Aplicação prática de testes de invasão (PENTESTs) para a identificação e mitigação de vulnerabilidades em servidores próprios em datacenters

Tiago José de Andrade, Mario Alexandre Gazziro
{andrade.tiago@ufabc.edu.br, Mario.gazziro@ufabc.edu.br}

INTRODUÇÃO

A dependência das organizações em tecnologia da informação vem aumentando e tornando os datacenters essenciais, mas também expondo-as a ameaças cibernéticas. Em 2023, o custo médio de violação de dados em infraestruturas críticas foi de US$ 5,04 milhões[1]. A Appgate registrou um aumento de 77% nos incidentes globais, com a América Latina sendo a mais afetada[2].

Este trabalho explora a importância dos testes de invasão (PENTESTs) em datacenters para garantir a segurança das informações. PENTESTs são testes realizados por hackers éticos que identificam vulnerabilidades e protegem a rede contra invasores. A prática regular de PENTESTs é crucial para prevenir ataques e fortalecer a segurança cibernética.

Esta pesquisa destaca os benefícios da realização periódica de PENTESTs em datacenters trazendo luz a infraestruturas por vezes negligenciadas. Este estudo visa fornecer uma visão abrangente sobre vulnerabilidades e a importância dos testes de invasão para a proteção dos ativos de informação e a continuidade dos negócios.

OBJETIVO

Este TCC estuda a segurança em servidores próprios de datacenters, como servidores de controle de acesso e monitoramento. O foco é identificar vulnerabilidades em sistemas, redes e aplicativos através de testes de invasão (PENTESTs), avaliando a capacidade da organização de detectar e responder a ataques e a eficácia dos protocolos de segurança. O estudo também revisa políticas e procedimentos de segurança, garantindo sua correta aplicação e elaboração de um procedimento claro para testes constantes. Por fim, busca assegurar a conformidade do datacenter com regulamentações e padrões de segurança da informação, comparando práticas atuais com requisitos de conformidade.

METODOLOGIA

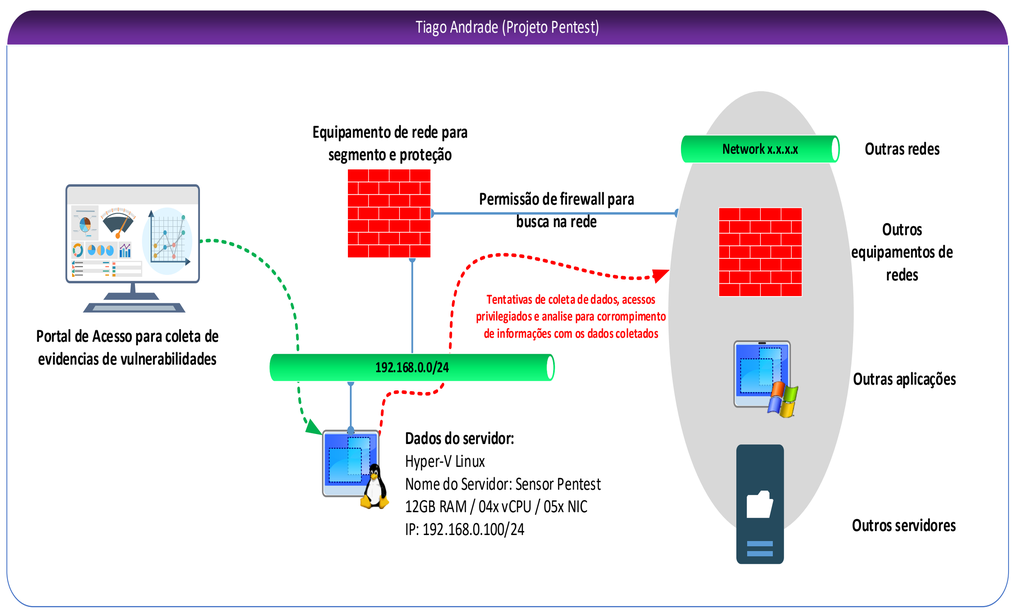

FIGURA 1: Topologia utilizada no Pentest

FONTE: Do Autor.

A metodologia e os procedimentos adotados para este trabalho serão divididas em cinco etapas principais:

- Pesquisa de soluções, escrita do Procedimento e coleta de autorizações necessárias, preparação do ambiente, tentativas de alcançar outras redes, testes de coleta de informações, análise dos resultados, documentação e relatório

Varreduras realizadas: Varredura de rede é uma etapa inicial de um PENTEST, analisando dispositivos conectados para identificar vulnerabilidades como portas abertas e serviços vulneráveis. A varredura autenticada usa credenciais privilegiadas para uma avaliação mais profunda das vulnerabilidades internas.

A varredura de aplicações web identifica falhas específicas em aplicações web, como injeção SQL e XSS. Por fim, a varredura de conformidade verifica se os sistemas estão em conformidade com políticas de segurança e padrões regulatórios, como PCI-DSS e HIPAA.

RESULTADOS E DISCUSSÃO

A implementação das medidas de remediação recomendadas pelo AlienVault fortalecerá a segurança da aplicação web do datacenter, reduzindo o risco de injeção SQL e protegendo dados confidenciais. A ferramenta ajudou na identificação e correção da vulnerabilidade, otimizando o trabalho da equipe de segurança. A descoberta de vulnerabilidades, como a injeção SQL, mostrou o impacto potencial de falhas. O uso da plataforma AlienVault tornou o PENTEST mais eficiente, fornecendo um panorama completo das falhas e orientações para remediação.

CONCLUSÃO

A busca por um ambiente de datacenter seguro é um processo contínuo e dinâmico, que exige investimentos em ferramentas, tecnologias e, principalmente, na capacitação da equipe responsável pela segurança da informação. A metodologia de PENTEST, quando integrada a soluções completas como o AlienVault e amparada por políticas e procedimentos robustos, se consolida como um pilar fundamental para a proteção dos dados, da infraestrutura e da reputação da organização.

REFERÊNCIAS (exemplo)

[1]IBM. Cost of a Data Breach Report 2023. 2023. Disponível em: < https://www.ibm.com/reports/data-breach>. Acesso em: 21 abril de 2024.

[2]APPGATE. Fraud Beat Annual Report. 2023. Disponível em: https://www.appgate.com/resources/ebooks/fraud-beat-annual-report>. Acesso em: 24 abril de 2024