Universidade Federal do ABC

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

Aluno: Tiago José de Andrade
Orientador: Prof. Dr. Mario Alexandre Gazziro

Santo André
2024

RESUMO:

Os datacenters tornaram-se centrais no cenário tecnológico, sendo responsáveis por armazenar informações vitais e hospedar aplicativos cruciais para empresas de diversos setores. Entretanto, essa crescente dependência também tem exposto as organizações a uma série de ameaças cibernéticas. Especificamente nos datacenters, onde concentram-se grandes volumes de dados e recursos críticos, a realização regular de PENTEST's é essencial para garantir a integridade, confidencialidade e disponibilidade das informações. Nosso objetivo é realizar um estudo sobre a segurança em servidores próprios em datacenters, realizando para isso testes de invasão (PENTESTs) que identificam pontos fracos que podem ser alvos de ataques cibernéticos, com base numa metodologia dividida em cinco etapas: pesquisa, ambiente, tentativas, coleta e documentação.

ABSTRACT:

Datacenters have become central to the technological landscape, being responsible for storing vital information and hosting crucial applications for companies in different sectors. However, this growing dependence has also exposed organizations to a range of cyber threats. Specifically in data centers, where large volumes of data and critical resources are concentrated, regularly carrying out PENTEST's is essential to guarantee the integrity, confidentiality and availability of information. Our objective is to carry out a study on security on our own servers in data centers, carrying out invasion tests (PENTESTs) that identify weak points that could be targets of cyber attacks, based on a methodology divided into five stages: research, environment, attempts , collection and documentation.

1. TEMA ESCOLHIDO

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

2. INTRODUÇÃO

Nos últimos anos, a dependência das organizações em relação à tecnologia da informação tem aumentado drasticamente. Os datacenters tornaram-se centrais nesse cenário, sendo responsáveis por armazenar informações vitais e hospedar aplicativos cruciais para empresas de diversos setores. Entretanto, essa crescente dependência também tem exposto as organizações a uma série de ameaças cibernéticas. De acordo com um estudo recente da multinacional IBM [1], o custo médio de violação de dados em infraestruturas críticas em 2023 foi de US$ 5,04 milhões, o que representou US$ 1,26 milhões a mais que o custo em outros setores pesquisados e um aumento 4,26% no custo quando comparado ao mesmo estudo do ano anterior. Ainda em 2023, a Appgate, uma empresa especializada em segurança cibernética, registrou um aumento de 77% nos incidentes em todo o mundo [2]. A América Latina foi a região mais afetada, com um crescimento de 60% nos ataques em relação ao ano anterior. Essas informações são provenientes do relatório anual *Fraud Beat Report* [2], que reúne dados do setor e esclarece os principais aspectos da segurança cibernética que afetam empresas e consumidores globalmente. Em termos amplos, um ataque cibernético pode ser descrito como qualquer atividade que possa comprometer a integridade das informações de um sistema específico. Os ataques podem ser categorizados principalmente com base em três critérios: os resultados que geram, a maneira como são executados e a perspectiva da rede [3]. O relatório da Appgate [2] ainda ressalta um crescimento expressivo nas estratégias de ataque, evidenciando um cenário preocupante em toda a América Latina, conforme já mencionado. De acordo com o estudo, algumas das estratégias mais empregadas por criminosos cibernéticos no último ano incluíram *phishing*, uso não autorizado de marcas, divulgação de informações e *malware*. Portanto, é crucial que as empresas estejam preparadas para gerenciar essa exposição aumentada de maneira eficaz. Diante desse contexto, este trabalho visa explorar a relevância dos testes de invasão/intrusão, conhecidos

como PENTEST's, focando em servidores próprios localizados em datacenters. No âmbito dos testes de vulnerabilidade, os ataques simulados por estes testes são a forma mais direta e transparente de avaliar a gravidade potencial de uma falha de segurança específica. Neste cenário, um PENTEST ou teste de intrusão é um método de teste utilizado por hackers éticos para testar a segurança cibernética de uma infraestrutura de sistema ou rede totalmente integrada e operacional [4]. O teste de penetração ou intrusão é definido como um procedimento para encontrar vulnerabilidades presentes no sistema alvo ou na infraestrutura de rede, a fim de tomar medidas para proteger a rede de reais invasores. Ele auxilia a verificação da capacidade um invasor de penetrar na rede de uma organização ou não. Esta técnica de teste é realizada por um hacker ético ou uma equipe composta por profissionais especialistas em segurança da informação e técnicas de proteção da rede, simulado com usuários não autorizados, que atacam o sistema ou executam a penetração no sistema em teste em busca de vulnerabilidades [4].

Especificamente nos datacenters, onde concentram-se grandes volumes de dados e recursos críticos, a realização regular de PENTEST's é essencial para garantir a integridade, confidencialidade e disponibilidade das informações. O hacking ético, em contraste com práticas como o *hacking black hat* ou *hacking* com intenções maliciosas, desempenha um papel crucial em organizações e empresas que dependem da Tecnologia da Informação (TI) [5]. Essa prática garante que a infraestrutura seja submetida a testes regulares, visando prevenir ataques de hackers mal-intencionados. Os testes de invasão são uma tentativa legal e autorizada de localizar, explorar e invadir sistemas de computadores com o intuito de tornar esses sistemas mais seguros. O processo inclui sondar as vulnerabilidades, bem como oferecer ataques que funcionem como prova de conceito para demonstrar que eles são reais [6]. Busca-se neste trabalho mostrar a necessidade das empresas em empregar especialistas em PENTEST's ou contratar serviços especializados para avaliar regularmente os sistemas operacionais de servidores e hosts em busca de vulnerabilidades, além de evidenciar a importância de implementar recomendações que fortaleçam a segurança desses sistemas [5]. É papel de toda empresa que lida com dados zelar pelos três princípios fundamentais da segurança da informação [7]: confidencialidade, integridade e disponibilidade. Confidencialidade refere-se à proteção das informações contra acesso não autorizado [7]. Integridade garante que as informações sejam precisas e não sejam alteradas sem autorização [7]. Disponibilidade assegura que as informações estejam disponíveis

quando necessárias, evitando interrupções não planejadas nos serviços de informação [7]. Esses princípios formam a base para garantir a proteção adequada dos dados e sistemas de uma organização.

Existem basicamente dois tipos de testes de intrusão: o Físico e Virtual. No teste físico, os testadores avaliam ativos tangíveis, como Data Centers e equipamentos de rede, buscando falhas de segurança no acesso físico e, além disso, inclui a proteção contra desastres naturais. Já no teste virtual, são analisados ativos intangíveis, como sistemas operacionais e servidores web, onde a maioria dos ataques ocorre [8]. Proteger ativos virtuais é mais desafiador e consome a maior parte dos esforços de segurança, representando um desafio maior do que os ativos físicos na segurança da informação [8] e será o foco deste trabalho.

Esta pesquisa abordará os principais benefícios dos PENTEST's em datacenters próprios, destacando como esses testes podem fortalecer as defesas cibernéticas da empresa e prevenir futuros incidentes de segurança. Há diversas recomendações para Datacenters aumentarem a sua segurança cibernética como o uso de firewalls, criptografia de dados, entre outras tecnologias, para proteger a rede e os sistemas do data center [9]. A utilização de sistemas de detecção e prevenção de intrusões ajudará a mitigar problemas com indisponibilidade de serviços, perdas de dados, modificação e adulteração de dados, impactos financeiros e impactos na reputação [9].

Atualmente, espera-se que a inteligência artificial (IA) impulsione e deixar futuros ataques de *ransomware* mais sofisticados, com processos de ataques automatizados, *phishing* mais convincente e desenvolvimento de malware mais rápidos. No entanto, também poderá aprimorar a segurança cibernética, com detecção mais eficaz e rápida de ameaças. Além disso, os testes de intrusão também podem ser beneficiados pela IA tornando-se mais eficazes e abrangentes do que são atualmente [10]. Neste trabalho serão discutidas práticas para a realização de PENTEST's eficazes, considerando os desafios específicos associados aos ambientes de datacenters, como a complexidade da infraestrutura e a diversidade de sistemas e aplicativos hospedados.

Espera-se após estudo fornecer uma visão abrangente para a empresa sobre todas as vulnerabilidades encontradas, ressaltando a importância dos testes de invasão geralmente

esquecidos em relação aos demais testes de vulnerabilidades de infraestrutura, demonstrando como essas práticas podem contribuir significativamente para a proteção dos ativos de informação e a continuidade dos negócios em um ambiente cada vez mais desafiador de cibersegurança.

3. OBJETIVO DA PESQUISA

Neste Trabalho de Conclusão de Curso (TCC), o objetivo é realizar um estudo sobre a segurança em servidores próprios em datacenters. Neste caso, define-se como servidores próprios aqueles utilizados para fins próprios do Datacenter, como servidores de controle de acesso, servidores de câmeras, servidores dos sistemas de monitoramento e outros. Inicialmente, o foco é descobrir vulnerabilidades em sistemas, redes e aplicativos que podem ser exploradas por invasores, realizando para isso testes de invasão (PENTESTs) que identificam pontos fracos que podem ser alvos de ataques cibernéticos. Além disso, o estudo pretende testar a capacidade de uma organização de detectar e responder a ataques e a eficácia dos seus protocolos de segurança existentes. Isso permitirá avaliar os procedimentos de segurança da informação da organização para lidar com incidentes de segurança e identificar áreas que precisam de melhorias.

O estudo também visa verificar se as políticas e procedimentos de segurança estão sendo aplicados corretamente, através da revisão das políticas existentes e da verificação de sua implementação prática. Além disto, para aplicação dos testes será elaborado um procedimento claro, de fácil leitura e execução, de forma a garantir que seja possível executá-lo de maneira constante.

Por fim, o objetivo é assegurar que o datacenter esteja em conformidade com as regulamentações e padrões de segurança da informação, através da revisão das práticas atuais e da comparação com os requisitos de conformidade da empresa e do mercado.

4. PROBLEMA

O problema central que os testes de invasão (PENTESTs) buscam resolver e este trabalho detalhará está ligado à segurança cibernética dos servidores próprios em datacenters. Com a crescente dependência das organizações em relação à tecnologia da informação e a ampliação da exposição na mídia da empresa na qual será feita o estudo de caso neste trabalho, há uma série de

desafios relacionados à proteção de seus ativos de informação contra ameaças cibernéticas. A solução para esse problema requer um enfoque proativo e abrangente para garantir a proteção dos servidores e dos dados críticos hospedados nos datacenters da empresa, mitigando os riscos associados à exposição na mídia e à crescente ameaça de ataques cibernéticos.

A crescente dependência tecnológica das empresas exige a execução constante de atividades como atualizações de sistemas operacionais, instalação de patches de segurança e manutenções preventivas em hardware e software. Essa necessidade de acesso contínuo, tanto por parte de funcionários quanto de terceiros, expõe as organizações a um risco elevado de incidentes de segurança. Ataques cibernéticos, como invasões, malware e engenharia social, podem comprometer a integridade dos sistemas, resultando em vazamento de dados confidenciais, interrupção dos negócios e danos à reputação da empresa.

Nesse contexto, os testes de invasão desempenham um papel fundamental na identificação proativa de vulnerabilidades nos sistemas e redes dos datacenters. Ao simular ataques controlados por hackers éticos, os *PENTESTs* permitem que as empresas descubram e corrijam falhas de segurança antes que sejam exploradas por agentes mal-intencionados. Isso não apenas ajuda a proteger os ativos de informação da empresa, mas também demonstra um compromisso com a segurança cibernética aos clientes, parceiros e stakeholders, fortalecendo a confiança e a reputação da empresa.

5. JUSTIFICATIVA

A segurança da informação em datacenters é um tema cada vez mais importante devido ao crescente volume de dados armazenados e processados nesses ambientes. Os ataques cibernéticos contra datacenters estão se tornando mais frequentes e sofisticados, o que coloca em risco a confidencialidade, integridade e disponibilidade dos dados.) Os testes de invasão (PENTESTs) desempenham um papel crucial diante deste cenário. Eles simulam ataques controlados para identificar vulnerabilidades e avaliar a eficácia das medidas de segurança implementadas.

6. METODOLOGIA

6.1. PROCEDIMENTO DE INVESTIGAÇÃO SUGERIDO

Neste estudo, propomos uma metodologia voltada ao desenvolvimento de uma solução interna em Datacenters para a realização de PENTEST's de segurança da informação. Através destes testes de segurança cibernética, avaliaremos a segurança de uma rede de computadores, sistemas e infraestrutura de tecnologia da informação de um Datacenter. O objetivo principal é identificar e explorar vulnerabilidades nestas redes, da mesma forma que um hacker malicioso faria, porém de maneira ética e autorizada. De forma geral, espera-se encontrar e explorar brechas de segurança em sistemas, aplicativos, dispositivos de rede e outros componentes de TI que possam ser usados por invasores para ganhar acesso não autorizado, roubar informações confidenciais, interromper serviços ou comprometer a integridade dos dados. Abaixo a topologia proposta, a ser utilizada para os testes mencionados nas etapas acima.

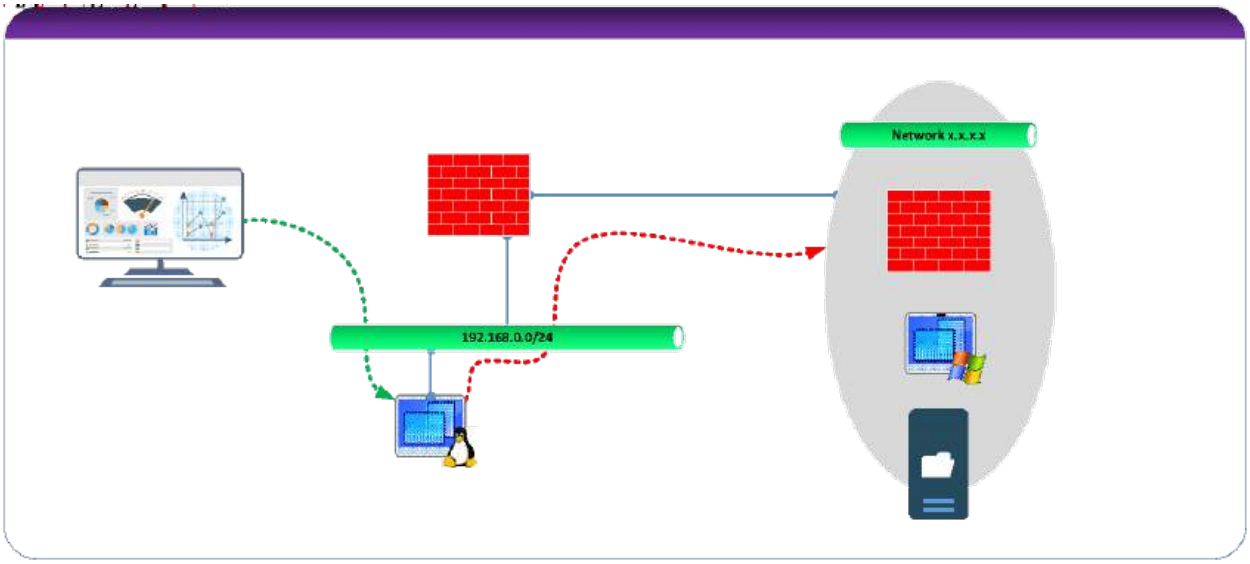


Figura 1. Topologia a ser utilizada para o PENTEST

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:** Nesta etapa será definido o escopo da atividade e as soluções que serão adotadas com a finalidade de resolver o problema relacionado a segurança da informação. Também será realizada uma pesquisa sobre quais ameaças esperamos preparar procedimentos e adotar medidas de defesa. Será escrito um procedimento detalhado com toda a descrição das

atividades a serem feitas, riscos, plano de comunicação interno e aprovações necessárias, plano de retorno em caso de problemas, entre outros. Toda esta preparação terá como finalidade garantir a correta execução e mitigar impactos.

- **Preparação do Ambiente:** Inicialmente, implementaremos um servidor virtual Linux utilizando o Hypervisor Hyper-V. Este servidor será configurado com especificações detalhadas, incluindo a versão do sistema operacional, a quantidade de memória e espaço em disco alocados. Este servidor será então alojado dentro de uma Virtual Local Area Network (VLAN) isolada com o seguinte endereço (192.168.0.0/24). Não está previsto neste trabalho a explicação de como criar servidores.
- **Tentativas de Alcançar Outras Redes:** Utilizando o sistema implementado nesta VLAN isolada, serão iniciadas as tentativas de "alcançar" outras redes, sistemas ou serviços. Para isso, serão utilizadas técnicas específicas, como a varredura de portas e a tentativa de estabelecer conexões. As ferramentas utilizadas e os resultados obtidos serão registrados de forma sistemática.
- **Testes de Coleta de Informações:** Nesta etapa, serão realizados testes através de portas de comunicação específicas para coletar informações. Técnicas como a varredura de portas e a enumeração de serviços para realizar análises que podem identificar possíveis interrupções de serviço e acessos privilegiados. Para mais resultados nas varreduras, será criado um usuário com privilégios de administradores nos sistemas e equipamentos para maiores validações de vulnerabilidades de varredura autenticada.
- **Análise dos Resultados:** As vulnerabilidades são classificadas com base em sua gravidade, utilizando métricas como CVSS (Common Vulnerability Scoring System). Elas podem ser categorizadas como Baixa, Média, Alta ou Crítica.
- **Documentação e Relatório:** Após a conclusão dos testes os resultados serão documentados. As vulnerabilidades identificadas serão registradas, os riscos associados avaliados e recomendações de mitigação devem ser desenvolvidas. O resultado será um relatório detalhado que descreve as vulnerabilidades encontradas, os riscos associados e as recomendações para fortalecer a segurança da rede.

As portas mencionadas nas análises serão as abaixo incluindo a de RDP 3389:

Origem	Tipo	Porta	Destino
192.168.0.100	SSH	22	Outras Redes, Sistemas, Servidores.
	HTTP	80	
	UDP	514	
	TCP	601	
	TCP	602	
	Traffic Mirring	4789	
	WSMANS	5987	
	TLS/TCP	6514	
	TLS/TCP	6515	
	TCP	9000	
	Graylog	12201	
	TCP (RDP)	3389	

Figura 2. Tabela relacionando as portas a serem testadas durante o PENTEST

6.2. INSTALAÇÃO DO AGENTE

Para realizar análises de vulnerabilidades de maneira mais abrangente e contínua, é realizada a instalação de um agente nos servidores, com o objetivo de coletar e enviar dados e varreduras dos sistemas para o servidor do *AlienVault*. No contexto dessa arquitetura, o *AlienVault* é designado como servidor de logs (*Syslog*) e servidor de remediação de vulnerabilidades.

A instalação do agente requer acesso administrativo no servidor alvo. Após realizar login, deve ser iniciado o *PowerShell* com privilégios administrativos e executado o script de instalação do agente.

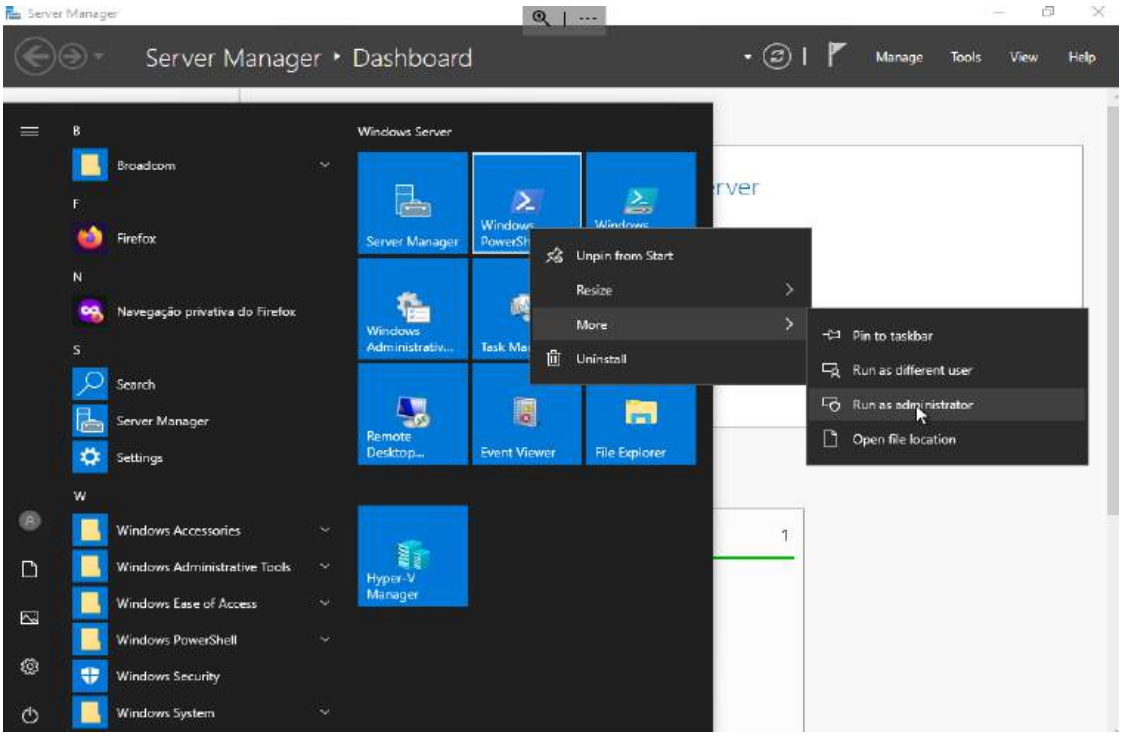


Figura 3. Instalação do agente AlienVault

No console de operação do (*PowerShell*), será executado o script conforme abaixo:

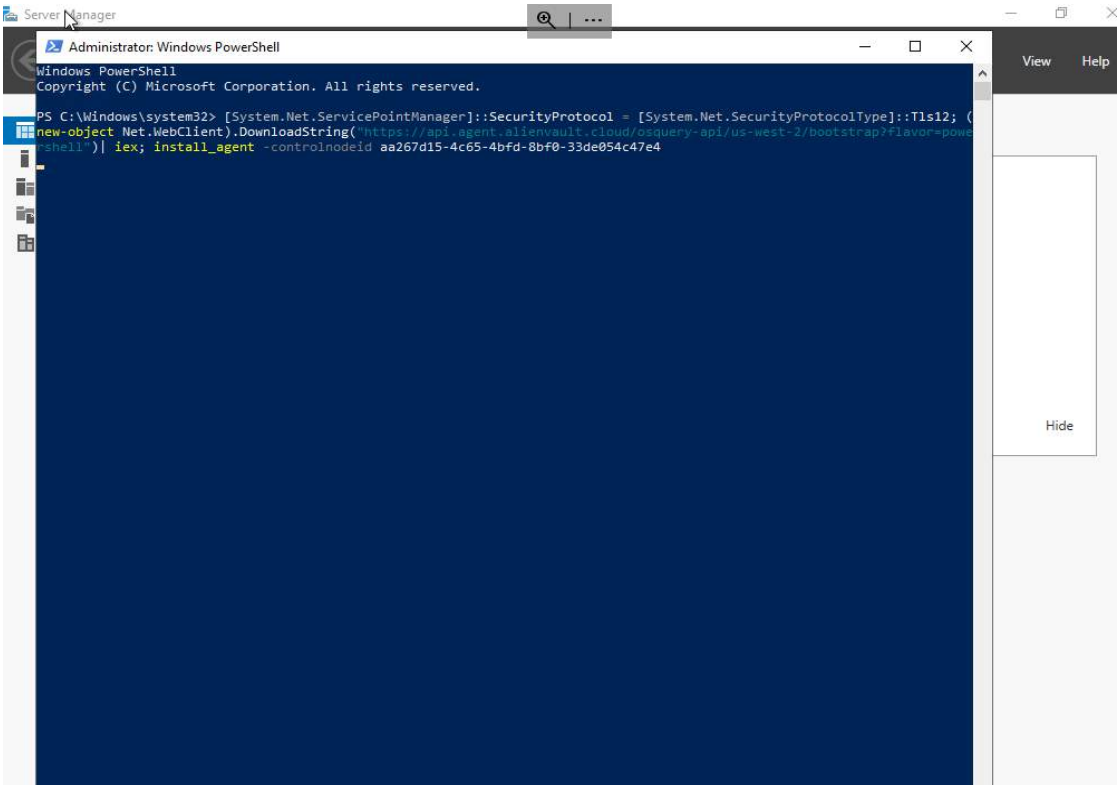


Figura 4. Etapa de instalação do Agente AlienVault

6.3. VALIDAÇÃO E GESTÃO DE AGENTES

Após as intervenções nos servidores, é necessário acessar a plataforma de gerenciamento do AlienVault e verificar se o servidor já está listado na plataforma para realizar as devidas análises e ações. Para realizar essa verificação, será acessada a plataforma de gerenciamento do AlienVault através do site oficial do AlienVault com credenciais de acesso válidas.

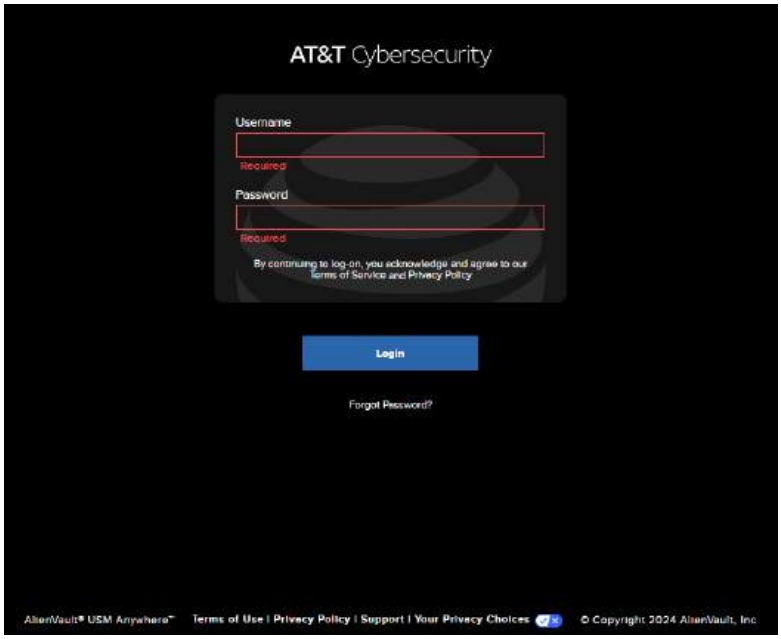


Figura 5. Acesso ao portal do Agente AT&T

Ao fazer login na plataforma, um painel padrão é apresentado por padrão, conforme mostrado abaixo. Este painel pode ser personalizado de acordo com as necessidades do usuário.

Figura 6. Dashboard padrão do agente AllienVault

No menu mostrado abaixo são exibidos os principais dados de agentes instalados e notificações abaixo. Neste caso, há 02 (dois) agentes que precisam ser associados a algum ativo (asset):

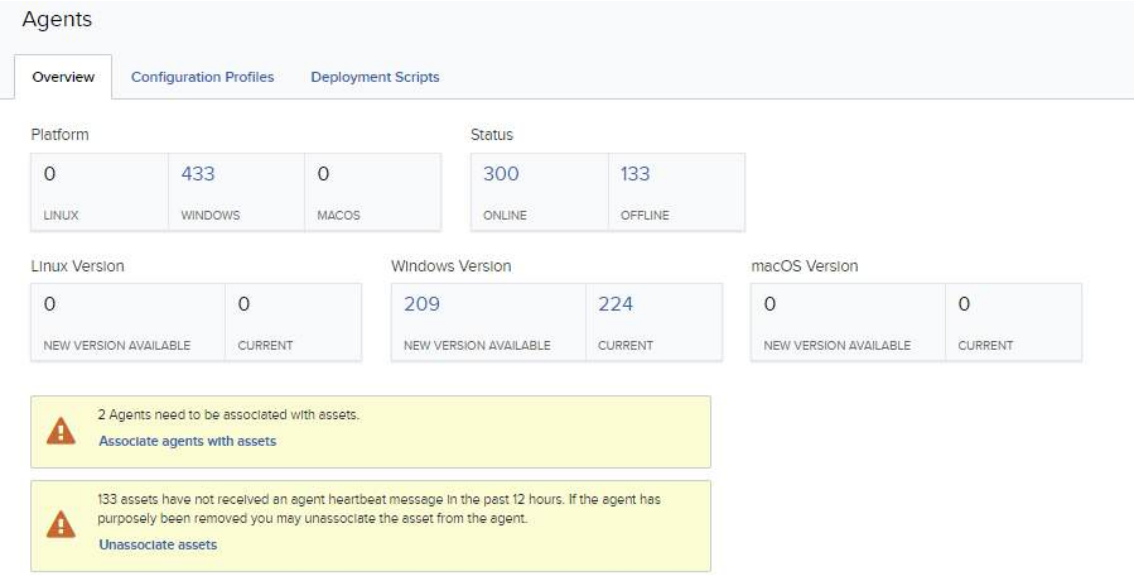


Figura 7. Tela de notificações do agente AllienVault

Uma vez que os novos servidores tenham sido selecionados, a criação de um novo ativo (Creat New Assets) pode ser realizada com um simples clique. Isso permite a análise de possíveis vulnerabilidades presentes nos servidores. Dependendo do nível de risco identificado, medidas corretivas podem ser tomadas, se necessário.

A partir deste ponto, o servidor já se encontra sob monitoramento para identificar vulnerabilidades, alarmes, eventos, problemas, conexões e softwares mal-intencionados. É relevante destacar que a análise padrão de vulnerabilidades realizada pelo AlienVault é baseada em CVEs divulgados. O número CVE, sigla em inglês para Common Vulnerabilities and Exposures (Exposições e Vulnerabilidades Comuns, em tradução livre), é um identificador empregado por fornecedores como Microsoft, RedHat, entre outros, para catalogar vulnerabilidades.

6.4. TIPOS DE VARREDURAS REALIZADAS

A varredura de rede é uma das etapas iniciais de um PENTEST, permitindo a análise de dispositivos conectados à rede para identificar vulnerabilidades conhecidas, como portas abertas, serviços vulneráveis e sistemas desatualizados. Já a varredura autenticada envolve o uso de credenciais de acesso privilegiado, permitindo uma avaliação mais profunda e precisa das vulnerabilidades que exigem acesso interno para serem detectadas. Em paralelo, a varredura de aplicações web foca na identificação de falhas específicas em aplicações web, como injeção SQL, cross-site scripting (XSS) e configurações inseguras de servidores web. Por fim, a varredura de conformidade verifica se os sistemas estão em conformidade com políticas de segurança, padrões regulatórios (como PCI-DSS e HIPAA) e melhores práticas de segurança.

- **Varredura de Rede:** Analisa dispositivos na rede para identificar vulnerabilidades conhecidas. Isso inclui a detecção de portas abertas, serviços vulneráveis, e sistemas desatualizados.
- **Varredura Autenticada:** Realiza varreduras com credenciais, permitindo que o sistema de varredura de vulnerabilidades tenha acesso privilegiado a sistemas e possa identificar vulnerabilidades que exigem acesso interno para serem detectadas.
- **Varredura de Aplicações Web:** Focada em aplicações web, busca vulnerabilidades específicas de web como injeção SQL, cross-site scripting (XSS), e configuração insegura de servidores web.
- **Varredura de Conformidade:** Verifica se os sistemas estão em conformidade com políticas de segurança, padrões regulatórios (como PCI-DSS, HIPAA), e melhores práticas de segurança.

6.5. EXECUÇÃO DA VARREDURA

A varredura de vulnerabilidades envolve uma série de processos automatizados e internos do sistema. Aqui está um detalhamento das principais etapas internas do sistema de varredura de vulnerabilidades utilizado neste projeto:

- **Descoberta de Ativos**
    - **Varredura de Rede**: O sistema de varredura de vulnerabilidades começa identificando todos os dispositivos e sistemas dentro do escopo especificado. Isso inclui a detecção de endereços IP ativos, hosts, e sistemas operacionais. Essa etapa pode usar técnicas como *ping sweep (técnica simples e eficaz para identificar dispositivos ativos em uma rede)* e varredura de portas para mapear a rede.
    - **Enumeração de Portas**: O sistema de varredura de vulnerabilidades verifica as portas abertas nos dispositivos identificados, determinando quais serviços estão em execução e quais portas estão acessíveis externamente.
- **Identificação de Serviços**
    - **Detecção de Serviços**: O sistema de varredura de vulnerabilidades tenta identificar os serviços que estão rodando nas portas abertas (por exemplo, HTTP, FTP, SSH etc.). Ele também identifica as versões dos softwares desses serviços.
    - **Fingerprinting de Sistemas**: A ferramenta realiza a "impressão digital" dos sistemas operacionais e aplicativos para determinar com precisão suas versões, o que é crucial para identificar vulnerabilidades específicas.
- **Varredura de Vulnerabilidades**
    - **Pesquisa em Banco de Dados de Vulnerabilidades**: O sistema de varredura de vulnerabilidades utiliza um banco de dados atualizado de vulnerabilidades conhecidas, incluindo CVEs (Common Vulnerabilities and Exposures). Ele compara as versões dos sistemas e serviços identificados com as vulnerabilidades conhecidas.
    - **Teste de Exploração**: Em alguns casos, o sistema de varredura de vulnerabilidades pode tentar explorar certas vulnerabilidades de forma controlada para confirmar sua existência. No entanto, geralmente a exploração é limitada para evitar causar danos aos sistemas.
- **Varredura Autenticada (Opcional)**
    - **Acesso Autenticado**: Se configurado com credenciais, o sistema de varredura de vulnerabilidades realiza uma varredura autenticada, o que permite acessar o sistema com privilégios mais elevados. Isso possibilita a detecção de

vulnerabilidades que não seriam visíveis em uma varredura não autenticada, como configurações inseguras, software desatualizado ou permissões inadequadas.

- **Verificação de Configurações**: O sistema de varredura de vulnerabilidades também verifica as configurações do sistema em busca de configurações inseguras, políticas fracas de senha, ou configurações padrão que poderiam ser exploradas.

7. RESULTADOS E DISCUSSÃO

7.1. RESULTADOS DOS TESTES PÓS INSTALAÇÃO DOS AGENTES

No servidor recém-utilizado para registro neste trabalho, não foram identificadas quaisquer vulnerabilidades, problemas de configuração ou softwares mal-intencionados. É claro que, por tratar-se de um servidor recém configurado e seguindo todas as políticas de segurança da informação da companhia, este era um resultado esperado.

Figura 8. Tela de alarmes pós instalação do agente e configuração do servidor

A presença de notificações na coluna de alarmes no software de análise de vulnerabilidade é desencadeada por eventos que fogem à operação normal do servidor. Exemplos disso podem incluir a criação de um novo usuário ou até mesmo a modificação de uma política de atualização. Assim, todas as análises são realizadas em todos os alarmes apresentados, conforme ilustrado na figura subsequente.

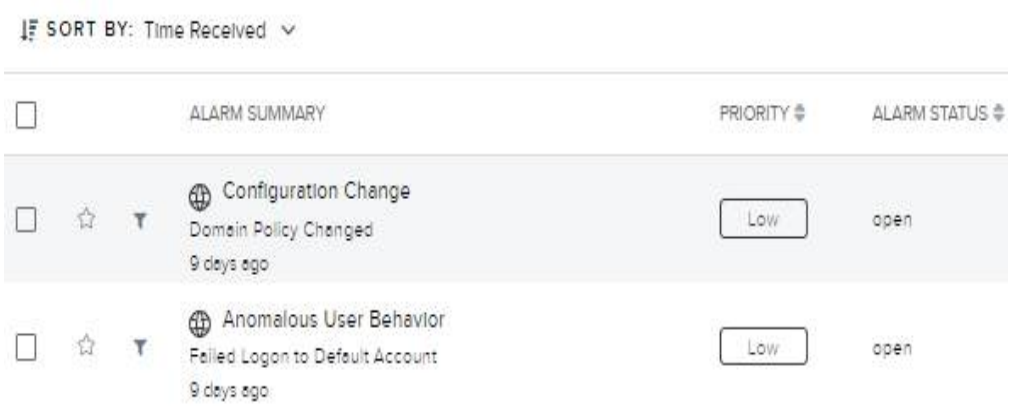


Figura 9. Tela de vulnerabilidades encontradas a partir de comportamentos estranhos à operação normal do servidor

No exemplo a seguir, introduzimos um gerenciador de chaves de licença, que é comumente usado para modificar o número de licença de um software original. Isso permite o acesso completo ao software em questão de maneira ilegal e sem custos. Logo após a cópia deste arquivo para o servidor, o software de gerenciamento de chaves de licença foi automaticamente bloqueado e uma notificação foi enviada para a central de alarmes do portal de vulnerabilidades, conforme pode ser observado na imagem subsequente.

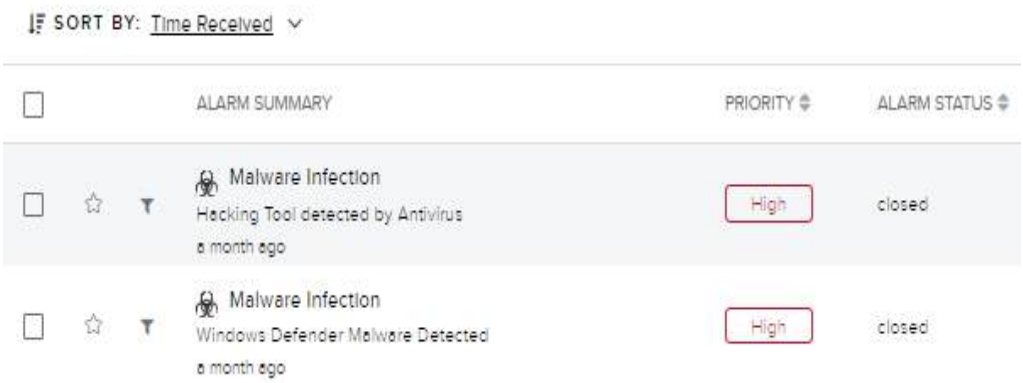


Figura 10. Detecção de software malicioso detectado pelo sistema

Abaixo o relatório detalhando a ação que remediou imediatamente a infecção pelo Malware:

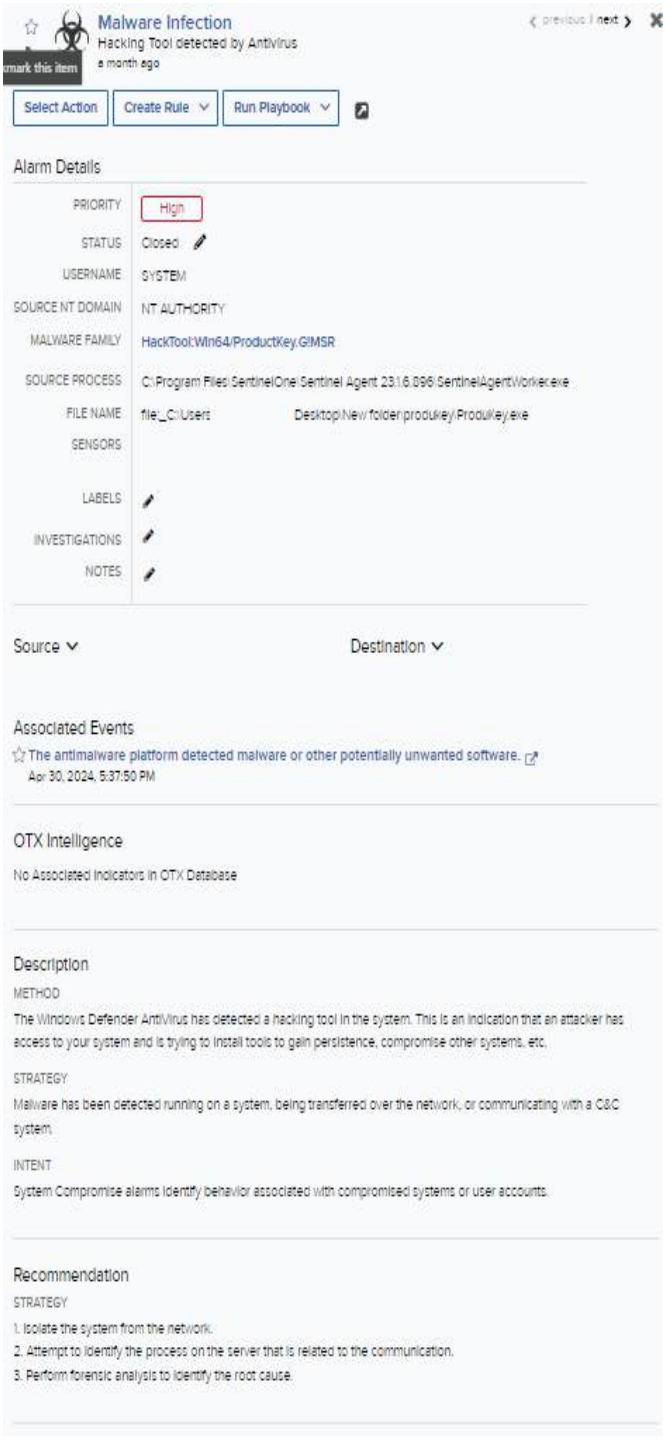


Figura 11. Relatório gerado pelo agente para o problema encontrado

7.2. Vulnerabilidade: Injeção SQL na Aplicação de Gerenciamento do Datacenter

Durante a fase de reconhecimento do PENTEST, utilizando o scanner de vulnerabilidades do AlienVault da AT&T, identificamos uma aplicação web interna utilizada para gerenciar os recursos do datacenter. A ferramenta se mostrou crucial para a identificação dessa aplicação, que não havia sido inicialmente mapeada durante o levantamento de informações, demonstrando a importância de uma varredura abrangente com ferramentas especializadas. A aplicação, acessível apenas por meio da rede interna, permitia aos administradores controlarem servidores, configurar firewalls, gerenciar backups e outras tarefas críticas. Após o mapeamento da aplicação com o AlienVault, direcionamos os testes para o seu formulário de login.

Utilizando as funcionalidades de testes de intrusão presentes no AlienVault, simulamos um ataque de injeção SQL, explorando a falha na validação e tratamento adequado das entradas de dados do usuário no campo de nome de usuário. A ferramenta não apenas identificou a vulnerabilidade, mas também forneceu detalhes sobre a sua criticidade e exemplos de vetores de ataque, agilizando o processo de exploração e demonstrando o impacto real que a falha poderia ter. Ao inserir uma string SQL maliciosa, conseguimos manipular a consulta SQL que valida as credenciais de login, obtendo acesso ao sistema como um administrador, sem a necessidade de uma senha válida.

A exploração bem-sucedida dessa vulnerabilidade, facilitada pelas ferramentas e informações fornecidas pelo AlienVault, permitiu o acesso completo à aplicação de gerenciamento, o que configura um risco crítico para a segurança do datacenter. Um atacante poderia:

- **Controlar toda a infraestrutura:** Com o acesso de administrador, seria possível iniciar, parar ou reiniciar servidores à vontade, causando disrupção total das operações do datacenter.
- **Manipular dados:** A manipulação do banco de dados da aplicação poderia causar perdas ou alterações irreversíveis em dados confidenciais de clientes, configurações cruciais do sistema e backups.

- **Implantar backdoors:** A instalação de backdoors garantiria ao atacante acesso persistente ao ambiente, mesmo após a correção da vulnerabilidade original.

A causa raiz da vulnerabilidade foi a falta de medidas de segurança na codificação da aplicação web, permitindo a injeção de código SQL malicioso. A ausência de validação e tratamento das entradas do usuário, especificamente no campo de nome de usuário do formulário de login, possibilitou a manipulação da consulta SQL e o acesso não autorizado.

Para mitigar a vulnerabilidade, o AlienVault forneceu recomendações específicas de segurança, incluindo:

- **Implementação de Instruções Parametrizadas (Prepared Statements):** Essa técnica impede a interpretação direta das entradas do usuário como código SQL. O AlienVault forneceu exemplos de código e melhores práticas para a implementação dessa técnica na linguagem de programação utilizada pela aplicação.
- **Validação Rigorosa de Entradas:** O AlienVault recomendou a utilização de expressões regulares e listas brancas para validar o tipo, tamanho e formato dos dados inseridos pelos usuários nos formulários da aplicação.
- **Utilização de um Framework de Segurança:** A ferramenta sugeriu frameworks de desenvolvimento web específicos com mecanismos robustos de proteção contra injeção SQL, compatíveis com a linguagem e arquitetura da aplicação.
- **Atualização Constante da Aplicação:** O AlienVault, por ser uma solução integrada, permitiu a configuração de alertas para notificar os administradores sobre novas vulnerabilidades e atualizações de segurança para a aplicação em questão.

7.3. Vulnerabilidade: Acesso direto aos servidores pelo protocolo TCP/RDP

Durante a fase de varredura do PENTEST, uma das primeiras vulnerabilidades apontada pelo AlienVault da AT&T foi a liberação em todos os servidores do protocolo TCP/RDP porta 3389 e possibilidade diretamente de acesso de qualquer terminal (computador) que esteja conectado à rede do servidor ou com acesso de uma determinada *VLAN*.

O *Remote Desktop Protocol (RDP)*, que opera na porta TCP/3389, é amplamente utilizado para permitir o acesso remoto a sistemas Windows. Embora seja uma ferramenta poderosa para administração remota, o RDP é frequentemente alvo de ataques cibernéticos devido a diversas vulnerabilidades e configurações inadequadas. Aqui estão algumas das principais vulnerabilidades associadas ao acesso via RDP na porta 3389:

- Força Bruta e Ataques de Dicionário: O RDP é particularmente vulnerável a ataques de força bruta, onde os atacantes tentam várias combinações de nomes de usuário e senhas até conseguirem acesso. Esses ataques são facilitados por credenciais fracas ou padrões (como "admin" e "password").
- Vulnerabilidades de Softwares: BlueKeep (CVE-2019-0708): Uma vulnerabilidade crítica que afeta versões antigas do Windows, permitindo a execução remota de código sem autenticação. Se explorada, pode permitir que um atacante assuma o controle completo do sistema.
- Credenciais em Texto Simples: Em versões mais antigas do RDP, as credenciais podem ser transmitidas em texto simples, facilitando o roubo de credenciais se o tráfego RDP for capturado por um atacante.
- Exposição Direta à rede: Expor o RDP diretamente à rede torna os sistemas extremamente vulneráveis a ataques automatizados e direcionados. Muitas vezes, essas portas são identificadas por varreduras de rede automatizadas. Para mitigar esta vulnerabilidade é recomendado utilizar *jump servers* ou *bastion hosts* como intermediários seguros. Alterar a porta padrão do RDP de 3389 para outra menos conhecida, embora isso seja mais uma medida de obscuridade do que de segurança real.

O RDP, especialmente quando configurado inadequadamente ou exposto à Internet sem proteções adequadas, é um alvo atraente para atacantes. Proteger o acesso ao RDP na porta 3389 exige uma combinação de práticas recomendadas de segurança, como a aplicação de patches, o uso de autenticação multifatorial, o controle de acesso rigoroso, e a configuração de criptografia adequada. Essas medidas ajudam a minimizar os riscos associados a essa importante ferramenta de administração remota.

7.4. Automação na varredura e monitoramento de vulnerabilidades: Envio de Alertas

Com o agente do AlienVault implementado nos servidores, o envio de e-mail é uma função essencial para a detecção e resposta a incidentes de segurança. Com a capacidade de personalizar, priorizar e automatizar alertas, a plataforma oferece uma solução robusta para o gerenciamento de eventos e a proteção da infraestrutura de TI. Abaixo estão descritos os tipos de alarmes configurados no sistema de varredura e monitoramento de vulnerabilidades AlienVault:

- Configuração de Políticas de Detecção
    - Regras de Correlação: O AlienVault USM utiliza regras de correlação para analisar eventos e identificar padrões de comportamento suspeito ou malicioso. Essas regras podem ser baseadas em eventos específicos (como tentativas de login falhas) ou em combinações de eventos.
    - Assinaturas de Detecção: A plataforma vem com assinaturas de detecção atualizadas regularmente, permitindo a identificação de ataques conhecidos e comportamentos anômalos.
- Detecção de Eventos e Geração de Alertas
    - Eventos de Segurança: Quando um evento é detectado, como um ataque de força bruta, exploração de uma vulnerabilidade ou comunicação com um endereço IP malicioso, ele é registrado pelo sistema.
    - Alertas Automáticos: Com base nas regras configuradas, o AlienVault USM gera alertas automaticamente. Esses alertas podem variar de informativos a críticos, dependendo da gravidade do evento.

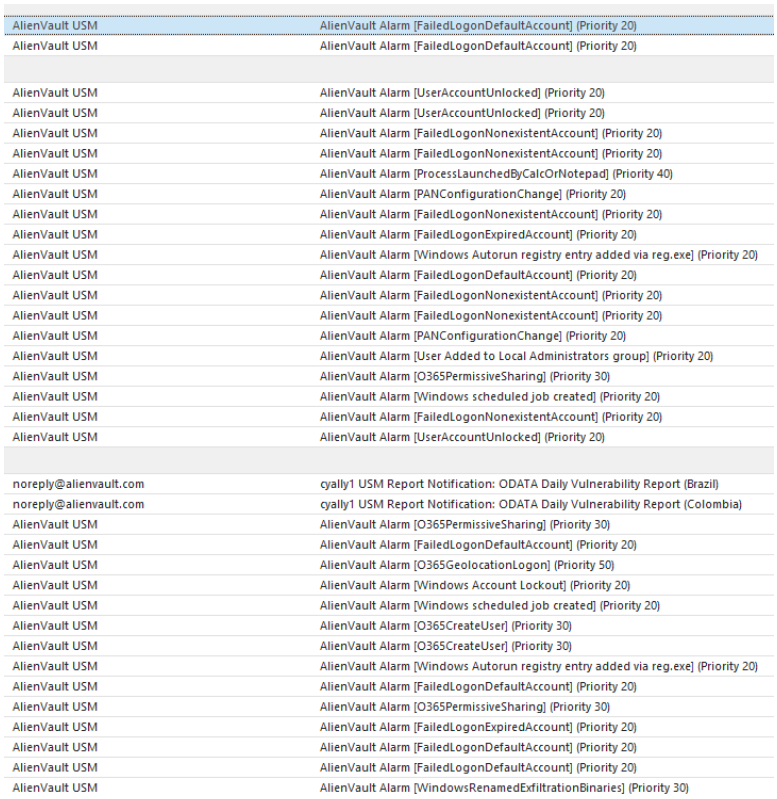
- Envio de Alertas
    - Notificações por E-mail: O AlienVault pode enviar alertas por e-mail para os administradores ou equipes de segurança. Esses e-mails contêm detalhes sobre o evento, como a origem, o tipo de ameaça, e as ações recomendadas.
- Gestão e Priorização de Alertas
    - Correlação de Eventos: O sistema permite correlacionar múltiplos alertas para identificar incidentes maiores. Por exemplo, uma série de tentativas de login falhas seguida por uma tentativa de exploração pode ser agrupada em um único incidente.
    - Ação Imediata: Para alertas críticos, o AlienVault pode ser configurado para acionar respostas automatizadas, como bloquear um endereço IP malicioso ou isolar um dispositivo comprometido da rede.
- Configuração de Critérios de Alerta
    - Customização: Os administradores podem customizar os critérios que geram alertas, como definir um limite para o número de tentativas de login falhas que dispararam um alerta, ou ajustar as regras de correlação para diferentes tipos de ataques.
    - Silenciamento de Alertas: Para evitar sobrecarga de alertas, a plataforma permite o silenciamento de certos tipos de eventos ou alertas para determinados períodos ou situações específicas.
- Relatórios e Auditorias
    - Geração de Relatórios: Além do envio de alertas, o AlienVault USM permite a geração de relatórios detalhados sobre incidentes de segurança e alertas gerados. Esses relatórios são úteis para auditorias de segurança e conformidade.
    - Logs de Alertas: Todos os alertas e eventos são logados, permitindo uma análise posterior e ajudando na identificação de tendências ou na investigação de incidentes.

7.4.1. Benefícios do Envio de Alertas

O envio de alertas é uma funcionalidade central da plataforma, auxiliando as equipes de segurança de TI a responder de forma ágil a incidentes. Neste projeto, foram realizadas

configurações para o envio automatizado de alertas, garantindo que qualquer tipo de ação nos sistemas, seja ela um evento realizado por um administrador autorizado ou um erro de operação e administração, seja imediatamente notificada. Abaixo, apresenta-se uma imagem ilustrando um exemplo de recebimento desses alertas:

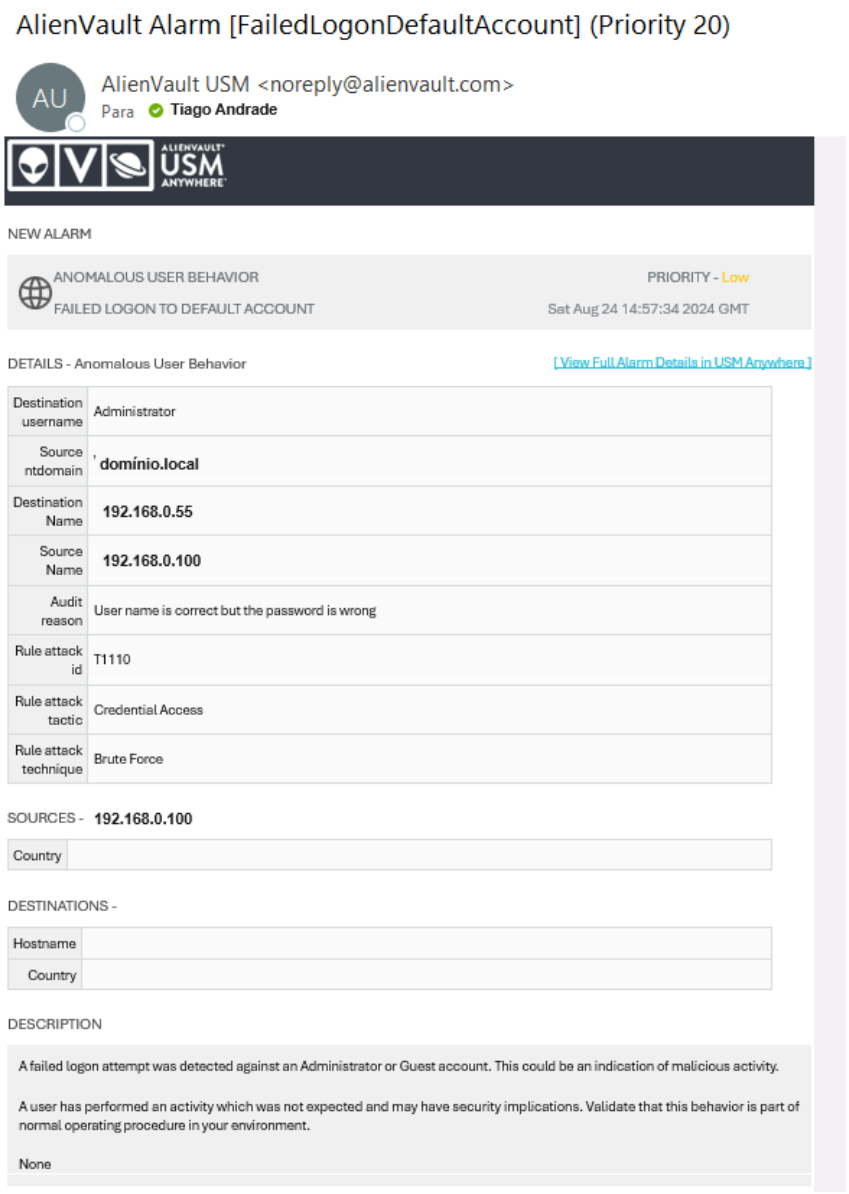
- Resposta Rápida a Incidentes: Alertas em tempo real permitem que as equipes de segurança respondam rapidamente a incidentes, minimizando o impacto.
- Centralização de Informações: Com a capacidade de integrar e correlacionar informações de várias fontes, o AlienVault oferece uma visão unificada da segurança da rede.
- Automação de Respostas: A possibilidade de configurar respostas automáticas a certos tipos de alertas ajuda a mitigar ameaças sem intervenção manual imediata.



AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [UserAccountUnlocked] (Priority 20)
AlienVault USM	AlienVault Alarm [UserAccountUnlocked] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [ProcessLaunchedByCalcOrNotepad] (Priority 40)
AlienVault USM	AlienVault Alarm [PANConfigurationChange] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonExpiredAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [Windows Autorun registry entry added via reg.exe] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [PANConfigurationChange] (Priority 20)
AlienVault USM	AlienVault Alarm [User Added to Local Administrators group] (Priority 20)
AlienVault USM	AlienVault Alarm [O365PermissiveSharing] (Priority 30)
AlienVault USM	AlienVault Alarm [Windows scheduled job created] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonNonexistentAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [UserAccountUnlocked] (Priority 20)
noreply@alienvault.com	cyally1 USM Report Notification: ODATA Daily Vulnerability Report (Brazil)
noreply@alienvault.com	cyally1 USM Report Notification: ODATA Daily Vulnerability Report (Colombia)
AlienVault USM	AlienVault Alarm [O365PermissiveSharing] (Priority 30)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [O365GeolocationLogon] (Priority 50)
AlienVault USM	AlienVault Alarm [Windows Account Lockout] (Priority 20)
AlienVault USM	AlienVault Alarm [Windows scheduled job created] (Priority 20)
AlienVault USM	AlienVault Alarm [O365CreateUser] (Priority 30)
AlienVault USM	AlienVault Alarm [O365CreateUser] (Priority 30)
AlienVault USM	AlienVault Alarm [Windows Autorun registry entry added via reg.exe] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [O365PermissiveSharing] (Priority 30)
AlienVault USM	AlienVault Alarm [FailedLogonExpiredAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)
AlienVault USM	AlienVault Alarm [WindowsRenamedExfiltrationBinaries] (Priority 30)

Figura 12. Alertas gerados pela plataforma

Abaixo um exemplo do e-mail recebido com as informações de alerta de tentativa de acesso:


AlienVault Alarm [FailedLogonDefaultAccount] (Priority 20)

AU

AlienVault USM <noreply@alienvault.com>

Para Tiago Andrade

ALIENVAULT USM ANYWHERE

NEW ALARM

ANOMALOUS USER BEHAVIOR

FAILED LOGON TO DEFAULT ACCOUNT

PRIORITY - Low

Sat Aug 24 14:57:34 2024 GMT

DETAILS - Anomalous User Behavior

[View Full Alarm Details in USM Anywhere]

Destination username	Administrator
Source ntdomain	' domínio.local
Destination Name	192.168.0.55
Source Name	192.168.0.100
Audit reason	User name is correct but the password is wrong
Rule attack id	T1110
Rule attack tactic	Credential Access
Rule attack technique	Brute Force

SOURCES - 192.168.0.100

Country	

DESTINATIONS -

Hostname	
Country	

DESCRIPTION

A failed logon attempt was detected against an Administrator or Guest account. This could be an indication of malicious activity.

A user has performed an activity which was not expected and may have security implications. Validate that this behavior is part of normal operating procedure in your environment.

None

Figura 13. Exemplo de notificação ao usuário

7.5. DISCUSSÕES

A implementação das medidas de remediação recomendadas pelo AlienVault fortalecerá significativamente a segurança da aplicação web de gerenciamento do datacenter, reduzindo o risco de exploração da vulnerabilidade de injeção SQL e protegendo a infraestrutura crítica e os dados confidenciais contra acessos não autorizados. A utilização da ferramenta não apenas auxiliou na identificação da vulnerabilidade, mas também forneceu um guia detalhado para a sua correção, otimizando o trabalho da equipe de segurança.

Este Trabalho de Conclusão de Curso demonstrou a importância crítica da segurança em datacenters, especialmente em servidores próprios, e como a metodologia de PENTEST se mostra uma ferramenta indispensável para alcançar um nível de segurança robusto e resiliente. Através da simulação de ataques reais, o estudo identificou vulnerabilidades em sistemas, redes e aplicações que poderiam ser exploradas por invasores, colocando em risco dados confidenciais e a continuidade das operações.

A descoberta da vulnerabilidade de injeção SQL na aplicação de gerenciamento do datacenter, por exemplo, evidenciou como falhas aparentemente pontuais podem ter um impacto devastador, possibilitando o controle total da infraestrutura por parte de um atacante. No entanto, o estudo foi além da simples identificação de vulnerabilidades. Ao utilizar a plataforma AlienVault da AT&T, o processo de PENTEST se tornou mais abrangente e eficiente, fornecendo não apenas um panorama completo das falhas, mas também orientações detalhadas para a sua remediação.

Os testes realizados também destacaram a presença de riscos adicionais, como a liberação inadequada do protocolo TCP/RDP na porta 3389, que permite o acesso remoto a partir de qualquer terminal conectado à rede. Esta configuração, comumente utilizada para a administração de sistemas, revelou-se altamente vulnerável a ataques como força bruta e exploração de falhas críticas, como o “BlueKeep”. Para reduzir o risco associado a essa prática, foram recomendadas ações como o uso de servidores intermediários seguros, a implementação de autenticação multifatorial, e o controle rigoroso do acesso e da criptografia.

A análise da capacidade de detecção e resposta a incidentes, por sua vez, permitiu avaliar a efetividade dos protocolos de segurança existentes. A simulação de ataques e o disparo de alertas falsos revelaram pontos fortes, como a detecção em tempo real de atividades maliciosas

pelo sistema SIEM, mas também apontaram para oportunidades de aprimoramento, como a necessidade de melhor aderência aos procedimentos de resposta a incidentes.

A revisão das políticas e procedimentos de segurança vigentes, em consonância com as normas e regulamentações do mercado e da própria empresa, confirmou a importância da sua constante atualização e, principalmente, da sua aplicação prática. A elaboração de um procedimento claro e objetivo para a realização de PENTESTs periódicos, como proposto neste trabalho, garantirá que a segurança do datacenter seja constantemente avaliada e aprimorada, criando um ciclo virtuoso de proteção.

7.6. CONCLUSÃO

Conclui-se, portanto, que 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.

7.6.1. RECOMENDAÇÕES

Dado o escopo deste trabalho, algumas áreas merecem maior atenção em estudos futuros. Recomenda-se a realização de pesquisas adicionais sobre o uso de inteligência artificial e aprendizado de máquina na detecção de ameaças em tempo real em ambientes de datacenter. Além disso, seria valioso explorar o impacto de novas arquiteturas de rede, como redes definidas por software (SDN), na mitigação de vulnerabilidades e na melhoria das respostas a incidentes de segurança.

Outro tema relevante para futuras investigações é a análise da eficácia de diferentes soluções de autenticação multifatorial em ambientes corporativos de alta criticidade. Adicionalmente, estudar a integração de sistemas de monitoramento de segurança com soluções de blockchain para garantir a integridade dos dados de auditoria e a transparência nas ações de resposta a incidentes pode oferecer insights importantes para o aprimoramento contínuo das práticas de segurança em datacenters.

Por fim, também é recomendável investigar os efeitos de ataques cibernéticos simulados em larga escala, com o objetivo de avaliar o desempenho das equipes de resposta a incidentes e identificar possíveis lacunas nas políticas de recuperação de desastres.

8. BIBLIOGRAFIA

[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.

[3] LEPESQUEUR, Alexandre; OLIVEIRA, Rodrigo. **PENTEST, ANÁLISE E MITIGAÇÃO DE VULNERABILIDADES**, Trabalho de Graduação, Universidade de Brasília, Brasília, 2006.

[4] RAVINDRAN, Urshila & POTUKUCHI, Raghu. (2022). **A Review on Web Application Vulnerability Assessment and Penetration Testing**. Review of Computer Engineering Studies. 9. 1-22. 10.18280/rces.090101.

[5] FULAFIA JOURNAL OF SCIENCE AND TECHNOLOGY; **Operating System Security And Penetration Testing**., [S. l.], v. 2, n. 2, p. 151–157, 2016. Disponível em: https://lafiascijournals.org.ng/index.php/fjst/article/view/66.. Acesso em: 24 abril de 2024.

[6] ENGEBRETSON, Patrick. **Introdução ao Hacking e aos Testes de Invasão: facilitando o hacking ético e os testes de invasão**. Nova York: Novatec, 2014. 302 p. Tradução de: Lúcia Kinoshita.

[7] Aslan, Ö.; Aktu ˘g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. **A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and**

Solutions. Electronics 2023, 12, 1333. Disponível em: https://doi.org/10.3390/electronics12061333. Acesso em: 25 abril de 2024.

[8] Yaqoob, Irfan & Hussain, Syed & Mamoon, Saqib & Naseer, Nouman & Akram, Jazeb & Rehman, Anees Ur Rehman. (2017). **Penetration Testing and Vulnerability Assessment.** Journal of Network Communications and Emerging Technologies (JNCET), 2017. Disponível em: https://www.researchgate.net/publication/349077887_Penetration_Testing_and_Vulnerability_Assessment. Acesso em: 27 abril de 2024.

[9] SOUZA, Tiago. **Data Centers sob ataque: como contornar os perigos cibernéticos?**.2023. Disponível em: https://www.datacenterdynamics.com/br/opini%C3%B5es/data-centers-sob-ataque-como-contornar-os-perigos-ciberneticos/. Acesso em: 27 de abril de 2024.

[10] Allianz. **Cyber security trends 2023**. 2023. Disponível em: < https://commercial.allianz.com/news-and-insights/reports/cyber-security-trends-2023.html>. Acesso em: 27 abril de 2024.

Assinatura do Orientador