**Relatório de Implementação de Segurança de Rede no DEI**

-> US - 650 Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução

Introdução:

Este relatório descreve a implementação de medidas de segurança para garantir que apenas clientes da rede interna do DEI, seja via conexão cablada ou VPN, tenham acesso à nossa aplicação.

O objetivo é restringir o acesso ao servidor da aplicação para aumentar a segurança e controlar o tráfego.

Metodologia:

A estratégia envolveu o uso do iptables, uma ferramenta de manipulação de tabelas de roteamento do kernel do Linux, para filtrar o tráfego de rede.

A configuração foi projetada para bloquear todo o acesso não autorizado ao servidor e permitir apenas tráfego de IPs específicos.

Etapas de Implementação:

Definição de Política Padrão:

Configuramos a política padrão da cadeia INPUT para DROP.

Isso significa que todos os pacotes que chegam serão descartados por padrão, a menos que correspondam a uma regra definida.

Comando utilizado: iptables -P INPUT DROP.

Configuração de IPs Permitidos:

A gama de IPs permitidos foi definida com base na rede interna do DEI (192.168.43.0/24). Apenas os pacotes originados desta faixa de IP foram permitidos para o porto 4000, que é usado pela nossa aplicação.

Comando utilizado: iptables -A INPUT -s 192.168.43.0/24 -p tcp --dport 4000 -j ACCEPT.

Bloqueio de Acesso Não Autorizado:

Para reforçar a segurança, adicionamos uma regra para bloquear explicitamente qualquer acesso não autorizado ao porto 4000.

Comando utilizado: iptables -A INPUT -p tcp --dport 4000 -j DROP.

Persistência da Configuração:

Para garantir que as regras do iptables permaneçam ativas após reinicializações do sistema, salvamos a configuração em um arquivo de texto.

Comandos utilizados: iptables-save | tee /etc/iptables/rules.v4 para salvar e iptables-restore < /etc/iptables/rules.v4 para carregar.

Conclusão:

Com estas configurações, conseguimos garantir que apenas os clientes da rede interna do DEI possam acessar a aplicação. Este procedimento fortalece significativamente a segurança do nosso sistema, protegendo-o contra acessos não autorizados e possíveis ameaças externas.

Feito por: Jorge Cunha 1200618.