

Fundamentos de Segurança Informática

LAMEGO, 2023



Fundamentos de Segurança Informática

Docente: Francisco Soares

Trabalho realizado por:

David Couteiro (pv26016)

Pedro Almeida (pv26024)

LAMEGO, 2023

**ÍNDICE**

[1. INTRODUÇÃO 6](#_Toc138407539)

[1.1 Objetivo do Projeto 6](#_Toc138407540)

**Introdução**

*Objetivo do projeto*

*Escopo do projeto*

*Descrição da empresa "Marketing Repolhos"*

**Componente de Ataque**

**2.1 Identificação de Vulnerabilidades**

*Exploração da porta 22 (SSH) aberta*

*Uso da wordlist rockyou.txt para ataque de bruteforce*

**2.2 Resultados do Ataque**

*Consequências do acesso não autorizado ao website*

*Identificação de informações sensíveis comprometidas*

**Componente de Defesa**

**3.1 Resposta à Deteção do Ataque**

*Restrição do tráfego proveniente do IP do atacante*

*Fecho da porta 22*

**3.2 Medidas de Segurança Implementadas**

*Controles de acesso adicionais*

*Monitorização contínua do tráfego e atividades suspeitas*

**Componente de Auditoria**

**4.1 Objetivos da Auditoria**

*Verificar a eficácia das medidas de segurança*

*Avaliar a extensão do dano causado pelo ataque*

**4.2 Métodos de Auditoria**

Análise de registos de acesso e logs do sistema

Revisão das configurações de segurança

**4.3 Resultados da Auditoria**

*Identificação de lacunas na segurança*

*Recomendações para melhorias futuras*

**Conclusão**

*Sumarização dos principais resultados e lições aprendidas*

*Considerações finais sobre a segurança informática da empresa "Marketing Repolhos"*

**índice de imagens**

[Figura 1 - Modelo ER da base de dados da ARCL efetuada no TOAD Data Modeler 8](#_Toc138197775)

[Figura 2 - Form Login 11](#_Toc138197776)

[Figura 3 - Form Registar 11](#_Toc138197777)

[Figura 4 - Form Home 12](#_Toc138197778)

[Figura 5 - Form registar intervenção 12](#_Toc138197779)

[Figura 6 - Atividades disponíveis 13](#_Toc138197780)

# INTRODUÇÃO

A segurança informática é um elemento essencial para qualquer organização que depende de sistemas e tecnologia para conduzir seus negócios. Com a crescente ameaça de ataques cibernéticos, é fundamental que as empresas adotem medidas robustas de proteção para salvaguardar seus ativos e informações sensíveis.

O presente relatório apresenta o projeto de segurança informática realizado para a empresa "Marketing Repolhos". O objetivo deste projeto foi identificar vulnerabilidades nos sistemas da empresa, implementar medidas de defesa adequadas e conduzir uma auditoria para avaliar a eficácia das medidas implementadas.

***Considerações Importantes:***

*Durante o relatório observamos que o endereço IP da empresa “Marketing Repolhos” variou ao longo do tempo. Isso ocorreu devido ao facto de o computador host não estar sempre conectado à mesma rede durante todo o processo e também devido à utilização do protocolo DHCP (Dynamic Host Configuration Protocol), uma vez que não foi possível configurar um endereço IP estático. Qualquer discrepância nos IPs deve ser ignorada.*

*No cenário hipotético que irá ser apresentado, deve também ser considerado que a porta 9050 foi publicada na firewall para permitir o acesso ao serviço SSH por meio de uma rede externa*. *Será desta maneira que irá ser possível o acesso ao serviço SSH pelo proxy que será utilizado posteriormente.*

## **1.1 Objetivo do Projeto**

O objetivo principal do projeto é fortalecer a segurança informática da empresa "Marketing Repolhos", minimizando o risco de acesso não autorizado, protegendo informações sensíveis e garantindo a integridade dos sistemas.

**1.2 Finalidade do Projeto**

O escopo deste projeto abrange a análise e proteção do website da empresa "Marketing Repolhos". Será realizada uma simulação controlada de ataque, explorando uma vulnerabilidade identificada na porta 22 (SSH) aberta, será também explorada a porta 5601 dos serviços ELK Stash. Em seguida, serão implementadas medidas de defesa para restringir o tráfego do IP do atacante e fechar a porta 22. Posteriormente, será conduzida uma auditoria para avaliar a eficácia das medidas implementadas.

**1.3 Descrição da Empresa "Marketing Repolhos"**

A empresa "Marketing Repolhos" é uma organização fictícia do ramo de marketing e publicidade. A empresa utiliza serviços online para promover os seus produtos e relacionar-se com os seus clientes. O seu website desempenha um papel crucial na interação com clientes e na exposição de informações sobre os seus serviços.

A screenshot of a computer

Description automatically generated with medium confidence

Figura 1 - Website de Marketing Repolhos Lda.

**Componente de Ataque**

**2.1 Identificação de Vulnerabilidades**

Durante a análise do website da empresa "Marketing Repolhos", foram identificadas vulnerabilidades significativas. A principal vulnerabilidade encontrada foi a porta 22 (SSH) aberta, o que representa um risco potencial de acesso não autorizado aos sistemas da empresa. Essa vulnerabilidade poderia permitir que um atacante explorasse as credenciais de acesso e obtivesse acesso privilegiado ao ambiente da empresa. Além disso, foram identificadas outras portas abertas, como a porta 80 (HTTP), a porta 5601, a porta 9050, bem como a porta 9200 e a 9300. Essas portas abertas também podem representar riscos de segurança, permitindo possíveis ataques ou explorações aos sistemas da empresa.

Durante a realização dos scans e ataques à empresa "Marketing Repolhos", o atacante utilizou a ferramenta Proxychains. Esta ferramenta é uma solução que permite a ocultação do endereço IP real do atacante, redirecionando o tráfego através de uma cadeia de proxies.

Ao utilizar o Proxychains, os atacantes conseguem mascarar a nossa localização e tornar mais difícil a identificação do ponto de origem dos ataques.

A screenshot of a computer

Description automatically generated

Figura 2 - Ficheiro de configuração do Proxychains

A picture containing text, screenshot, font

Description automatically generated

Figura 3 - Resultado do Scan às portas do IP host do website

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Figura 4 - Resultados do scan na ferramenta de deteção de vulnerabilidade Nessus

**2.2 O ataque**

O atacante aproveitando a descoberta da porta 5601 aberta, começou por direcionar os seus esforços para o serviço ELK Stash que hospedava os logs da rede em questão. Com o fim de realizar um ataque, desenvolveu um script personalizado em Python, um web crawler, com o propósito de realizar um ataque bruteforce à página web do Kibana, que dá uma interface aos outros serviços do ELK Stash, pertencentes à empresa em questão.

Foi utilizada a wordlist "rockyou.txt", uma lista popular de passwords comprometidas, como base para esse ataque, esta lista tem cerca de 1 bilhão de passwords.

Por meio deste web crawler, o atacante procurou obter acesso aos registos do sistema presentes na página do Kibana. Com esse acesso, a intenção era verificar as informações disponíveis para a equipa de defesa, desativar regras que existissem para gerar alertas, além de potencialmente apagar registos existentes, caso fosse possível, assegurando assim uma menor probabilidade da equipa de defesa ser alertada para o seu próximo ataque.

A screen shot of a computer program

Description automatically generated with medium confidence

Figura 5 - Script de Python desenvolvido pelo atacante para atacar o serviço Kibana

**A screenshot of a computer

Description automatically generated**

Figura 6- Script a executar o ataque Bruteforce

**A picture containing screenshot

Description automatically generated**

Figura 7- Output da consola, a última password é a correta

**A screenshot of a computer

Description automatically generated**

Figura 8- Visão do atacante após o ataque Bruteforce ser bem-sucedido

A screenshot of a computer

Description automatically generated

Figura 9- O atacante tem agora acesso aos logs da rede

Como o atacante tem agora acesso aos logs do sistema, este tem agora a capacidade de explorar estes para obter informações adicionais sobre o ambiente e as suas configurações. Ao analisar os logs, o atacante pode identificar detalhes sobre a infraestrutura de rede, sistemas operacionais, aplicações em uso, serviços ativos e até mesmo descobrir vulnerabilidades não corrigidas.

Além disso, o acesso aos logs permite que o atacante acompanhe as atividades do sistema, identifique padrões de uso, descubra credenciais de utilizadores, monitorize tentativas de defesa e até mesmo ocultar as suas próprias atividades maliciosas. Com esta visibilidade detalhada do sistema, o atacante pode planear e executar ataques subsequentes de forma mais precisa e direcionada, aumentando o risco para a empresa e os seus clientes.

**A screenshot of a computer

Description automatically generated**

Figura 10- Alertas desligados pelo atacante

A screen shot of a computer code

Description automatically generated with low confidence

Figura 11 - Start da ferramenta de exploitation xHydra ao utilizar a proxy

A screenshot of a computer

Description automatically generated

Figura 12 - Configurações do alvo do alvo do ataque bruteforce SSH

A screenshot of a computer

Description automatically generated

Figura 13 - Configuração do nome de utilizador e da wordlist para serem utilizados no ataque

A screenshot of a computer program

Description automatically generated with medium confidence

Figura 14- Configuração das opções de performance para o ataque

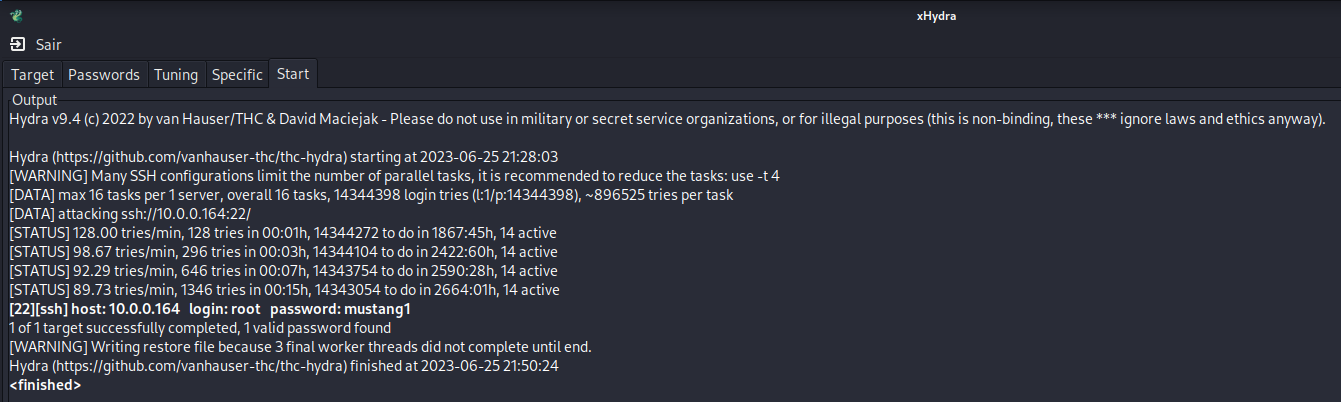


Figura 15 - Descoberta da Password da vítima

**2.2 Resultados do Ataque**

A exploração bem-sucedida da porta 22 (SSH) aberta e a utilização da wordlist "rockyou.txt" resultaram em graves consequências para a empresa "Marketing Repolhos". O atacante conseguiu acesso não autorizado ao website e exfiltrou uma quantidade significativa de dados sensíveis antes que a equipa de defesa pudesse detetar a violação. Essa intrusão comprometeu informações críticas, incluindo dados de clientes, informações de projetos e estratégias de marketing. A exposição destes dados confidenciais representa um risco sério, que pode resultar em prejuízos financeiros, perda de reputação e impacto nas operações da empresa. A necessidade de implementar medidas robustas de segurança e resposta a incidentes torna-se evidente diante desta violação de segurança.

**Componente de Defesa**

**3 Deteção do Ataque**

A equipa de Defesa só percebeu que os seus sistemas tinham sido comprometidos quando ocorreu uma auditoria externa, realizada pela Deloitte. A ausência dos alertas no ElasticSearch foi descoberta durante essa auditoria, revelando a extensão do incidente de segurança. Infelizmente, a equipa falhou na deteção atempada da intrusão, permitindo que os atacantes extraíssem dados essenciais tanto para o funcionamento interno da empresa como para os seus clientes. A intervenção da auditoria externa destacou a importância de uma monitorização contínua e de sistemas de alerta eficazes para garantir a segurança dos sistemas de informação.

**3.1 Resposta à Deteção do Ataque**

Após a deteção do ataque, a equipa de defesa da empresa "Marketing Repolhos" tomou medidas imediatas para mitigar o risco e proteger os seus sistemas. A resposta à deteção do ataque envolveu a restrição do tráfego proveniente do IP do atacante, impedindo qualquer acesso adicional aos sistemas comprometidos. Além disso, a porta 22 (SSH) foi imediatamente fechada para evitar tentativas de acesso não autorizado até ser averiguada a extensão dos danos causados pelo ataque e até ser implementada uma solução de segurança adequada. Essa medida visa proteger o sistema contra possíveis invasões e garantir a integridade dos dados armazenados. Uma vez que a porta 22 foi fechada, os utilizadores não terão acesso remoto ao sistema através do protocolo SSH, mas outras medidas de segurança serão implementadas para minimizar os riscos e restaurar a normalidade das operações. Assim que a extensão dos danos for avaliada e uma solução de segurança adequada for encontrada, a porta 22 será reaberta, permitindo novamente o acesso autorizado ao sistema.

**3.2 Medidas de Segurança Implementadas**

A equipa de defesa implementou várias medidas de segurança para fortalecer a postura de segurança da empresa "Marketing Repolhos" e prevenir ataques futuros.

**3.2.1 Medidas de segurança implementadas**

* **Uso de chaves de autenticação:** Em vez de depender apenas de passwords, a autenticação baseada em chave pública e privada pode ser implementada para acesso ao serviço SSH. Isso envolve a geração de um par de chaves (pública e privada) e a configuração do servidor SSH para permitir apenas a autenticação por meio dessas chaves.
* **Restrição de acesso por endereço IP:** É possível restringir o acesso ao serviço SSH permitindo apenas conexões de endereços IP específicos. Essa abordagem limita a exposição do serviço a fontes confiáveis e diminui o risco de acesso não autorizado.
* **Implementação de VPN (Rede Virtual Privada):** O uso de uma VPN permite que os utilizadores se conectem de forma segura à rede interna da empresa antes de aceder ao serviço SSH. Isso adiciona uma camada adicional de segurança, uma vez que o acesso ao SSH só é possível após a autenticação e conexão bem-sucedidas à VPN.
* **Deteção de comportamento suspeito:** Utilizar sistemas de deteção de intrusões (IDS) ou soluções de análise comportamental pode ajudar a identificar atividades suspeitas ou anomalias no serviço SSH. Essas ferramentas monitorizam padrões de tráfego e comportamentos de acesso, alertando para possíveis ameaças e permitindo uma resposta rápida.

**3.2.2 Atualizações e correções de segurança**

Foi estabelecido um processo regular de atualização de software e aplicação de patches de segurança para garantir que os sistemas estejam protegidos contra vulnerabilidades conhecidas. Essa abordagem proativa e contínua é essencial para manter a segurança dos sistemas da empresa "Marketing Repolhos" e mitigar riscos associados a vulnerabilidades conhecidas.

**Componente de Auditoria**

**4.1 Objetivos da Auditoria**

A auditoria teve como objetivo verificar a eficácia das medidas de segurança implementadas após o ataque e avaliar a extensão do dano causado. Além disso, procurou identificar quaisquer lacunas de segurança remanescentes e fornecer recomendações para melhorias futuras.

**4.2 Métodos de Auditoria**

**Para realizar a auditoria, foram utilizados os seguintes métodos:**

**4.2.1 Análise de registos de acesso e logs do sistema:** Foram examinados os registos de acesso e os logs do sistema para identificar possíveis atividades suspeitas, tentativas de acesso não autorizado e quaisquer alterações indevidas nos sistemas. Essa análise permitiu identificar eventuais falhas ou anomalias.

**4.2.2 Revisão das configurações de segurança:** As configurações de segurança foram revistas em busca de possíveis falhas de configuração ou configurações inadequadas que poderiam comprometer a segurança dos sistemas. Essa revisão foi realizada em firewalls, sistemas de deteção de intrusões e outros componentes de segurança.

**4.3 Resultados da Auditoria**

A auditoria identificou algumas lacunas na segurança do ambiente da empresa "Marketing Repolhos". Foram encontrados pontos de melhoria nas seguintes áreas:

**4.3.1 Políticas de segurança**: Recomenda-se a revisão e o fortalecimento das políticas de segurança, incluindo a implementação de políticas de passwords mais rigorosas, a definição de privilégios de acesso adequados e a realização de sessões de conscientização de segurança informática para os funcionários.

**4.3.2 Monitorização de segurança:** Sugere-se o aprimoramento do sistema de monitorização contínua, com a implementação de soluções de deteção de intrusões mais avançadas e a análise regular dos registos de acesso e logs do sistema.

**4.3.3 Atualizações e patches de segurança**: Recomenda-se a manutenção regular de atualizações e patches de segurança em todos os sistemas da empresa, para garantir que estejam protegidos contra vulnerabilidades conhecidas.

**Conclusão**

Este projeto de segurança informática para a empresa "Marketing Repolhos" destacou a importância de implementar medidas eficazes de defesa para proteger os sistemas contra ameaças cibernéticas. Através da identificação de vulnerabilidades, resposta à deteção do ataque e auditoria, f­oi possível tomar ações corretivas e preventivas para garantir a segurança dos ativos e informações da empresa.

As principais lições aprendidas incluem a necessidade de manter os sistemas atualizados, implementar práticas adequadas de gerenciamento de passwords, realizar monitoração contínua e estabelecer uma cultura de conscientização em segurança informática entre os funcionários. A segurança informática é um esforço contínuo que requer atenção constante e adaptação às nova­s ameaças.

Considerações finais sobre a segurança informática da empresa "Marketing Repolhos" destacam a importância de investir em recursos adequados de segurança, incluindo uma melhor configuração dos seus sistemas de deteção de intrusões e auditoria regular, bem como a encriptação de dados sensíveis, por meios digitais ou adotar uma encriptação dos discos que armazenam informação deste tipo, utilizando por exemplo, a solução BitLocker. A proteção dos dados sensíveis e a preservação da reputação da empresa são fundamentais para o sucesso e a continuidade dos negócios.

­