dispositivos monitorados, o *backend* utiliza APIs RESTful, que garantem uma interação eficiente e segura.

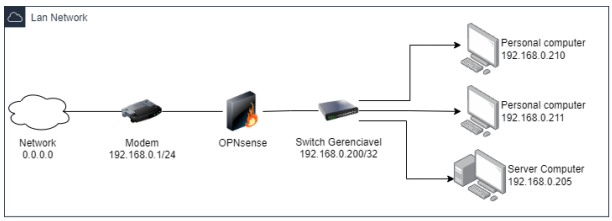
Módulos de Segurança: A camada de segurança do sistema inclui funcionalidades para a detecção de incidentes e respostas automatizadas, como bloqueio de endereços IP suspeitos mediante regras de firewall. Este módulo é responsável por executar ações proativas, como a restrição de tráfego em caso de ataque DDoS ou o bloqueio de portas específicas. Inicialmente, a configuração das regras de firewall foi feita manualmente, contudo, o objetivo final é automatizar este processo com base em políticas de segurança predefinidas.

A abordagem modular foi escolhida para facilitar a integração de diferentes ferramentas de monitoramento e garantir uma estrutura escalável, capaz de se adaptar às necessidades específicas de pequenas e médias empresas. As tecnologias escolhidas para a implementação incluem Zabbix e Zeek para monitoramento, Grafana para visualização de dados e JavaScript para o desenvolvimento do *backend* e extensão do *frontend*.

3.1 Arquitetura do Sistema

O software proposto planeja trabalhar com um conjunto de ferramentas integradas, entre elas o OPNsense[10], sendo um firewall baseado no sistema operacional FreeBSD de código aberto. Portanto, é possivel observar na Figura 2 a arquitetura proposta para utilização do CyberWatch Guard.

Figura 2. Arquitetura proposta para uma rede empresarial.



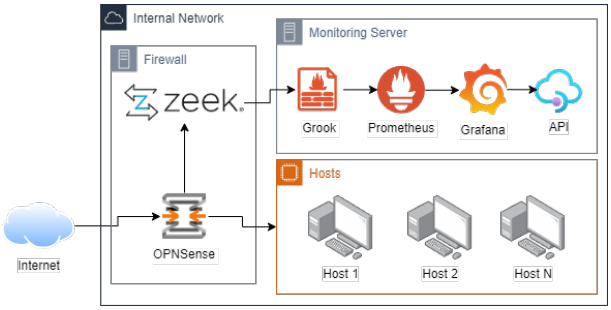
Fonte: Autor (2024).

Na Figura 2 percebe-se que os hosts estão centralizados em um switch gerenciável, o principal objetivo de utilizar esse tipo de switch é utilizar a função de espelhamento de portas para realizar o monitoramento de todo o tráfego da rede com o objetivo do sistema Zeek analisar e gerar os arquivos de logs, posteriormente, esses dados serão enviados para o Grafana. Por fim, os pacotes devem ser inspecionados pelo firewall para saída na Internet.

3.2 Integração das Ferramentas

Durante o desenvolvimento do sistema, as ferramentas foram integradas com o objetivo de fornecer um nível mínimo de segurança para o ambiente empresarial. A arquitetura atual do projeto é observada na Figura 3.

Figura 3. Arquitetura atual do projeto

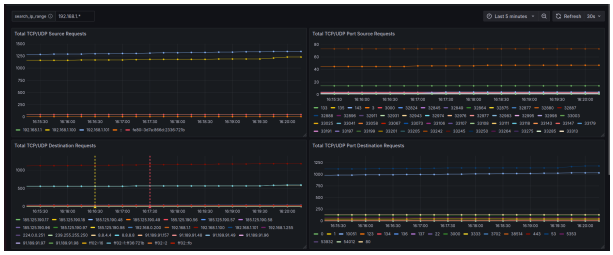


Fonte: Autor (2024).

O Zabbix é utilizado para monitorar o estado dos dispositivos conectados à rede e para analisar o uso de hardware. A adição de novos hosts ao monitoramento é realizada por meio de um *script* em Bash já desenvolvido. Esse *script* é executado pelo administrador da rede, que faz o download e a instalação do agente Zabbix e, em seguida, realiza a configuração na máquina local. Durante a execução, uma requisição é enviada para a API (*backend*), contendo no corpo da mensagem o nome do host, seu endereço IP e a interface de rede utilizada, informações essenciais para o cadastro no servidor do Zabbix.

A API, ao receber a solicitação, realiza duas requisições subsequentes: uma para o Grafana, com o corpo da requisição contendo o modelo em JSON do novo *dashboard* a ser criado, e outra para o Zabbix, registrando o dispositivo na lista de dispositivos para monitoramento contínuo. Para a análise do tráfego de rede em tempo real, a aplicação Zeek é utilizada, monitorando o tráfego por meio de espelhamento de portas e salvando-o em arquivos de *logs* que podem ser posteriormente analisados. A normalização dos dados dos arquivos de *logs* do Zeek é realizada com o programa Grok[11], que utiliza expressões regulares para ajustar os dados antes de enviá-los para o Prometheus[12], o resultado é observado na Figura 4

Figura 4. Métricas observadas pelo software Zeek e enviadas para o Grafana

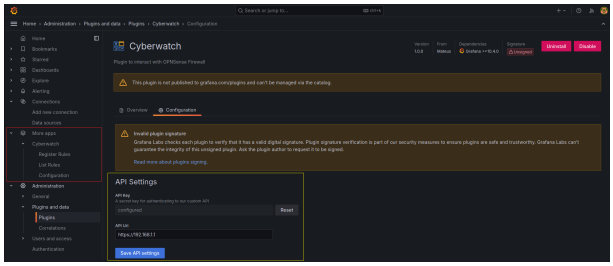


Fonte: Autor (2024).

Para que todos os dados sejam exibidos no Grafana, uma base de dados foi adicionada ao Zabbix utilizando o *plugin alexanderzobnin-zabbix-app*[7], o que permite que os dados monitorados pelo Zabbix sejam encaminhados ao Grafana. Para exibir os dados oriundos do Prometheus, a base de dados nativa do Grafana foi utilizada, eliminando a necessidade de instalação de bibliotecas externas. A escolha do Grafana como plataforma de visualização foi baseada em sua flexibilidade, capacidade de criação de *dashboards* interativos e na presença de uma comunidade ativa.

Por fim, uma última integração foi realizada entre o Grafana e o OPNSense. Para este propósito, foi desenvolvido um *plugin* conforme a Figura 5 que interage com a API do firewall, permitindo ao usuário criar, editar e excluir regras diretamente pela *interface* do Grafana, centralizando as atividades do administrador em uma única plataforma.

Figura 5. CyberWatch *plugin*



Fonte: Autor (2024).

O desenvolvimento da API (*backend*) foi essencial para aumentar a versatilidade do sistema em situações em que uma integração nativa entre os sistemas não era viável, suas principais funções incluem o gerenciamento dos *dashboards*, a interação do usuário com as ferramentas da arquitetura e o tratamento dos alertas gerados, além de auxiliar no processo de automatização de atividades que, de acordo com [13], grande parte das empresas atuais não possui as estruturas necessárias para a implementação de recursos de segurança. Neste sentido, enfatiza-se a necessidade de utilização dos processos automatizados para minimizar o déficit técnico e financeiro que possam impactar e fragilizar a segurança de uma pequena e média empresa.

4 Validação e Testes

A validação do protótipo foi realizada em um ambiente controlado, com testes que simularam diferentes cenários de ataques e falhas na rede. Conforme a Tabela 1 observa-se a configuração do ambiente,

Dispositivo	Sistema Operacional
Computador 1 (Desktop)	Ubuntu 22.04
Computador 2 (Servidor)	Ubuntu 22.04
Computador 3 (Firewall)	OPNSense
Switch Gerenciável	TL-SG10BE

Tabela 1. Fonte: Autor (2024).

que foi adotado para simulação de uma rede de pequena e média empresa. O ambiente utilizado segue a arquitetura apresentada na Figura 2 e a rede utiliza uma máscara de sub-rede /24, sendo possível adicionar um total de 254 hosts.

O sistema foi testado quanto à sua capacidade de detectar incidentes, como ataques DDoS, e gerar alerta para os administradores. Ainda, foi avaliada a precisão dos dados exibidos nos dashboards e a capacidade do sistema de adaptar-se automaticamente a mudanças na topologia de rede. Os resultados dos testes indicaram que o sistema consegue fornecer métricas em tempo real e responder a incidentes eficazmente, embora ainda precise de ajustes na automação nos processos de segurança e na otimização do desempenho. O próximo passo é realizar testes em ambientes de produção para refinar a solução e identificar novos pontos de melhoria.

5 Conclusão

O desenvolvimento do software de monitoramento integrado para redes empresariais mostrou-se viável e promissor, alcançando os objetivos iniciais de centralizar informações de segurança e oferecer uma interface

[7] alexanderzobnin disponível em: https://grafana.com/grafana/plugins/alexanderzobnin-zabbix-app/

amigável para os administradores de rede. A solução, composta por camadas de *frontend*, *backend* e módulos de segurança, demonstrou ser eficiente na coleta de métricas e detecção de incidentes, utilizando ferramentas notáveis como Zabbix, Zeek e Grafana. Os testes realizados em ambiente controlado confirmaram a capacidade do sistema de identificar anomalias e gerar alerta em tempo real, proporcionando um monitoramento mais eficiente e proativo.

No entanto, algumas limitações foram observadas, indicando que o software ainda precisa passar por melhorias. Em particular, a automação das respostas a incidentes de segurança, como o bloqueio automático de tráfego malicioso, deve ser aprimorada para garantir uma proteção mais abrangente. De maneira adicional, ajustes na otimização do desempenho serão necessários para suportar mais dispositivos monitorados sem comprometer a responsividade do sistema. A integração de diferentes fontes de dados e o gerenciamento de grandes volumes de logs também exigem refinamentos para assegurar a consistência e agilidade no processamento das informações.

Apesar dessas áreas a serem melhoradas, os resultados obtidos são promissores e apontam para o potencial do software em atender às necessidades de monitoramento e segurança de pequenas e médias empresas. O trabalho futuro envolverá a realização de testes em ambientes reais, a adição de novas funcionalidades e a integração com outras ferramentas para tornar o sistema ainda mais robusto e adaptável. A continuidade dos esforços de desenvolvimento permitirá transformar a solução proposta em um produto maduro e capaz de contribuir significativamente para a segurança de redes empresariais.

Declarações complementares

Referências

1 Souza, K. *Tentativas de ataques virtuais crescem 75% na pandemia, diz estudo.* Mar. 2021. Disponível em: https://exame.com/tecnologia/tentativas-de-ataques-virtuais-crescem-75-na-pandemia-diz-estudo/.

2 Santos Pinheiro, J. M. dos. Ameaças e ataques aos sistemas de informação: Prevenir e antecipar. *Cadernos UniFOA*, v. 3, n. 5, p. 11–21, 2017.

3 LLC, Z. *Zabbix Monitoring Solution.* 2024. Disponível para Linux, Windows e outros sistemas. Disponível em: https://www.zabbix.com. Acesso em: 15 nov. 2024.

4 Project, Z. *Zeek Network Security Monitor.* 2024. Disponível para Linux. Disponível em: https://zeek.org. Acesso em: 15 nov. 2024.

5 Labs, G. *Grafana.* 2024. Plataforma de visualização e criação de dashboards interativos. Disponível em: https://grafana.com. Acesso em: 15 nov. 2024.

6 Neto, U. Dominando linux firewall iptables. *Rio de Janeiro: Ciência Moderna*, 2004.

7 Oliveira, T. B. de *et al.* Redes de Computadores-SIM–Sistema Integrado para o Monitoramento de Redes de Computadores. *Anais SULCOMP*, v. 5, 2010.

8 4Linux. *O que é Zabbix?* Set. 2021. Disponível em: https://4linux.com.br/o-que-e-zabbix/.

9 Filho, A. G.; Geremias, J. AVALIAÇÃO DA FERRAMENTA ZABBIX. *TCC (Especialização)*, 2010.

10 OPNsense. *OPNsense Firewall.* 2024. Solução de firewall e roteamento de código aberto. Disponível em: https://opnsense.org. Acesso em: 15 nov. 2024.

11 Stäber, F. *Grok Exporter.* 2024. Ferramenta para exportação de logs usando expressões regulares, compatível com Prometheus. Disponível em: https://github.com/fstab/grok_exporter. Acesso em: 15 nov. 2024.

12 Authors, T. P. *Prometheus Monitoring System & Time Series Database.* 2024. Ferramenta de monitoramento e banco de dados de séries temporais. Disponível em: https://prometheus.io. Acesso em: 15 nov. 2024.

13 Silva Costa, J. da. Segurança de redes de computadores na internet. *Revista Inova Ação*, v. 1, n. 2, p. 77–88, 2014.