INSTITUTO FEDERAL GOIANO – CAMPUS CERES
SISTEMAS DE INFORMAÇÃO
LAURA SOUSA LIMA
LÁYZA FERREIRA LOPES
MARIA EDUARDA DE SÁ
RAYLLANDER ANTONIO MATIAS DE MORAIS

INFRAESTRUTURA DE REDE – FARMÁCIA MODELO

CERES – GO
2023

Avaliação da Estrutura Atual

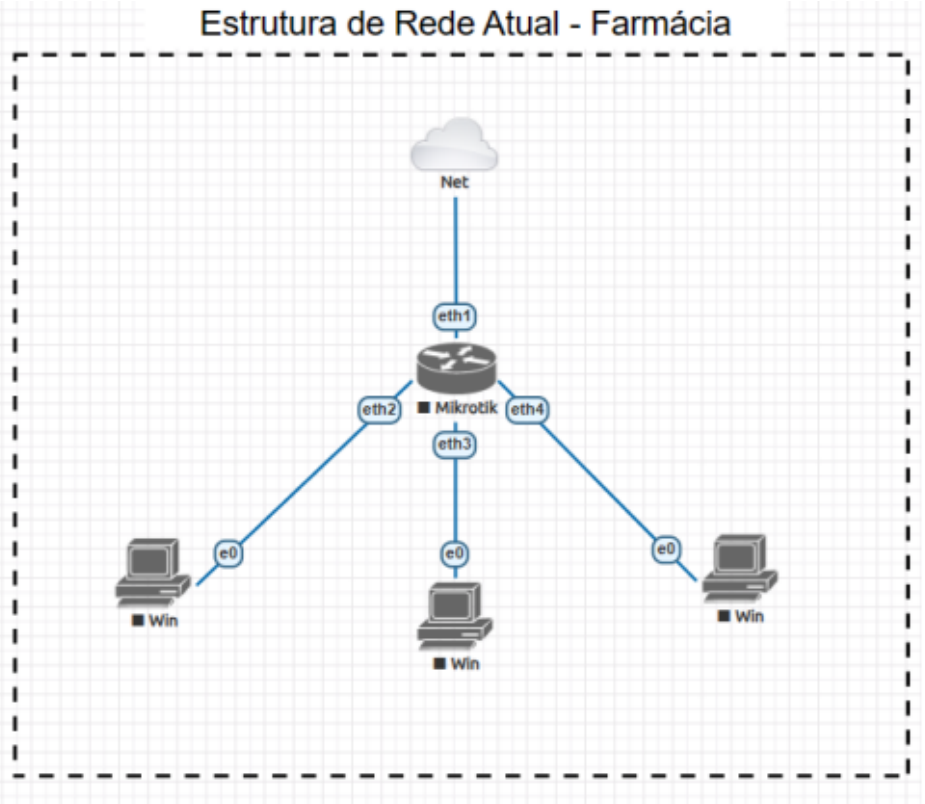
A Farmácia Modelo, localizada na cidade de Ceres/GO, possui uma infraestrutura de rede sólida e eficiente para suportar suas operações diárias. A estrutura é composta por diversos elementos que trabalham em conjunto para garantir uma conectividade estável e segura. No entanto, diante do contínuo avanço da base tecnológica da farmácia, tornou-se necessário aprimorar sua segurança cibernética. Essa iniciativa busca alcançar maior redundância e resiliência, fortalecendo ainda mais a proteção dos dados essenciais da farmácia contra ameaças potenciais.

A Farmácia Modelo utiliza -se de um link de internet fornecido por um provedor local confiável. Esse link é crucial para diversas atividades, como processamento de vendas, atualizações de estoque, e acesso a informações relevantes sobre medicamentos. Na ponta inicial da rede, encontra-se um roteador MikroTik. Este dispositivo desempenha um papel central na gestão do tráfego de dados. Ele é responsável por receber o sinal do provedor de internet e direcioná-lo adequadamente para a rede interna da farmácia.

A partir do roteador MikroTik, a rede é distribuída para os diferentes dispositivos dentro da farmácia. A infraestrutura de rede interna é projetada para fornecer conectividade confiável e eficiente.

A farmácia utiliza três computadores conectados à rede interna. Esses computadores desempenham funções críticas, como registro de vendas, controle de estoque, e interação com sistemas de informações sobre medicamentos. Cada computador é configurado para acessar a internet de forma segura e rápida, permitindo que a equipe execute suas tarefas diárias de maneira eficiente.

Segue abaixo a estrutura atual da Farmácia sendo representada pelo software de simulação EVE-NG.



Na implementação de um sistema em nuvem para a Farmácia Modelo, optou-se pela AWS (Amazon Web Services), que disponibiliza uma ampla gama de serviços de Infraestrutura como Serviço (IaaS) para facilitar o alojamento e gestão de recursos na nuvem. Um exemplo proeminente desse modelo IaaS é o Amazon S3 (Simple Storage Service), um serviço que oferece armazenamento de objetos escalável e durável, especialmente adequado para o arquivamento de dados, gestão de arquivos e backups.
O Amazon S3 destaca-se como uma solução versátil que pode ser aplicada em diversas instâncias na Farmácia Modelo, tais como:

• Armazenamento de Documentação e Regulamentação: Garantindo um repositório seguro e acessível para documentos críticos relacionados à regulamentação e conformidade.

• Backup e Recuperação de Dados: Facilitando a criação de backups regulares e eficiente recuperação em caso de necessidade.

• Armazenamento de Imagens Médicas e Resultados de Testes: Oferecendo um local centralizado para imagens médicas e resultados laboratoriais, facilitando o acesso e referência.

• Arquivamento de Dados Históricos: Permite a organização e arquivamento eficiente de registros históricos, como histórico de vendas e prescrições antigas, otimizando o espaço e facilitando a busca quando necessário.

Análise de Vulnerabilidade

Na busca por informações essenciais sobre a infraestrutura de rede, empregamos ferramentas especializadas, destacando-se o Nmap. Essa ferramenta viabiliza uma análise minuciosa, abordando desde a identificação de portas acessíveis e serviços em operação até a enumeração de endereços IP associados aos dispositivos presentes na rede. Para localizar portas acessíveis, recorremos ao comando nmap -sV 192.168.56.10.

Ao realizar uma análise das portas por meio do Nmap, identificamos a presença da porta 22 aberta, associada a um serviço comum de SSH. Essa constatação levanta preocupações, uma vez que, no contexto deste projeto, o Vagrant foi empregado. A hipótese sugere que o desenvolvedor possa não ter alterado as credenciais padrão do Vagrant. Considerando essa possibilidade, percebemos um potencial vulnerabilidade, onde a utilização das credenciais padrão "vagrant" para ambos o nome de usuário e senha possibilitaria um acesso fácil:

ssh vagrant@192.168.56.10

Essa abordagem concederia acesso irrestrito à máquina, representando uma lacuna significativa na segurança.

O Nuclei é uma ferramenta robusta e essencial no conjunto de recursos dos profissionais de segurança da informação, sendo amplamente empregado para a identificação e verificação de vulnerabilidades em aplicações web. Essa ferramenta desempenha um papel crucial ao automatizar o processo de análise de servidores e serviços, proporcionando uma abordagem eficaz na detecção de possíveis brechas de segurança. Outro aspecto crucial a ser abordado na análise é a avaliação de potenciais erros de configurações comuns em aplicações. Essa abordagem possibilita identificar e corrigir brechas decorrentes de configurações inadequadas, fortalecendo assim a resiliência da infraestrutura contra possíveis ameaças. Para utilizar o Nuclei e realizar verificações específicas de vulnerabilidades, podemos empregar o seguinte comando:

nuclei -severity info,low,medium,high,critical -target 192.168.56.10

Ao analisar a resposta fornecida pelo Nuclei, destacam-se diversas informações pertinentes à aplicação web básica. Notavelmente, observa-se a exposição do diretório do Git, uma falha comum que os desenvolvedores, por vezes, negligenciam ao realizar o upload do projeto para o repositório Git:

http://192.168.56.10 /.git/

Para abordar essa vulnerabilidade, é aconselhável adotar medidas corretivas, como a remoção do diretório exposto ou a restrição de acesso ao mesmo. Essas práticas são cruciais para mitigar riscos associados à divulgação inadvertida de informações sensíveis.

Ao detectar essa lacuna, torna-se possível identificar informações cruciais sobre o projeto contidas no repositório Git. Portanto, é imperativo que os desenvolvedores estejam cientes dessa fragilidade e adotem práticas de segurança sólidas ao gerenciar e compartilhar código-fonte, garantindo assim a preservação da confidencialidade e integridade do projeto. A falha de git exposto neste projeto é apenas um exemplo do que pode acontecer ao negligenciar a pasta git.

O tcpdump é uma ferramenta essencial de linha de comando em ambientes Unix, destacando-se por sua capacidade de capturar e analisar pacotes de rede em tempo real. Sua aplicação abrangente abarca desde o monitoramento do tráfego de rede até a facilitação na resolução de problemas, análise de desempenho e detecção proativa de potenciais ameaças cibernéticas.

Essa abordagem abrangente não apenas identifica potenciais vulnerabilidades, mas também proporciona insights valiosos para fortalecer proativamente a postura de segurança da rede. A análise de vulnerabilidades é um componente crítico na manutenção da integridade e segurança da infraestrutura, garantindo uma resposta eficaz a possíveis ameaças cibernéticas.

Implementação de Firewalls e Propostas de Melhoria

Para demonstrar o ambiente de maneira mais eficiente, optamos pelo uso do software Vagrant para a geração simplificada de máquinas virtuais. Esse ambiente proporciona facilidade na configuração e realização de testes virtualizados.

Iniciamos as configurações no Vagrant para criar inicialmente o servidor Gateway, designado como "Gateway" dentro do ambiente Vagrant. Em seguida, procedemos à criação das máquinas clientes, identificadas como Vm1, Vm2, todos com S.O Linux.

Após a inicialização da máquina Gateway, procedemos à configuração da interface de rede, criando duas interfaces: uma privada (Private Network) com o IP 192.168.56.1 e outra pública (Public Network) destinada a ser utilizada como uma interface WAN.

Posteriormente, foram criadas as máquinas clientes Vm1 – IP 192.168.56.10, Vm2 – IP 192.168.56.20. Todas essas máquinas foram configuradas com interfaces de rede privada (Private Network) e o Gateway padrão definido como 192.168.56.1. Esse processo visa estabelecer uma infraestrutura de rede coesa e eficiente para a Farmácia Modelo.

Segue abaixo código utilizado no arquivo Vagrantfile.

Vagrantfile (1) | Workspace Trust

D: > Downloads > Vagrantfile (1)

```
Vagrant.configure("2") do |config|
  # Configuracao da Gateway - Servidor Gateway e Firewall
  config.vm.box = "generic/ubuntu2004"

  config.vm.define "gateway" do |gateway|
    gateway.vm.hostname = "gateway"
    gateway.vm.network "private_network", type: "static", ip: "192.168.56.1"
    gateway.vm.network "public_network", type: "dhcp"
    gateway.vm.provider "virtualbox" do |vb|
      vb.memory = "512"
    end
    gateway.vm.provision "shell", inline: <<-SCRIPT
      # Instalacao do Apache
      sudo apt update
      sudo apt install net-tools
      sudo apt install -y apache2
    SCRIPT
  end

  # Configuracao da VM1 - Maquina Cliente 01
  config.vm.define "vm1" do |vm1|
    vm1.vm.hostname = "vm1"
    vm1.vm.network "private_network", type: "static", ip: "192.168.56.10"
    vm1.vm.provider "virtualbox" do |vb|
      vb.memory = "512"
    end
    vm1.vm.provision "shell", inline: <<-SCRIPT
      # Instalacao do MySQL
      sudo apt update
      sudo apt install net-tools
      sudo apt install -y mysql-server
      sudo ip route add default via 192.168.56.1
    SCRIPT
  end

  # Configuracao da VM2 - Maquina Cliente 02
  config.vm.define "vm2" do |vm2|
    vm2.vm.hostname = "vm2"
    vm2.vm.network "private_network", type: "static", ip: "192.168.56.20"
    vm2.vm.provider "virtualbox" do |vb|
      vb.memory = "512"
    end
    vm2.vm.provision "shell", inline: <<-SCRIPT
      # Instalacao do MySQL
      sudo apt update
      sudo apt install net-tools
      sudo apt install -y mysql-server
      sudo ip route add default via 192.168.56.1
    SCRIPT
  end
```

Monitoramento contínuo de tráfego

Assegurar a segurança da rede é de suma importância, e para alcançar esse objetivo, a implementação de ferramentas avançadas de monitoramento de tráfego torna-se imperativa. Essas ferramentas não apenas identificam padrões anormais, mas também oferecem a capacidade de configurar alertas, mantendo a equipe de segurança informada sobre atividades suspeitas em tempo hábil.

Entre as ferramentas mais eficazes para esse propósito, destaca-se o Tcpdump.É robusto o suficiente para analisar o tráfego de rede em tempo real, permitindo também salvar informações para referências futuras. A flexibilidade proporcionada na criação de filtros é crucial, permitindo a detecção precisa de tráfego incomum. Dessa forma, ao configurar alertas personalizados, é possível automatizar notificações, garantindo uma resposta ágil diante de possíveis ameaças. A utilização eficaz do tcpdump envolve comandos específicos, como exemplificado abaixo:

```
sudo tcpdump -i eth0 -w captura.pcap
```

Esse comando captura o tráfego em tempo real na interface designada e salva os resultados no arquivo "captura.pcap". Em seguida, para análise subsequente do tráfego armazenado, empregamos o comando:

```
tcpdump -r captura.pcap
```

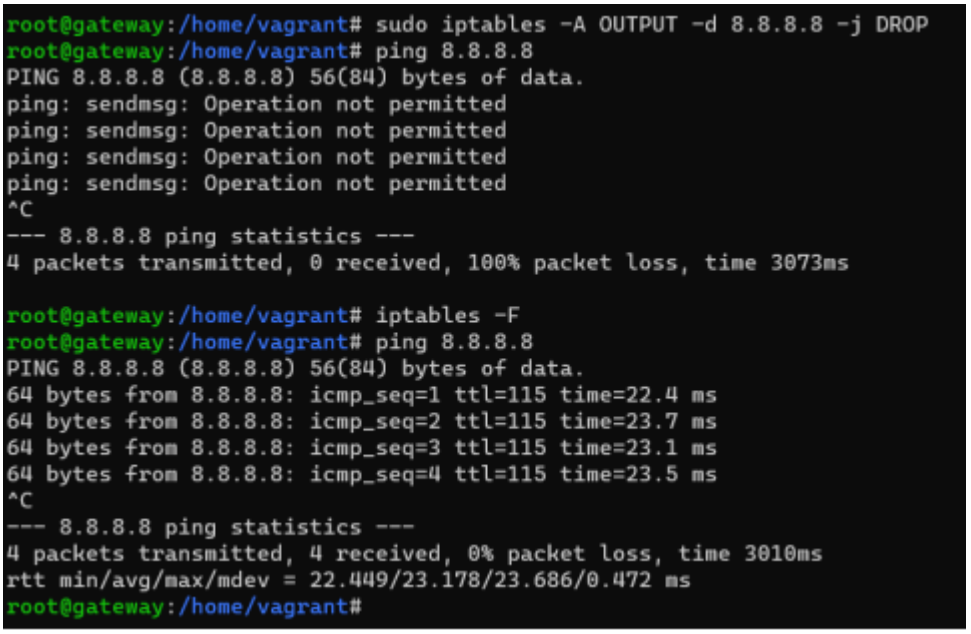
A condução de testes de simulação é outra prática de grande importância. Esses testes não apenas oferecem parâmetros sobre a eficácia dos protocolos de segurança estabelecidos, mas também auxiliam na avaliação do desempenho das ferramentas de monitoramento. A realização desses testes em um ambiente controlado é crucial para aprimorar as capacidades de resposta a incidentes.

Neste contexto, é vital enfatizar que o monitoramento contínuo não se trata apenas de uma medida reativa, mas também de uma abordagem proativa na identificação e mitigação de ameaças potenciais. Ao investir em ferramentas de ponta e conduzir testes regulares, a equipe de segurança está mais bem equipada para manter a integridade da rede e responder de forma eficaz a qualquer eventualidade.

Resultados esperados e Conclusão

Dessa forma, é possível concluir que, no âmbito do planejamento estabelecido, a rede da farmácia experimentou uma notável redução de vulnerabilidades. Isso se deve à implementação de novos métodos de gerenciamento de rede, com a introdução de um servidor Gateway dedicado, aliado à utilização da ferramenta IPtables para aplicação de regras, como bloqueio de IPs e portas específicas.

Segue abaixo um exemplo da implementação de uma regra pelo IPtables.



Além disso, observou-se uma considerável melhoria na capacidade de detecção e resposta a ameaças com a incorporação das ferramentas Nuclei e Tcpdump. Essas ferramentas possibilitaram uma análise em tempo real do tráfego de rede em nosso ambiente, fortalecendo a segurança e proporcionando uma abordagem mais proativa na gestão de potenciais riscos.