Somaxi SECURITY

# SCAN DE VULNERABILIDADES

## PROCESSO DE SCAN DE VULNERS

O scan de vulnerabilidades é uma análise minuciosa de sistemas, redes e aplicações para identificar falhas que podem ser exploradas por atacantes. Ele é essencial para proteger sua infraestrutura e evitar prejuízos causados por brechas de segurança

## COMO O SCAN É FEITO?

O scan de é realizado através de uma abordagem que combina scans externos e internos, conforme a necessidade de segurança. O scan externo (Black Box) simula um ataque de fora da organização, sem informações internas, focando em pontos de entrada como firewalls, servidores e aplicativos web, para identificar vulnerabilidades externas. Já o scan interno é realizado com informações de acesso fornecidas pela organização, permitindo uma análise mais profunda da infraestrutura interna, como servidores, sistemas operacionais e dispositivos, para identificar falhas que não seriam visíveis externamente.

## TECNOLOGIAS UTILIZADAS

O Somaxi Security utiliza diversas ferramentas e frameworks de segurança para realizar o scan de vulnerabilidades, como OWASP Top 10, MITRE ATT&CK, Nessus, OpenVAS e Metasploit. O OWASP Top 10 identifica as vulnerabilidades mais críticas em aplicativos web, enquanto o MITRE ATT&CK ajuda a mapear as táticas e técnicas de ataque cibernético. Essas ferramentas, junto com outras como Nessus e OpenVAS, realizam varreduras detalhadas, fornecendo recomendações de mitigação.

## ANÁLISES E VARREDURAS

O Somaxi Security realiza uma varredura abrangente em toda a infraestrutura de rede, identificando vulnerabilidades em dispositivos, firewalls, servidores e outros componentes críticos, utilizando protocolos como SSH, SNMP e HTTP para garantir que todos os pontos de entrada sejam analisados. Além disso, realiza uma análise detalhada de aplicativos web, detectando falhas como injeções SQL, XSS e problemas de autenticação, utilizando ferramentas avançadas para simular ataques cibernéticos. A plataforma também realiza varreduras de sistemas operacionais e endpoints, como computadores e dispositivos móveis, identificando software desatualizado, configurações inseguras e outras falhas de segurança.

## POR QUE REALIZAR O SCAN?

Realizar o scan de vulnerabilidades é essencial para identificar falhas de segurança antes que sejam exploradas por criminosos, garantindo a proteção proativa contra ataques. Além disso, ajuda a assegurar que a organização esteja em conformidade com as regulamentações de segurança e contribui para a redução de riscos, como danos financeiros, perda de dados e danos à reputação.



Jonas Pacheco
@jonas.pacheco


Somaxi Group